IsecT Ltd.

"Putting **sec**urity into **IT**"

Frequently Avoided Questions
about
Computer Auditing

by

Dr **Gary Hinson** CISA CISM CISSP MBA

This PDF was updated in **October 2006**

Please check on-line for the very latest version:
http://www.isect.com/html/ca_faq.html

email: info@isect.com

Websites: www.isect.com and NoticeBored.com

Contents

1 Introduction

1.1 Scope and purpose

This document is published on the World Why Wait as a public resource. Our purpose is twofold: to inform and entertain. Please forgive the British humour, spelling*, InCorrect Capitalisation and distinctly cynical style ... but do experience the passion. We sincerely hope that it answers all your basic questions about computer auditing, but if not, please see the feedback section towards the end – we would really appreciate your feedback and suggestions on how to improve this FAQ. More questions. More answers. And better jokes.

The FAQ explains the main aspects of computer auditing to someone with limited prior knowledge of the topic (the Clueless But Interested). Reading the whole FAQ will give you a good overview of the whole subject and should help put it into context but don't feel too embarrassed about being bored stiff by the tenth line (or earlier if you are a quick reader). It's not everyone's cup of tea. Just pick some slightly-less-boring topics from the contents list and browse the hyperlinks until you slump over your keyboard.

If you are an auditee about to be visited for the first time by a computer auditor, you may find some clues here about the grilling you are about to endure. Our aim is to allay your worst fears by explaining the computer audit process straightforwardly. Have a dream meeting not a nightmare.

The FAQ should also prove beneficial for students and others nuts enough to consider actually becoming computer auditors, or for other nontechnical auditors (*e.g.* financial and operational auditors).

1.2 About IsecT Ltd.

IsecT is a British IT governance consultancy, specialising in computer audit (of course) and information security. Please visit our website www.isect.com for the full unexpurgated story. We offer a range of conventional IT consultancy services and some not-quite-so-conventional, including NoticeBored, our unique information security awareness service: let us help you kick-start an effective awareness program and create a security-aware culture. After that brief word from our sponsor, we return to the matter in hand.

1.3 About the author

Gary has been working in IT, information security and computer audit since the mid-1980s for employers and clients in a variety of industries (manufacturing, utilities, aerospace, banking, pharmaceuticals, technology). His qualifications include a PhD in genetics from the University of Leicester (home of DNA fingerprinting) which will surely come in handy one day if he is ever asked to audit the human genome project. Gary is a self-confessed computer geek, bookworm and web junkie. His CISA, CISSP, CISM and MBA certificates grace the wall of the office, along with world maps and plaques from amateur radio contests and photographs of Deborah, his ~~conscience~~ better half. Gary enjoys auditing, public speaking, training and Morse code, though not all at once. What little spare time he has left gets frittered away helping the ISSA or attending ISACA meetings.

* *Special note for our American cousins. Try ignoring superfluous letter u's and mentally swap the occasional 's' for a 'zee'. I speak the Queen's English not "British". You speak "American" not "English".*

2 All about computer auditing

2.1 What is computer auditing all about?

Computer auditing is a branch of general auditing concerned with governance (control) of information and communications technologies (computers). Computer auditors primarily study computer systems and networks from the point of view of examining the effectiveness of their technical and procedural controls to minimise risks. Actually, to be honest, they spend rather more of their time dealing with the people who specify, develop, test, manage, administer, use and abuse the computer systems.

2.2 Also known as ...

Computer auditing is also known as IS, IT or ICT auditing and systems auditing. In certain quarters, auditors who challenge the status quo are known as “Red Teams” or sometimes simply “Them”.

2.3 OK, so what is auditing then?

Auditing, in general, is described as: "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 improvements to limit risks". There are several significant, if somewhat boring terms in that description:

- **Independent** - the auditors should not be directly involved with the operations or management of a function being audited. They should report to a separate line of management and be free to state the facts of a situation and their honest opinions without fear of recrimination from those in the subject area. Just as importantly, independence is also a state of mind *i.e.* freethinking, able to consider situations objectively. Switzerland has the right idea. Some judicial systems come close.
- **Examination** - auditing involves the gathering and assessment of factual information from various sources. It is important that the formal outputs of the auditing process (primarily audit reports containing recommendations for control improvements) are traceable to valid information sources.
- **Records and other information**, including what are often called "audit records". 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). Computer auditors often use data analysis tools to examine computer records. Furthermore, all auditors normally interview staff in the business areas under review and may use other observational techniques to examine business processes in action.
- **Opinion** - 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. You don't have to agree with us but if you do, you'd better be ready for a ‘full and frank discussion’.
- **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.

- **System of controls** - different types of control operate at many levels. Computer auditors work with technical controls built-in to the computer systems, of course, but also procedural controls (operations procedures *etc.*), legal controls (software licences *etc.*), Human Resources controls (employment contracts *etc.*) *etc.* These controls may be preventive ('You can't do that'), detective ('I know exactly what you did and I'm really not happy') or corrective in nature ('Sort that mess out and don't do it again').
- **Recommend** - auditors generate "audit recommendations" but have neither the authority to implement suggested changes nor can we force management to do so. We achieve improvements 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.
- **Control improvements** - improving the system of controls generally means adding necessary controls that were missing. In rare cases, auditors may recommend removing controls, generally because they are ineffective, disruptive or wasteful. There's more on control just below.
- **Limit** - risks, like fraudulent politicians or spam emails, can be reduced but not totally eliminated. Good business involves making decision to minimise risks cost-effectively, and being prepared for the worst if things go wrong (contingency planning).
- **Risk** – is the chance that something might go horribly wrong. Formally, 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 the brown stuff hits the fan).

Here's another view: auditing is a mechanism for examining the effectiveness of organizations, systems, processes, risks and controls. Audits enable management and other stakeholders to:

- Discover what's really going on at a point in time
- Find out about potential problems, hopefully before it's too late to fix them
- Evaluate business situations objectively
- Face up to the truth and make informed, if difficult decisions
- Implement corrective actions, changes and improvements where needed
- Do what they really wanted to do all along but didn't have the nerve to carry off (provided, that is, the auditors agree)
- Sleep more soundly, in the end

2.4 What's so interesting about risk and control?

Risk and control are what makes auditors of all persuasions tick.

The independent eye can often see risks in a situation that those intimately involved with it either cannot see or cannot face. With training and experience, auditors come to appreciate that risk is not a purely theoretical concept – bad things *really do* happen sometimes. This is what gives auditors a bad name. If an auditor sees a boy taking his first tentative ride on a new bicycle, he sees the potential for grazed knees. His father sees a supreme athlete. His mother sees her little boy leaving home. This sense of perspective and foreboding is what distinguishes a good auditor from a cynic. It gives auditors something in common with insurance salesmen, weather forecasters and soothsayers.

Controls help to minimise risks. The insurance man expects his client to install pick-proof locks as a condition of insuring against burglary. The auditor tries to persuade management that fitting a shiny new 5-lever mortise lock on a rotten door is a false economy. He needs to understand that the insurance man sees the lock, the manager sees the cost of the lock, and the burglar sees a business opportunity.

At the same time, the auditor needs to recognise that business is about profit. Bad managers don't see the risks, take risks with little thought as to the consequences, or conversely avoid taking perfectly acceptable risks because they fear the consequences. Good managers will often push the boundaries by cutting corners and taking acceptable risks, in order to minimise costs and maximise net gain. Outstanding managers consistently make good calls, consider the potential downside and often have contingency arrangements.

This line of reasoning introduces the issue of the cost of control. We all know first hand that controls are a pain. Login controls, for instance, interfere with our legitimate use of technology. Controls are costly to specify, implement, manage and maintain. The obvious problem when designing, implementing, managing and maintaining a system of controls is to strike a balance between the cost of control and the cost of impacts resulting from risks that materialise. The real issue is that the costs we are supposed to take into account are not hard-and-fast facts, which brings us back to commercial judgement and net benefit: "Can I expect to save more by implementing control X and reducing the incidents, than I would save by not implementing control X and suffering the incidents?"

The bottom line here is that auditors inevitably take a greater interest if the stakes are high. "Let's implement an Enterprise Resource Planning system" rates somewhat above "We need a new overtime spreadsheet".

2.5 Isn't it really just accounting?

Um, well no, not really. Honest. A computer 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 recognised accountancy qualification. The study of an organization's financial/management accounting system would typically be done by a computer 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 computer audit and accounting qualifications, or teams containing each type of auditor.

2.6 Is it anything to do with counting PCs?

No! Absolutely not!! Unless, perhaps, it is necessary to substantiate a control failure *e.g*. a stock count if someone may have been stealing PCs, or if there are more PCs than licensed copies of operating systems … Computer auditors don't normally count boxes, in the same way that other auditors and accountants don't usually count beans (unless they work for Heinz). That said, certain recruitment companies persist in advertising "PC audit" jobs that turn out to be assignments for school-leavers to count PCs and check software licenses. Applicants' intellectual capacity is presumably less important than their dress sense. Here's a classic example: "Large IT service provider are urgently looking for Audit Engineer to cover site tonight from 4.00pm until midnight. Must be able to start tonight. Call for more information." [This was a genuine vacancy notice. I'm tempted to get some new business cards printed: "Gary Hinson, IsecT Ltd., emergency IT auditor. 24x7 callout. No job too large. Own overalls."]

2.7 What do computer auditors audit against?

All audits are performed in relation to certain Risks identified by the auditor which he/she believes are important ("material" in the lingo, in other words "things that would keep the shareholders up at night if they ever found out"). Analysis of the Risks leads to the definition of Control Objectives: for example, the auditor might be concerned that a finance system could be modified by unauthorized persons, so would determine that there is a Control Objective to prevent modification of the finance system by unauthorized persons.

The specific Controls that are actually embedded in or associated with IT systems and processes are then assessed to determine whether they adequately address ("mitigate", "reduce", "minimize") the Risks, meaning that they satisfy the Control Objectives. The specific Controls that the auditor looks for are typically derived from the auditor's experience or Best Practice, although there are often many alternative controls that might be adequate to satisfy the Control Objectives in a given situation: the auditor should be reasonably happy with almost any Control if the Risk is addressed, although there are advantages and disadvantages to certain Controls over others that may make them more or less attractive. And, let's be honest, security is relative not an absolute concept. So long as the Controls are Good Enough, that should be fine. Many lengthy and impassioned arguments stem from the ambiguity in that statement.

A common way out of this, um, mess is for the auditor, instead of looking for what he/she believes should be in place, to look for Best Practice Controls, an interesting concept in itself that raises more questions. Who defines Best Practice, and on what basis? What gives them the authority anyway? And if I have some other non-Best Practice control, is that necessarily A Bad Thing? So let's look at the available sources of Best Practice.

The most obvious source of Best Practice for information security is ISO, the coordinating body for most of the world's national standards bodies. ISO 17799, for example, started as British Standard BS 7799 but was adopted by ISO in 2000 and was revised and reissued in June 2005 to incorporate feedback from the wider international audience. It will become part of a more coherent and comprehensive set of information security standards (the ISO 27000-series) over the next year or two, and will continue evolving throughout its life. In information security, Best Practice is not a static goal.

There are several more sources of Best Practice:

- National standards bodies such as NIST issue lots of carefully-considered guidance on information security and other areas that could be considered Best Practice, at least within the specific scope of their intended application
- Professional bodies such as $(ISC)^2$, SANS, ISSA, ISF and ISACA also promote best information security practices in an international arena. The CISSP CBK (Common Body of Knowledge), COBIT and GAISP/GASSP (Generally Accepted Information/Systems Security Practices) are examples, in effect, of generally agreed standards of Best Practice
- Some industry bodies define their own generic information security related standards too *e.g*. SAS 70 for financial services
- Governments and legislatures define standards in the forms of laws and regulations *e.g*. for electronic signatures, copyright & governance. Some of these are really mandatory (comply or go to prison), most are highly recommended (comply or risk going to prison), and some are advisory (comply or risk spending a fortune on lawyers defending your position)
- Some individual companies set and promote their own best practice standards *e.g*. the VISA and Mastercard security programs for merchants

- Consultancies such as KPMG, PwC, E&Y *etc*. typically have their own interpretations of security standards but are increasingly using ISO 17799 and the like as the benchmarks, and fall back on professional auditing standards
- Information security professionals (CISSPs, CISMs and others) typically bring with them their own individual sets of 'accepted good practice' based on their professional experiences which, in most cases, coincide with generally accepted best practice. This is in the nature of a skilled craft - the craftsman brings his own unique mix of skills, competencies, attributes and experience to each job, and is well placed to select and adapt generic standards to the task at hand. However, beware the advice of recent college graduates without Real World Experience, some of whom scored higher on theory than common sense.

2.8 Auditing is all about compliance, right?

Not exactly although some senior auditees would find it convenient to lock it in this particular box. Many audits do include an element of checking that someone or something conforms to "the rules", whether that's internally-generated corporate policies/standards/procedures or externally-imposed laws, regulations and contractual terms ... but compliance is really management's day job. Good auditors are more likely to check whether management processes for achieving and assessing compliance are effective, and that "the rules" are suitable and sufficient, and so on. They mostly see compliance failures not so much as findings as symptoms of deeper problems.

Software license audits are a classic example. Auditors will naturally look for and report unlicensed software. Depending on scope, they may also examine and report on the organization's processes for managing software licenses, for procuring software, reallocating licenses when people leave, licensing corporate software to third parties and all manner of other things, perhaps even the corporate stance on "ethics". The auditors might trace the origin of the unlicensed software to understand why the control processes failed (this is one reason why auditors are turned on by good audit trails). Undeniable evidence of a few unlicensed copies of Office may be insignificant in the grand scheme of things but might be exactly the lever necessary to get management to wake up and smell the coffee, then fix a broken IT asset management system. It's all a matter of risk.

That said, finding twenty seven thousand unlicensed copies of Debbie Does Dallas in a secret DVD duplication factory at a Far Eastern subsidiary would probably be a different matter entirely.

2.9 How does computer audit fit with governance, risk management and information security?

Governance is a genuine solid-gold buzzword, essentially meaning systems of control. 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 to specific projects and systems.

For a rather formal perspective on the relationship between auditing and governance, read the Public Company Accounting Oversight Board (PCAOB)'s Auditing Standards. The PCAOB was established by the U.S. Securities and Exchange Commission - the SEC - as (yet another) independent oversight board to regulate/guide professionals involved in auditing companies, this time specifically regarding compliance with the Sarbanes Oxley Act of 2002 (SOX). Whether PCAOB was actually needed or not you can maybe judge for yourself from the fact that their Auditing Standard № 1 stated: "The Board has adopted as interim standards, on an initial, transitional basis, the generally accepted auditing standards, described in the American Institute of Certified Public Accountants' ("AICPA") Auditing Standards Board's Statement on Auditing Standards № 95, Generally Accepted Auditing Standards, in existence on April 16, 2003." The first standard goes on to provide template or example SOX audit reports that say virtually nothing of any practical use, but cost SEC-listed companies vast amounts to obtain. Auditing Standard № 2 further states: "In the United States, the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission has published Internal Control – Integrated Framework. Known as the COSO report, it provides a suitable and available framework for purposes of management's assessment. For that reason, the performance and reporting directions in this standard are based on the COSO framework." To give them their due, the 2nd standard does go on to describe the auditing processes in more depth but it is hardly revolutionary. <Rant over>

In relation to information and communications technology (ICT – another buzzword), proactive risk management generally implies the need to design and implement appropriate technical, procedural and physical controls, in other words information security control systems *i.e.* governance.

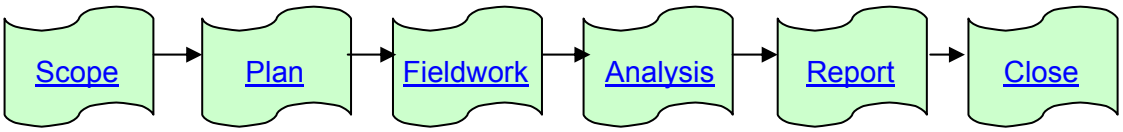
Information security managers develop, implement and operate information security control systems for ICT governance. Computer auditors review ICT governance/control systems in order to ascertain whether risks (including information security risks) are minimised. These may sound similar but are fundamentally different rôles: information security managers have executive responsibilities for securing the organisation's information assets against hackers, malware and other threats whereas computer auditors are irresponsible (if you get my drift). Auditors review, advise, report and persuade. Executive managers 'execute' … and carry the can. The common ground is minimisation 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'. ICT 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 ICT (*e.g.* the use of non-executive directors to review and guide executive management has nothing to do with ICT). Good computer auditors have a solid understanding of the practicalities of implementing their recommendations, yet are able to persuade certain auditees to go well beyond their comfort zones. With a stick if necessary.

3 How is a computer audit performed?

3.1 "How do they do that"?

Different audit organizations go about computer auditing in different ways and individual auditors have their own favourite ways of working. Purely for the sake of illustration, you understand, the main stages of a typical computer audit assignment are as follows:



Audit process flow chart[*]

1 **Scoping and pre-audit survey** - the auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading and web browsing, previous audit reports and, sometimes, subjective impressions that deserve further investigation.

2 **Planning and preparation** - during which the scope is broken down into greater levels of detail, usually involving the generation of an audit workplan or risk-control-matrix (don't be fooled, it's only a checklist with a bunch of interesting questions, space to scribble some notes and some other impressive-looking columns).

3 **Fieldwork** - gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes *etc.* This step may include the use of Computer Aided Audit Techniques (CAATs) - more info below.

4 **Analysis** - this step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Treats) or PEST (Political, Economic, Social, Technological) techniques may come in handy.

5 **Reporting** - desperately reviewing and trying to make sense of the analysis, then writing it up, re-writing it, re-re-writing it ... circulating it within the department for peer review, modifying it again, then circulating or presenting it to clients and client managers to have their say, and finally issuing it. [I bet this was a challenging process when the US Department of Health and Human Services (HHS) was audited by the Government Accountability Office (GAO), judging by the HHS comments after the report was published: "The frequent use of the word "significant" to describe control weaknesses documented throughout this GAO assessment evokes a negative connotation that is not reflective of the progress or current state of HHS' information security program," according to the HHS response." - as reported at GovHealthIT].

[*] The flow diagram could perhaps have been drawn more realistically like this:

6 **Closure** - in addition to sorting out the mess somewhat mistakenly called 'indexing and cross-referencing' and literally shutting the audit files, closure involves preparing notes for future audits and chasing-up management to complete the actions they promised months earlier. Neither the best nor the worst organizations do audit follow-ups, in both cases because there is literally no point. Most organizations however do need to 'close the loop'. Sometimes, there really are valid reasons why previously-agreed actions are not undertaken (one of the most common excuses being “Things have moved on”). Sometimes a quiet word in the CEO’s ear about the consequences (in terms of share price, career progression or jail sentence) if certain governance issues are not promptly resolved can work wonders. At the end of the day, Management not Audit carry the can (except perhaps for Arthur Anderson LLP as a result of the Enron debacle).

Steps 3 and 4 may on occasions involve the use of automated data analysis tools such as ACL or IDEA, if not Excel, Access and hand-crafted SQL queries. These can help sift through vast amounts of data on a system to identify problem areas, out-of-range values and things that simply-don’t-add-up. Automated system security analysis tools are also a boon for reviewing security parameters, and of course basic security management functions that are built-in to modern systems can help with log analysis, reviewing user access rights *etc*. Computer auditors have big toy boxes. See the section below on CAATs.

Step 5 - Reporting - is the official focus of the audit process and a great deal of attention is paid to it by both auditors and auditees. It is a fairly involved sub-process all by itself. The wise auditor starts by converting his/her thoughts that have been developing throughout the fieldwork and analysis phases into rough notes and reviewing them against the checklist and evidence. The unwise auditor just starts writing. Anyway, audit findings are summarised and analysed and tentative recommendations are made in the First Draft Report.

Audit’s fabled quality control process then springs lithely into action, in other words the First Draft is savaged by the seasoned campaigners of the department and rewritten by the auditor with their ‘assistance’ until it barely resembles the original draft. Remember, editing is a rewording activity. Someone, sometimes checks that ‘everything reportable is reported and everything reported is reportable’ which essentially means a file review. The audit manager/reviewer looks at the evidence, discounts much of the auditor’s analysis due to their ‘inexperience’ and (in the back of his mind) rewrites the audit report in his/her own inimitable style. The red-penned draft report is handed back for yet another round of ‘slight revision’ and so the game continues.

When at last everyone in Audit is thoroughly sick of it, the Final Draft Report is sent for its first external review by, or presented to, the auditees ... and then the real battle commences. The findings are challenged. The analysis is challenged. The scope is revisited. Every phrase and nuance is challenged. The spelling is challenged. Even the font and font size are challenged. The quality of the paper is challenged. The auditor’s competence is challenged. Even his/her parentage may be questioned if things really get nasty. The actual issues and recommendations are ignored as long as possible until, eventually, reality starts to dawn. Shock! Horror! The indignant auditees are being asked to change! And maybe, just maybe, the auditor has a point. This realisation is often a trigger to revisit the findings and analysis and to perhaps challenge those split infinitives just for good measure. Frustration mounts. Tempers fray. The full-and-frank discussion continues apace. Gallows are prepared. Clandestine meetings are held between senior auditees and senior auditors (a.k.a. UN Peacekeepers) to reach a negotiated settlement. And so, eventually, the Final Final Final Definitely The Last Draft Ever becomes Issued.

To auditees, I say “Get a life. Deal with it. You know it makes sense.” To auditors, this: “Walk a mile in a man’s shoes before criticising him. That way, when you voice your criticisms, you’re a mile away and you have his shoes.”

By the way, there's also a step 0, namely the audit schedule or audit plan. Like babies, audits don't just happen. Someone somewhere makes a decision to 'look at situations X and Y this year but leave Z until next year', according to their assessment of the risks in X, Y and Z. "How do you know the risks if you don't examine them first?" I hear you ask. Good question. That's why there are high-level and low-level audits, periodic audits, and management requested Special Investigations. And that's one reason why Audit Directors keep little black books locked in their desks. Upset the Audit Director at your peril.

3.2 How long does an audit take?

~~As long as a piece of string~~.

In our experience, the complete sequence of events for a discrete audit assignment normally takes months elapsed time from start-to-finish, almost regardless of the amount of time spent actually doing the fieldwork and analysis. The reporting and closure phases are often very drawn out, especially for those audits that are too broadly scoped, reveal particularly unwelcome news or recommend substantial changes. Conversely, narrowly focused audits on uncontentious material may be completed in just a few days … but then one would have to ask why such audits are ever performed as audit resources are normally directed to investigate high-risk issues.

As a rule of thumb, roughly equal amounts of elapsed time should be allocated to each of the six steps noted above. For the 'numerically challenged', that means an audit planned to include about a week of fieldwork will take approximately six weeks in total. At a push, it is possible to do a complete audit start-to-finish in a week provided you don't expect more than about a day's actual fieldwork. And the auditor works a six day week. Or very long days.

Progressive organizations audit their IT developments and other major change projects throughout the project lifecycles, from cradle-to-grave. In these cases, audits last as long as the projects in elapsed time but consume just a few percent of the total project man-days.

3.3 What questions should a computer auditor ask?

Here's a fairly typical query from someone who has read this FAQ and wants to give it a go themselves: "I'd like to know more about the specific questions that an auditor should ask a Systems Administrator about the types of system/application access controls in an application. I have compiled a brief list of questions that I think I would like to ask my systems administrators however, I don't want to miss anything important ..." And here's my answer:

"First of all, I'd suggest that the best way to start is to conduct some form of risk assessment as a starting point to your audit/review (it's only an audit if you are truly independent of the area under review). You can use a formal risk assessment method (there's plenty to choose from) but personally I prefer simply to think carefully and separately about the threats (generally the people, things or situations that could potentially cause loss), vulnerabilities (any weaknesses in the system of controls that might be exploited by threats) and impacts (what would be the [worst case] effects if some of those threats actually materialized and hit some of your vulnerabilities?). An interesting way to do this in practice is to brainstorm, perhaps with a colleague who understands the situation you are reviewing, someone who knows about risk and control (an experienced auditor or information security/risk manager, maybe a consultant), and ideally someone representing the business/IT owner(s) of the system under review (this person will probably end up being your main 'client' contact on the audit, and they will understand what's driving you to ask lots of awkward questions later on). You can safely ignore the 'low' threats, vulnerabilities and impacts, and you can probably set aside the 'mediums' too for now. You should definitely prioritize the 'highs' for obvious reasons. These are the things that would keep you, the system owners, the CEO and the

shareholders (if only they knew!) awake at night. They are the main areas of concern that you will need to explore in the actual audit fieldwork.

Next, I like to develop some reasonably realistic, business-oriented scenarios in which the high risks could come to pass. These help me think-through the risks and are helpful if, later on, people start pushing back when I'm asking those awkward questions.

Next, develop your 'audit checklist', mind-map or whatever you use to map out the things you want to check, the issues that concern you, and the boundaries of your audit. This is an important step, drawing on the control objectives and specific controls that you are going to go looking for.

After all that preparation, the actual audit work is quite straightforward! It's time to gather your evidence, ask questions, take copious notes, explore the threats/vulnerabilities/impacts, check the controls, challenge things that seem suspect, ask more questions, look for evidence that the controls are actually working or not, think hard and ask the really awkward/tough questions that nobody wants to answer, and generally probe around, following your nose until the time is up.

The hardest bit of all involves taking all the information from the previous steps into account, thinking it over, checking the details and making sense of it in your head, then developing rational arguments for why Something Must Be Done. This is the primary output of the audit - the impetus for change.

The last bits are to prepare a draft report, decide on some recommended changes, discuss/negotiate these with the client, update the report and finally present and 'issue' the report. Easy peasy ... OK not really, but not too hard if the previous steps have been done thoroughly. You should be in a strong position to argue your point, but even now you sometimes need to be prepared to concede weaker points in order to push through your main points, and always be prepared to go back and 'take another look' if someone insists you have got a fundamental point or finding wrong.

And if that's all too much, find yourself a real computer auditor but stick to them the way non-stick paint sticks on a frying pan so, next time, maybe you'll have the nerve to fly solo.

Ok, now to answer your original question. You're asking me to go directly to step 3 and come up with specific audit questions to ask your sysadmins about access control on a system of which I have no knowledge at all. Sorry, no go. The best I can do is refer you to some generic audit checklists such as those at ASAP ... but don't expect too much. If you want to do a good job and be reasonably certain of not missing any serious risks, you really need to start with steps 1 and 2 above to figure out your own questions."

3.4 How long should a computer audit take?

In our experience, the complete sequence of events for a discrete audit assignment normally takes months from start-to-finish, almost regardless of the amount of time spent actually doing the fieldwork and analysis. The reporting and closure phases are often very drawn out, especially for those audits that are too broadly scoped, reveal particularly unwelcome news or recommend substantial changes. Conversely, narrowly focused audits on uncontentious material may be completed in just a few days … but then one would have to ask why such audits are ever performed as audit resources are normally directed to investigate high-risk issues.

As a rule of thumb, roughly equal amounts of elapsed time should be allocated to each of the six steps noted above. For the 'numerically challenged', that means an audit planned to include about a week of fieldwork will take approximately six weeks in total. At a push, it is possible to do a complete audit start-to-finish in a week provided you don't expect more than about a day's actual fieldwork. And the auditor works a six day week. Or very long days. Geddit?

Progressive organizations audit their IT developments and other major change projects throughout the project lifecycles, from cradle-to-grave. In these cases, audits last as long as the projects in elapsed time but consume just a few percent the total project man-days.

3.5 What is the scope of computer audit?

The scope of a particular computer audit is normally defined by the scoping document produced near the start of the assignment – typically it relates to certain key risks of concern to management that centre around the computer and/or telecommunications systems. The scope of an audit assignment is normally a balance between breadth (*i.e.* the range of matters to be reviewed) and depth (*i.e.* the amount of detail reviewed in each matter). Clever audit plans allow for a bit of both through mixing broadly-scoped high-level audits (designed to find the most important risk areas) with narrowly-scoped in-depth audits (to give those pesky high risk areas a thorough going-over), and clever audit managers allow staff to blow the budget on certain jobs that just deserve more time.

The scope of computer audit, as a function, is hard to define as it depends on the size and make-up of the audit team: in large audit teams, computer audit may have a number of dedicated and specialised staff solely responsible for technology auditing, but more often the computer auditors are expected to contribute to other types of audit (and vice versa). In really small, unenlightened audit teams, it is not uncommon for the computer auditor to be treated as the Ravenous Bugblattered Beast of Traal.

The scope of the computer audit function is defined by a combination of factors, including:

- The remit of the Department (for Internal Audit) or the contract (External Audit) in relation to other review and control functions (*e.g.* information security, risk management, legal)
- Audit resources *i.e.* the number of computer auditors, other auditors and their managers, plus the breadth and depth of their experience in computer audit (*e.g.* in some departments, IT-skilled business auditors cover a lot of areas that would be left to IT auditors elsewhere)
- Scope of the individual computer audit assignments
- The audit plan for the period - usually documents the high-risk topics the auditors are likely to cover
- State of relations with client functions. Whereas some departments refer to formal definitions, 'audit friendly' folk tend to be more chilled-out to the extent that auditors may even occasionally be called upon to perform conventional (internal) consultancy rôles.

Typically, however, the computer audit function covers the following areas:

- Operational computer systems (servers, workstations), networks (LANs, WANs) and data
- Computer systems under development and/or being tested or implemented
- The IT Department whether central or distributed and their relationship with management, user departments, end-users, support/admin functions (*e.g.* Human Remains, Legal), customers, suppliers, partners, regulators *etc*.

In each case, computer audit resources are primarily directed towards "high-risk situations" ('business-critical' applications may be reviewed annually), although lower-risk areas may be audited on a less frequent basis (perhaps reviewed on a 3 year cycle, soon after an 'incident' or 'breach', or more prosaically when senior management finally notices that an important company system or department has never been independently reviewed ~~and is a pile of poo~~). There is an important point here: audit should always align itself according to risks to the organisation.

3.6 What is the difference between Internal and External (computer) audit?

Cynical answer: “Only the latter have leather seats in their cars” ... but in fact the main distinction is the degree of independence from the organization being audited.

External Auditors are always employed by a separate organization and are normally contracted by the organization to perform audits as part of the annual process of preparing company accounts. In practice, External Auditors are mostly employed for a few months a year to examine and provide a formal opinion on the veracity of the organization's financial accounts. Their formal opinion is normally presented in a highly-stylised form in the organization's annual report to shareholders. Computer auditors working for an External Audit company are typically concerned with integrity of the client's core financial data and accounting systems (general ledger *etc*.) and other important systems involved in generating and processing financial records (*e.g*. sales order processing systems).

Internal Auditors, by contrast, are permanently employed by the organization to examine and comment on its control systems and processes on an ongoing basis, although (as noted earlier) they do not normally report to the organization's conventional executive management structure. Some organizations outsource Internal Audit to external consultancies but this merely clouds the issue. Their remit usually extends well beyond the core financial systems, encompassing the broader systems of corporate governance (also known as 'management controls'). In some organizations, the External and Internal Auditors have separate but complementary areas of scope: External Auditors primarily cover the core financial systems whilst Internal Auditors primarily cover the remainder. In most cases, however, the two functions overlap, working together on some parts.

Certain External Auditors like to sell consultancy services to their audit clients but this creates an interesting moral dilemma and a governance paradox. “As your game-keeper, I’m delighted to recommend the services of my favourite poacher …”.

3.7 What are the main types of computer audit?

Operational computer system/network audits: review the controls within and surrounding operational computer systems and networks, at various levels *e.g.* network, operating system, layered software, application software, databases, logical/procedural controls, preventive/detective/corrective controls, crypto, logging ...

IT installation audits: take a look at the computer building, suite, room or cupboard, including aspects such as physical security (walls, CCTV, locks, guards, barbed wire, visitor procedures ...), environmental controls (fire and flood protection, power supply, hair conditioning), computer and network operations processes and management systems, oh and the IT equipment itself.

Developing systems audits: typically cover either or both of two aspects: (1) project/programme management controls (often, the auditor is the only person with the knowledge, experience and balls nerve to point out that the average project manager’s progress reporting is “somewhat optimistic” at best); and (2) the specification, development, testing, implementation and operation of technical and procedural controls, including classical technical information security controls and the related business process controls.

IT management audits: review the organization, structure, strategy, work planning, resource planning, budgeting, cost controls *etc.* and, where applicable, relationships with outsourced IT providers (in some cases, these aspects may be audited by operations and financial auditors, leaving the computer auditors to the more technological aspects).

IT process audits: review processes which take place within IT such as application development, testing, implementation, operations, maintenance, housekeeping (backups, preventive maintenance *etc.*), support, incident handling.

Change management audits: review the planning and control of changes to systems, networks, applications, processes, facilities *etc.*, including configuration management, control over the promotion of code from development through testing to production, and the management of changes to the organisation as a result of ICT.

Information security & control audits: review controls relating to confidentiality, integrity and availability of systems and data.

IT legal compliance audits: review legal and regulatory aspects of IT systems (*e.g.* software copyright compliance, protection of personal data).

Disaster contingency/business continuity planning/disaster recovery audits: review arrangements to restore some semblance of normality after a disaster affecting the IT systems, and perhaps assess the organisation's approach to risk management.

IT strategy audits: review various aspects of IT strategy, vision and plans, including their relationship to other strategies, visions and plans, or not as the case may be.

"Special investigations": this is audit-speak for contingency and un-pre-planned work such as investigating suspected frauds or information security breaches, performing due diligence review of IT assets for mergers and acquisitions *etc.* Or Christmas parties.

3.8 Computer Aided Audit Techniques CAATs

CAATs don't have fur, don't scratch you and don't poop in your neighbour's garden. CAATs are tools/utilities to help auditors select, gather, analyse and report audit findings. Starting with the basics, many computer applications have useful built-in data analysis/audit facilities. Microsoft Excel, for example, has functions for tracing dependencies between cells, sorting data ranges *etc*. Database programs typically have custom reporting facilities (such as SQL) and sometimes include pre-configured reports intended for auditors (these are usually written for specific applications such as SAP). Practically any specific database auditing queries can usually be crafted in SQL if the auditor has the expertise and access rights - the most important skill being the ability to ask meaningful questions in the first place. Specialised CAAT tools such as ACL (Audit Control Language) and IDEA (Interactive Data Extraction and Analysis) include libraries of prewritten queries to ask meaningful questions on data sets. Other utilities such as WizRule help explore complex data sets and applications.

Here are the sorts of questions a computer auditor (or an ordinary auditor working on a computer system) might want to ask:

- What were the top 10% of transactions by value last March?
- How many changes were made to the customer details file during the previous year?
- Are there any out-of-range or unusual data values in column 4, or any suspicious data patterns?
- Are any of our suppliers also employees?
- Who will win the next World Cup? [worth asking perhaps but can you trust the answer?]

CAATs are wonderful for asking bizarre audit questions that ordinary system users, managers, analysts and developers have probably never even considered, some of which can lead to the identification of frauds or confirmation that control weaknesses have not been exploited. Complex, highly convoluted and especially cunning CAAT queries can take hours to run against large data sets and are a great excuse for the computer auditor to slip away from the desk for quick coffee or (on a slow machine) a very long liquid lunch ... but the quality of the output is proportional to the quality of the question asked, not necessarily the time taken or the size of the report. Big thick auditors produce big thick reports. The real trick is to apply Occam's razor - find the simplest analysis that addresses the risks.

Information security applications such as intrusion detection systems, penetration testing and vulnerability assessment tools could also be considered CAATs since they can be used by auditors to find information security control weaknesses. This is a good example of the use of automation to 'leverage limited available skilled human resources'. The Center for Internet Security's excellent free system security benchmarking tools, for instance, make it a breeze to find common security weaknesses in Windows, UNIX and other platforms. Still it takes skill and judgement to figure out which of the long list of system security issues have to be resolved by next Tuesday.

3.9 Why don't the auditors stop IT development projects going off-the-rails?

Developing systems audits are arguably the most difficult type of computer audit assignment. They often involve a cat-and-mouse game of 'show me' and 'watch my lips', in other words the auditor asks for something truly obscure and weird such as "the business case" or "the security specifications" and someone with nothing better to do is sent into a dark corner to write it. Audited development projects almost invariably involve vast amounts of money since computer auditors seldom get the opportunity to audit small projects and end-user developments perceived (by management at least) as low risk.

It is an unfortunate truth that in IT, professional, disciplined and effective project management is the exception rather than the rule. An experienced computer auditor has generally witnessed all sorts of disasters at close range through auditing a number of development projects. For some obscure reason buried deep in human psychology, the symptoms of imminent disaster that loom large to an experienced computer auditor are mysteriously invisible to the average project manager … and indeed to their manager and senior management as a breed. But that's only the start of it. Persuading the organisation to stop a runaway project is very much like trying to stop a freight train at full speed. Ordinary brakes are simply not good enough. The reason is known as "corporate politics": big projects are almost invariably led by bigger-than-life characters, specifically appointed by management because they are "good blokes". The IT auditor's rôle is truly to proclaim that the king hath no clothes. And make like an enormous block of concrete and steel.

Do you remember the rather boring definition of computer audit? Audit is about encouraging management to manage and reduce if not eliminate their risks. Auditors help identify and find ways to limit the risks relating to IT developments. Proactive managers take note of audit recommendations and make effective business decisions. Others don't.

IT auditors, operational auditors and financial auditors potentially have a lot to offer the development projects such as:

- Reviewing business cases to see if they hold water and conform to corporate investment policies and 'risk appetite'
- Reviewing project management controls through attending the Project Control Group as a "nonvoting observer", reviewing project plans & progress reported, reviewing project risk and quality management processes etc. (including periodic or phase-end audits)

- Mentoring project managers, user management, project team members, users, testers *etc*.
- Reviewing risk assessments, system security designs etc. from Audit's (governance and control specialist) point of view
- Contributing to system designs, acting as specialist advisors on various risk and control topics
- Helping management specify "audit trails", "anti-fraud controls" and various other aspects of security and control functionality
- Hands-on testing of key controls
- Reviewing implementation processes and process or quality assurance controls (e.g. have sensible plans been prepared to “cleanse” malodorous data from the old system? Have new users, sysadmins and support people received appropriate training? Have new users, sysadmins and support people been assigned to suitable roles with appropriate access rights? Has “enough” testing been done? Are all approvals complete i.e. have appropriate people been involved in testing and signing-off the system? Is there clear accountability just in case the new system falls in a smoking heap on day 1?)
- Auditing project costs and benefits claimed by the project team and user departments
- Facilitating post-implementation review meetings to tease out the lessons learnt for future reference

3.10 Aren't computer auditors meant to stop (computer) frauds?

NO! At least not directly, unless the frauds are perpetrated within the computer audit function. Audit independence means that auditors do not form part of the routine system of controls in operational areas of an organization - that dubious honour usually belongs to "management" or, more broadly, "someone else". Managers and staff are responsible for designing, implementing, operating and maintaining the appropriate system of controls to prevent fraud or other control failures (*e.g*. accidental loss of key data, or even the keys to the fire safe). Auditors are responsible for examining and commenting on those controls but again it is management's duty to respond appropriately to audit reports and recommendations. You might say that auditors are irresponsible.

3.11 Who audits the auditors?

Look here ~~smartarse~~, auditors are (mostly) highly-trained professionals diligently following structured and formal processes that include all sorts of process controls. Their work is routinely scrutinised by themselves, by other auditors and audit managers, by auditees and by senior management. Conventional audit working practices ensure that everything considered reportable is in fact reported and that everything reported can be traced to objective evidence. The audit reporting process consists largely of repeated cycles of review and revision, including ‘quality reviews’ and/or ‘file reviews’ comparing reports to the actual evidence and analysis. If you want to audit the auditors, go ahead, make my day.

3.12 Do computer auditors give technical support to the rest of audit?

Sometimes but that is certainly not their main purpose in life. Because of their technical competence, familiarity with technology and their links within IT (OK, because they are geeks), computer auditors often find themselves nominated as local IT co-ordinators within the audit function but have to balance this rôle with the demands of their scheduled audit work. In much the same way, financial auditors might be willing to give advice to colleagues on their tax returns *etc.* but should not be expected to do so to the extent that audit assignments run late. It's all a matter of balance and judgement. And perhaps bribery.

3.13 What happens to the audit evidence?

"Audit evidence" in a typical computer audit comprises system dumps and printouts, interview notes and a whole variety of audit working papers (*e.g.* risk analysis, assessment of key risks, controls review checklists and draft audit reports). A full-scope detailed audit can easily generate several lever arch files stuffed with paperwork and megabytes of computer data. However, the value of an audit is emphatically NOT a function of the amount of material generated. Big is not necessarily better. Small is cool.

There is no hard-and-fast rule about what goes into the audit files, nor what stays there - it's mostly down to local practice and relates to the primary objective of the audit function. If the purpose is essentially to "improve the organization" through improved controls, reduced risks and greater efficiency (a classic consultancy-type mission for internal audit), then there is a different need to obtain and retain evidence, audit reports *etc.* than if the rôle is to "assess compliance with laws, regulations and policies, and identify and report weaknesses" (more like external audit).

Reports from the former type of audit function are not ends in themselves, but are means of persuading management to make improvements. They are typically the basis for an open discussion with management. So long as management eventually accepts the report and makes improvements, the aim is met. The final report plus management feedback (typically an agreed action plan naming responsible parties and with deadlines) should be sufficient record, although it is normal to retain other key audit evidence, working papers, risk assessments *etc.* for future work in the same area. The relationship between auditor and auditee/management is based on trust - management are responsible for enacting the recommendations as they see fit, audit merely advises and provides the motivation to act. Audit anticipates action even on items that were not reported formally, including less material points and issues which they believe to be true but were perhaps unable to prove.

Reports from the latter tend to be more formalized. They are the formal statements from audit which management had better act on, or else! In some cases, they are a matter of public record. The final issued report, plus the key evidence, plus the discussion on drafts - all are important elements of this formal style of auditing, and will probably be required if there is an "inquest" later. The audit-auditee relationship is based on distrust - audit has to report formally in order to get management to act at all, and expects that anything not stated formally in the final issued report will probably not happen. Unfortunate but essentially true.

Clearly, the differences have been exaggerated for the sake of emphasis. In practice, there is a continuum between these extremes (and even more extreme versions are possible I guess). Also, individual audits vary in formality.

A more prosaic method is simply to retain "everything" for, say, six months to a year in case they are needed, then trim out the junk and close the file. Even more pragmatic is the 'dump it in a dark corner of the filing cabinet until we have no more storage space left , then drop it in the shreddy bin while the boss is out' approach, common in practice but seldom acknowledged.

By the way, it is A Jolly Good Idea to insist that all auditors routinely use strong access controls (such as decent encryption and multifactor authentication for electronic data plus locked cabinets or safes for paper-base information) to protect audit evidence against unauthorised access. There have been far too many incidents recently where auditors' laptops have been stolen or lost. It is entirely reasonable to make this a firm requirement of the contract with external auditors and a corporate policy covering internal auditors. I'll leave the question of who should check that the controls are properly implemented as an exercise, dear reader.

4 How should I find a consultant IT auditor?

[In the dim and distant past, I have been a consultant IT auditor. I now have a real job. This is not a sales pitch. I am not for sale.] If you don't have the skills in-house, it is possible to contract with third party IT audit specialists but, before you sign on the dotted line, there are quite a few things to consider ...

4.1 How should I word an Invitation To Treat (ITT)?

I would say there are three key aspects to cover when preparing an ITT:

1 First is to define the audit such as the scope (what risks you want examining, depth and breadth of coverage, any constraints, any especially 'interesting' elements that need a really good poke around, number or percentage of locations/systems/networks/users to be reviewed and what they are to be reviewed against *e.g.* good practice information security management such as ISO 17799 or relevant legislation) and reporting (how and when is the assignment to be reported, and to what level of detail *e.g.* executive summary, management report, recommendations, structured audit files with evidence ... ?) [This information would of course still be needed if the audit was run by in-house employees]

2 Secondly, what type of auditor are you looking for? What qualifications and experience (*e.g.* CISA, QiCA, relevant industry and management experience - there's more information in the next section of this FAQ)? What are the personal characteristics that would suit the job, or conversely would not be suitable? What kind of person would you personally like to work with? Are you looking for a consultative or confrontational approach? How important is personal hygiene to you?

3 Thirdly, how will the assignment be managed? How would you like to relate to/manage/deal with the consultant(s)? Do you want them to take the lead, drive the job, report the findings, generate an agreed management action plan *etc.* or do you purely want someone to do the fieldwork to your specifications and guidance? Or something else? Are you thinking about someone to organise and coordinate/manage a team of auditors, a whole team, or someone to work alone? Do you want a weekly update, monthly reporting, or what? This is an important section of the ITT, often neglected. If you get this section right, your relationship with the consultant/s should be much less stressful all round (the same applies to the consultant/s).

4.2 Who should I "Invite To Tender"?

You have already demonstrated your initiative by finding this FAQ on the web - the web is the natural place to search for potential suppliers. Googling "it.audit.consultant" finds over 1.1 million pages so you shouldn't exactly be short of choice. The market is quite diverse, ranging from The Big ~~Six~~ ~~Five~~ Four up to little one-man-bands, but don't mistake sheer size for competence or suitability. If you need help to choose or manage the assignment, look for agencies that specialise in audit and information security or perhaps consider contracting with an independent, trustworthy and experienced consultant to run the assignment for you.

4.3 How should I select from the proposals?

Assuming you sent your ITT to a bunch of potential suppliers, and assuming that you thought carefully about your requirements and prepared a detailed ITT in the first place, it should be fairly straightforward to shortlist a small handful of suppliers simply by excluding those who clearly do not stand up to one or more of your selection criteria. Be ruthless: the amount of ruth should be inversely proportional to the number of respondents.

Now comes the interesting part: final selection.

Value for money is arguably the most important matter. I'm deliberately using 'value' not 'price': I don't mean that price is not important but if you have prepared a good ITT as described above, the consultants who propose should be more or less in the same range for man-day rates - those who look expensive are probably "pricey" (dare I say, "taking you for a ride") but may be offering additional value services, whereas those who look like bargains are probably "cheap and nasty" (or "bargain basement" as we say in England). Value-for-money is the flip side of you-get-what-you-pay-for.

One more tip for selecting is to look at the quality of the suppliers' proposals - this should be a guide to their ability to write a good audit report and gives you a clue about the way they intend to approach the job. Can they write good English (or whatever)? Look for proposals that actually reflect what YOU want from the job, not standard boilerplate responses that have been cut-and-pasted for your assignment. By the way, glossy brochures and so on are more boilerplate. Look behind the gloss and polish to see the real quality. Think 'second hand car salesmen' and you've got the right idea.

Finally, make sure to review the CV/s of, and ideally speak to, the actual person/people who will be leading and performing the assignment ... which means, by the way, that you really want to contract with a specific person or team of people, not a faceless "team". It is not unknown for sales pitches to be fronted by top-notch consultants but wet-behind-the-ears juniors to be placed on the job. Juniors are not necessarily A Bad Thing (we all had to start somewhere) but audit teams should be balanced. And it is not unreasonable to expect to pay much less for juniors than seniors. Now is the time to deal with this issue. If you'd like to meet the team, ask. If half the team is still in kindergarten, you have your answer.

4.4 OK, what next?

Prepare and sign a solid legally-binding contract, of course, but the contract is really just a last resort in case everything goes horribly wrong. Your real task is to initiate the relationship with the supplier, reiterate your requirements to the person or team, and initiate the assignment. This is not an excuse to abdicate all responsibility - all auditors need management support and guidance from time to time. At the start, especially, the auditor/s will welcome background information and contact details. If you can provide a well-written scope document, or else generate one now in conjunction with the auditor/s, and get it signed-off by your management, they will be all set to do the job.

Remember the third part of the ITT? This is where your preparation starts to pay off. Set up a management process to track and guide the audit as you wish, in conjunction with the audit leader. Invest some of your valuable time to get this process working smoothly and you will not regret it. The trick is to develop a management style that avoids nasty surprises for you but gives the auditors the latitude to apply their qualifications and experience. Good luck.

5 I think I want to become a computer auditor

~~Mad fool!~~ ~~First seek medical attention~~. ~~See your shrink~~. ~~Get some therapy~~.

"Computer audit seems cool. I'm sure I could do that! But how do I become a computer auditor?" This FAQ section helps you explore your options.

5.1 How should I start?

This section explains how to go about becoming a computer auditor by describing the competencies, qualifications and experience necessary. It may also prove useful for those interviewing, selecting and appointing computer auditors, especially if candidates present curious credentials.

The best place to start anything is at the beginning. Alice in Wonderland's "Begin at the beginning and go on till you come to the end; then stop" is still my favourite (OK, my only) literary example of a computer program. Read the whole of this FAQ. No really. Go back and read the bits you skipped earlier because they were just TOO boring. Read the whole of this section. Read the end bits. Follow the hyperlinks. Read all you can about computer auditing. The first, and for that matter the last lesson about auditing is to learn to *really* listen to what you are actually being told. Read the lines and then between the lines.

An editorial piece at CertMag.com advises you to think in terms of making a career move not just a job move, in other words you should invest in your chosen occupation. The article refers to careers information security but I find applies equally to computer auditing. Bill Royds offers more sage advice: "**Find something to do that you love doing and are passionate about. You then will be willing to work the hours and spend the effort to achieve in that field. You are unlikely to be successful in a field where you are not really willing to spend the effort of your peers who love it.**" Hear hear!

Your organization may advertise audit rôles on the standard jobs boards but it's probably worth taking the initiative and approaching the Head of Audit, the Head of Computer Audit, an ordinary auditor or someone in HR to ask if there are any job opportunities in audit. If you're not absolutely certain that audit is for you, you could try asking for a temporary secondment into audit, perhaps to help out on a planned computer audit (so long as it is not an audit of your own area!).

There are two main routes into computer audit: firstly, from technology (often information security, operations, project management, development or business analysis), alternatively from accountancy (general or financial audit, financial or management accounting). Other accepted entry routes include risk management, quality assurance and general management. A surprising number of companies insist that those destined for the Top Table (Board positions) take a spell in Audit, which almost makes it sound like an interesting career move. Straight out of college is also possible but not recommended. Let the backs of your ears dry first.

Information security is probably the most closely allied field to computer audit since it also encompasses the concepts of risk and control in relation to computer and telecommunications systems, and senior information security staff normally have reasonably good working relationships with both IT and 'the business' (outside of IT). Speaking personally, the whole of my professional career has alternated ('careered') between information security and computer audit rôles and I still enjoy both sides of the fence immensely. Just remember not to fall with one leg each side.

Finally, some of us became auditors because we were once audited and appreciated a job well done. Higher pay and not having to complete the Agreed Action Plan were just the icing on the cake, you understand.

5.2 I am already an auditor – can I become a computer auditor?

Probably – it depends on your level of technical awareness/competence. If you have a technology background, you may have sufficient awareness/competence already. If not, you will have to 'learn the trade'.

If you have been auditing business processes for the past N years, you are almost certainly familiar with auditing the use of computer systems and have maybe used one yourself once or twice. At one level, computer auditors simply take a deeper interest in the IT systems that, until now, may have seemed merely like tools of the trade to you. They have a fascination with the technology for technology's sake. They actually enjoy fiddling around in the back of a computer box, snooping around the source code for a database application or figuring out which protocols and ports are being used. Many of them have computer networks at home that they play with during their evenings and weekends, without even being paid. If pressed, they mostly admit to being nerds. A predilection for pizzas is a bit of a giveaway.

5.3 What qualifications do I need?

5.3.1 Computer audit & information security qualifications

Certification and Accreditation (C&A - nothing to do with the British clothes store of the same name) is something of a growth area for various professional computer audit, information security and certification organizations, partly because it is a 'nice little earner', so you face quite a choice. Check out our list of qualifications (in no particular order):

- BSc, PhD and similar academic qualifications in information security and/or computer auditing *e.g.* from eminent institutions such as Royal Holloway, University of Houston, University of Nebraska, University of Texas, University of Norwich and Colorado Technical University. Accused by those with their ears too close together of being "too academic", courses like these give students the conceptual framework, depth of understanding and confidence to tackle any infosec topic, including the most technical issues, provided they are prepared to put in the time and effort to gain real-world experience.
- GIAC: Global Information Assurance Certification by SANS - includes a general information security course plus specialisations (*e.g.* "G7799" is the GIAC ISO 17799 specialism). GIAC originally involved a practical element to the assessment but unfortunately it no longer does
- QiCA: Qualification in Computer Auditing from the Institute of Internal Auditors - a well-established qualification from a well-respected professional organization
- CISA: Certified Information Systems Auditor (here's an independent view of CISA which is also a well-established qualification from a well-respected professional body, probably the most widely trusted IT audit certification) and CISM Certified Information Security Manager (a newer certification, broadly similar to CISSP but with more emphasis on management judgment and experience on information security management matters), both from ISACA whose focus has shifted from IT audit to IT governance

- SSCP: Systems Security Certified Practitioner (aimed at practioners/professionals with a focus on information security implementation *i.e.* those people that enforce the information security policies, processes and procedures on a daily basis; requires 1 year's work experience; said to be ideal for those working toward or who have already attained positions as Senior Network Security Engineers, Senior Security Systems Analysts or Senior Security Administrators) and CISSP Certified Information Systems Security Professional (the world leading qualification in information security; scope a mile wide but an inch deep; requires 4 years' work experience), plus ISSAP, ISSEP and ISSMP (Information Systems Security Architecture/Engineering/Management Professional specialisations; an inch wide and a mile deep in each case; only available to people with CISSPs already) - all of these from (ISC)², the International Information Systems Security Certification Consortium that exists purely to certify infosec professionals
- CCE: Certified Computer Examiner from the International Society of Forensic Computer Examiners - for forensic IT specialists
- CEH: Certified Ethical Hacker, CHFI Computer Hacking Forensic Investigator, LPT Licensed Penetration Tester and ECSA EC-Council Certified Security Analyst, all from "EC Council" which is the self-styled International Council of E-Commerce Consultants, not some obscure body of the European Commission
- Security+: a basic entry-level information security qualification from CompTIA, the Computing Technology Industry Association
- MCSE:security and MCSA:security - Microsoft Certified Systems Engineer and Administrator certifications with security specialism from Microsoft
- ABCP, CBCP & MBCP: Associate, Certified & Master Business Continuity Professional certifications from DRII, the Disaster Recovery Institute International
- Certificate in Information Security Management Principles from BCS, the British Computer Society
- PCI & CPP: Professional Certified Investigator and Certified Protection Professional from ASIS International
- PCIP: Professional in Critical Infrastructure Protection (previously CCISP - Certified Critical Infrastructure Security Professional [?]) is a certification from the Critical Infrastructure Institute, covering the design, maintenance, and management of security architectures for critical infrastructure, SCADA and other high-availability environments
- CFE: Certified Fraud Examiner from ACFE, the Association of Certified Fraud Examiners.
- TICSA and TICSE: TruSecure's ICSA Certified Security Associate/Expert program. Although TruSecure runs the program and charges nearly $300 a pop, it is said to be vendor-neutral (we'd love to hear from you if you have been through the program and agree or disagree ...)
- CCSA, CCSE, CCSE Plus, CCMSE, CCMSE Plus VSX, CCSPA: are Check Point's no-bones vendor-specific certifications (CCSA is also the IIA's Certified Control Self Assessor qualification - there's more info in the next section)
- CCIE, CCSP, CCNP, CCIP, CCDP *etc*. are Cisco's no-bones vendor-specific certifications
- EnCE - Encase Certified Examiner vendor-specific certification by Guidance Software, supplier of Encase, the industry standard IT forensic software.

- IBM Certified Advanced Deployment Professional - Tivoli Security Management Solutions QED.
- ISS-CA, ISS-CE & ISS-CS - ISS-Certified Architect, Expert or Specialist from Internet Security Systems
- ISSPCS - the International Systems Security Professional Certification Scheme from the International Systems Security Engineering Association (ISSEA)
- CCO - Certified Confidentiality Officer from BECCA, the Business Espionage, Controls and Countermeasures Association

For another perspective, see here.

Professional qualifications bring two key benefits: firstly, you need to study to pass most of them, in other words you become more edumacated. Secondly, they demonstrate that you have achieved a certain level of competence ... which means a higher salary ... hopefully enough to more than offset the exorbitant fees charged for certification ... need I say more?

By the way, dear reader, if you are an employer/interviewer reviewing job applicants' CVs prior to grilling them at interview, it is worth following the links above if you see qualifications listed that you do not recognise. Take a good look at the entry criteria and continuing education process (if any) to assess whether they actually mean anything useful or are merely wallpaper. Oh and don't believe everything you read. Internal auditing is a responsible job giving frequent privileged access to sensitive information. It's probably A Pretty Good Idea to validate applicants' personal integrity and ethics before letting them loose on a technical audit of the Accounts Payable, Salary or Missile Control systems ...

5.3.2 Other useful qualifications

- **Being experienced** - there really is no substitute for understanding the auditees' points of view and it certainly makes one think twice before recommending actions one would not be prepared to take oneself (a.k.a. "putting your money where your mouth is"). Experience of programming, operations, information security and project management are helpful, and hands-on management experience helps when discussing strategy with ~~the big nobs~~ senior management
- IT **technical qualifications**, especially those with significant information security content - BSc (Bachelor of Science) in computing, programming *etc*., MCSA (Microsoft Certified Systems Administrator), MCSE (Microsoft Certified Systems Engineer), SCSA (Sun Certified System Administrator) and similar
- **General IT (not audit/security specific) qualifications** - there are loads of these such as ACP & CCP: Associate Computing Professional and Certified Computing Professional qualifications from the Institute for Certification of Computing Professionals. Also PMP (Project Management Professional) from the Project Management Institute. In some countries, 'official' financial audits must be signed-off ("attested") by a qualified audit professional
- **General (non-IT) audit qualifications** – *e.g.* CIA (Certified Internal Auditor), MIIA (Member of the Institute of Internal Auditors), CFSA (Certified Financial Services Auditor), CGAP (Certified Government Auditing Professional), CCSA (Certification in Control Self Assessment)
- **General management qualifications** - *e.g*. MBA (Master of Business Administration), useful to understand how IT fits into the business/commercial world and to relate to business managers in their strange native tongue
- **Accountancy qualifications** *e.g.* CA, ACA, CPA, CIMA, thirteen-times table

- PhD or other **academic qualifications** - the actual topic doesn't matter too much so long as you learnt how to work hard without someone looking over your shoulder and how 2 rite proper perfik ... which reminds me ...
- **Language skills** - a strong command of the Queen's English (and/or your own native tongue) and the ability to write in a formal, objective yet persuasive style is essential. Certain auditees have been known to argue about the syntax and spelling of a report as a deliberate ploy to avoid discussing the actual issues at hand (outrageous - but true! Former auditors are the worst. Trust me, I've been there, done that). Auditors skilled in the cryptic symbolic/shorthand language beloved of teenagers everywhere shud not Xpect 2 rel8 to mgmt in TXT (or SMS)-speak.

5.4 What resources would you suggest for those studying towards CISA?

A CISA study book recommendation depends partly on your level of experience in IT audit.

- If you are starting from zero, you will have a tough time to absorb sufficient knowledge from any single book - even one-on-one teaching will be tough! Almost any decent textbooks on information security, auditing and/or IT auditing will help.
- If, on the other hand, you have several years' experience in the field, then you might get away with just the outline exam information provided by ISACA and maybe some sample questions (see below).

Most candidates, however, fall somewhere in between these extremes and to them I recommend the following resources:

- The ISACA and CCcure websites.
- The latest version of the CISA Review Manuel from ISACA. ~US$105 for members or US$135 for infidels, plus P&P. It gets updated when the exam is updated so I'd be a little wary of using an out-of-date hand-me-down copy. Available in Spanish, Italian, Japanese and English - separately.
- The latest version of the CISA Review Questions, Answers and Explanations CDROM also from ISACA. ~US$150 for members or US$180 for ordinary human beings, plus P&P. Some 725 example questions will give you a jolly good idea of what to expect on the Big Day. To complete the full effect, try staying up late desperately revising, getting up early and travelling across town to an unfamiliar building, then sitting in absolute silence for several long hours with nothing but a pencil for comfort while you rack your brains for the 'most correct' answers. For some unfathomable reason, ISACA's CISA questions and explanations are also available in printed form for even more money for those budding IT auditors who find themselves short of a CDROM drive and/or system.
- The CISA Prep Guide: Mastering the Certified Information Systems Auditor Exam by Kramer & Kramer (~US$44 from Amazon).
- "Standards and Guidelines for the Professional Practice of Internal Auditing" from the Institute of Internal Auditors, seemingly out of print but worth hunting the bookshelves especially if you have any greybeard auditors in your department (my own well-thumbed copy is now 12 years old!). It is only 60-odd pages but provides sound guidance on the purpose and ethics behind auditing.
- Browse the IIA's ITaudit bulletin board where you will find a range of questions and answers, some of which have been contributed by a certain self-opinionated gentleman called "Gary" ;-)

5.5 What are the commonest routes into computer auditing?

Some people become auditors as a definite career choice but most seem to become auditors almost by accident. It is policy in some organizations for managers earmarked for Board positions to have "a spell in audit" (not in the Harry Potter sense) in order to expose them to the whole breadth of the organization, with greater appreciation of governance, risk and control concepts as a supplementary benefit. Less senior people may also be seconded into audit to help out with specific audits and star auditees are often earmarked by audit managers as potential future recruits. The cynical view that audit is where failed accountants go to die is thankfully outdated (although, come to think of it, I have met one or two dinosaurs in my time in audit - no names but you know who you are [well maybe]).

Many computer auditors came directly from IT (developers, operations, IT security, technical architecture, business analysts, testers, IT managers *etc.*) but some have, shall we say, more unusual backgrounds such as:

- Accountancy *e.g.* traditional financial audit
- Other types of auditing *e.g.* quality audit, health and safety audit
- IT and/or management consultancy
- Military intelligence and other oxymoronic rôles
- IT sales, marketing or product support
- Legal or regulatory compliance work
- Risk management
- "Security" as in the Police, security guards, bodyguards and nightclub bouncers (well maybe - some ex-military people have this kind of background)
- Other technical management rôles and sometimes even non-technical managers (who rely heavily on the support of technologically-competent computer auditors in their team)
- University, college or school-leavers (who typically enter at junior/apprentice level called 'auditor' grade a.k.a. "gofer")

5.6 What competencies should I have to be a computer auditor?

Aside from the formal qualifications, of course, practical on-the-job experience is a major advantage, particularly for the softer skills such as interviewing techniques and establishing rapport especially with evasive or nervous auditees. Whilst the computer systems can provide a lot of information, very few computer audits can be completed successfully without actually talking to real people such as end-users, managers and operations staff in the flesh in order to gather more facts and opinions. This becomes increasingly important in the latter stages of an audit since audit recommendations are unlikely to be adopted unless management understands and supports them, so you will need to make a case. Gaining their commitment to action the recommendations involves persuading and negotiating, along with a degree of tenacity and resilience, since computer auditing is practically worthless unless it achieves positive change within the organization. It takes strength of character to stand up for what's right ("The Truth") even at risk of upsetting powerful figures within the management hierarchy ("The Establishment") because the independence of audit more-or-less inevitably results in conflict situations at a personal as well as professional level.

Perhaps the most important benefit of audit experience is a thorough understanding of risk and control concepts. Auditors specialise in advising management on the need for controls to address the risks that they observe and/or surmise. Computer auditors need to:

- Identify actual and potential risks to the business associated with computer systems, networks, IT installations, applications, development projects *etc.*;
- Observe and review technical, physical and procedural controls in operation;
- Assess whether the level of risk is reasonable or whether control improvements are required;
- Justify and recommend more-or-less specific control improvements, persuading management to commit to resourcing and making the changes within a sensible timeframe.

Computer auditors' core expertise is naturally focused on ICT but their expertise in risk and control concepts has broader application. Reviewing and discussing ICT risks and controls in relation to the organisational environment as a whole is a powerful technique for influencing management. After all, in most organisations, ICT is a means to an end not an end in itself. This therefore implies a further competence at bridging between the worlds of technology and business.

A reasonable understanding of, and respect for, change management concepts and business management in general, are likely to make the computer auditor more effective overall. A good example is the notion that there is really no such thing as "an IT project": computer systems are developed to change the organisation in some way, normally to facilitate new, more efficient business processes. Reviewing major development projects as if they are primarily major organisational changes is an extremely powerful technique.

Cognitive abilities, coupled with the dedication for systematic, insightful analysis (a posh phrase for "brains") and presentational skills such as formal writing, are very important for success in computer audit or indeed in any branch of auditing. Proactivity and diligence (a.k.a. "get up and go") are useful characteristics, along with both an eye for detail and the ability to 'see the bigger picture'. Computer auditors who focus purely on technology and put too much emphasis on specific technical controls risk alienating senior management who have a business to run. Therefore, they need to be able to put their findings in context and work with management to find pragmatic solutions to business problems stemming from the technical weaknesses.

An incessant thirst for knowledge helps the computer auditor get through the day. The same is true of other auditors but computer auditors have a significant advantage: they can browse the Internet or intranet for hours on end with a more legitimate excuse. Constant learning and updating of skills is the real aim, of course, and is especially important in the case of ICT. It really helps to be a nerd – someone who loves technology for technology's sake and is not afraid to stay up late grappling with the intricacies of TCP/IP.

Computer auditors, like all auditors, need to be well aware of 'corporate politics' to deal efficiently with the strong personalities characteristic of most senior managers. At times, they certainly need thick skins! Pure aggression, though, is not the answer. Good auditors learn to manipulate the organization, not just the individual.

You have enemies? Good.

That means you've stood up for something, some time in your life.

Sir Winston Churchill

If this all sounds daunting, don't worry. Audit presents opportunities to learn and improve the skills and competencies listed here, if you are prepared to put in the effort. It is also a wonderful way to find out about the organization and the senior managers and others who run the show, often behind-the-scenes.

5.7 Institute of Internal Auditors' categories of IT knowledge for internal auditors

The IIA's International Advanced Technology Committee has identified the following three categories of IT knowledge for internal auditors.

Category 1 – All auditors from new recruits up through the chief audit executive

"Basic" IT knowledge encompasses understanding concepts such as the differences in software as used in applications, operating systems and systems software, and networks. It includes understanding basic IT security and control components such as perimeter defenses, intrusion protection, authentication, and application system controls. Basic knowledge includes understanding of how business controls and assurance objectives can be impacted by vulnerabilities in business operations and the related and supporting systems, networks, and data components.

Category 2 – Audit Supervisors

Audit supervisors must have basic knowledge, but must also understand IT issues and elements sufficiently to address them in audit planning, testing, analysis, reporting, follow-up, and the assignment of auditor skills to the elements of audit projects. Essentially, the audit supervisor must:

- Understand the threats and vulnerabilities associated with automated business processes;
- Understand business controls and risk mitigation that can, and should, be provided by IT;
- Plan and supervise audit tasks to address IT-related vulnerabilities and controls, as well as the effectiveness of IT in providing controls for business applications and environments where it is used;
- Ensure the audit team has sufficient competence, including IT proficiency, for audits;
- Ensure the effective use of IT tools in audit assessments and testing;
- Approve plans and techniques for testing of controls and information;
- Assess audit test results for evidence of IT vulnerabilities or control weaknesses;
- Analyze symptoms detected, and relate them to causes that may have their sources in business or IT: planning, execution, operations, change management, intrusion protection, authentication, or other risk areas;
- Provide audit recommendations based on business assurance objectives appropriate to the sources of problems noted rather than simply reporting on problems or errors detected.

Category 3 – Technical IT Audit Specialists

IT auditors may or may not function at the supervisory category, but must understand the components and underlying technologies supporting business components, and be familiar with the threats and vulnerabilities associated with the technologies. Technical IT auditors may also specialize in certain areas of technology.

5.8 What are the personality traits and abilities of good computer auditors?

Good computer auditors are like other good auditors, only better. Here are some of their characteristics:

- **Inquisitiveness** - more than just idle curiosity, this describes the urge to find out how things (computer systems and subsystems, work processes, organizational units, people) work and why they don't work better. Asking questions, both literally and figuratively, is what fieldwork or audit testing is all about.
- **Independence of thought** - formal independence of the audit function from line/executive management is only part of this aspect. Auditors need to 'think outside the box' more than most. It's all too easy to get drawn into the "that's how we've always done it" thought patterns constraining most auditees. Trustworthy computer hackers (if that's not an oxymoron) would probably make good computer auditors. Auditors might be called professional cynics, trained and encouraged to challenge the *status quo* (and other aging rock groups).
- **Assertiveness** - assertiveness (neither aggression nor arrogance) can be a subtle blend of charm, wit and forceful personality, or the more direct carrot-and-stick approach ("Do you think your manager would be surprised to know that you promised me this information six weeks ago?"). At times, auditors also need a degree of humility: auditees often know more about the realities of the detailed situation under review than the auditor - they are the real experts.
- **Analyticality** (??) - making sense of all that information you've gathered is quite a job. When you find yourself surrounded by an enormous pile of computer printouts, interview notes, findings sheets, checklists and half-eaten pizzas, and with the audit reporting deadline approaching, it's sometimes worth taking a break or asking for help. Personally, I recognize being in this state when I feel like I have had a headfull of spaghetti for a few days, until the time comes to strain the information out and rinse it off ready for consumption. The next step - writing up - comes as a great relief, a bit like serving a big meal (OK OK enough of the analogy already).
- **Report writing skills** - writing formal audit reports well is a skill that takes many years of trial-and-error and 'constructive criticism' from audit management and more-or-less direct feedback from auditees. Reports have to present bad news in such a fashion that auditees see little alternative but to making the improvements so helpfully suggested under 'audit recommendations'. [If you are trying to bend or avoid the truth, be careful how you put things to an experienced auditor: they are probably more practised wordsmiths than you.]
- **Presentational skills** - presenting audit findings and recommendations to senior management can be daunting, career-threatening or career-enhancing, depending on the circumstances, the auditor's skills and the eventual outcome. Whatever it takes, there is little point being an auditor unless you are prepared to (figuratively and/or literally) stand up and say what needs to be said. Achieving positive changes in the organization is the real prize *sine qua non*. It takes special skills to explain the ins-and-outs of a typical firewall ruleset to your average non-technical manager.

By the way, presenting is of course related but different to report-writing: reports can and usually are written and rewritten incessantly, crafted into literary masterpieces. An auditor may only have one short opportunity to stand up and present findings to the Board in the full glare of the corporate spotlight. This is where the auditors' most powerful secret weapon comes into its own. Auditors speak from knowledge of the key facts. Facts are an auditor's indisputable ally. Treat facts with respect, like your best friends, and they will be there when you need them most.

5.9 What experience is required?

That depends on the seniority of the post and the level of support available, as well as the organization's Human Relations policies. Most organizations that have a dedicated computer audit function within Internal Audit have an experienced Computer Audit Manager who has, typically, at least four or five years experience in computer audit. He/she may be the only person in small organizations and is often expected to perform other work outside of the normal remit of computer audit. In large organizations, he/she usually manages a small team of perhaps five to ten individuals, possibly supplemented with other resources (consultants, contractors, secondees from the business and other auditors).

Larger teams such as this usually include inexperienced trainees and part-experienced staff (juniors) but computer audit is not really an ideal 'entry level' profession. It may be hot with a high profile in the press these days, and may look more interesting than the drudgery of being a sysadmin or application programmer for a large and faceless corporation, but the reality is more than that. Technology knowledge alone is insufficient. You will need more than a Batchelors or Masters degree in IT or Information Security or a CISA certificate to make a successful career of it. It means communicating effectively with corporate politicians and commercial realities. Good IT auditors understand topics as diverse as management accounting, motivational psychology, social anthropology, public speaking, organisational design and business law. They combine empathy with assertiveness. Like the best generals, they have been in the trenches for a few years. They are dry behind the ears.

6 I'm about to be audited: what will happen?

~~The end of the world is nigh~~.

6.1 Should I fear being interviewed by a computer auditor?

Of course not! Trust me, the auditors are here to help! It is entirely natural to be a little nervous - not so much blind panic as 'exam nerves', especially the first time you are audited. Auditors are trained to take account of, and work with, nervous auditees. They should explain the audit process and confirm their scope with you, and give you plenty of opportunities to ask your own questions or make relevant comments to amplify your responses to their questions. Auditors are really just professionals trying to do a good job. They may ask lots of questions and can occasionally appear somewhat dubious about your responses, but they are not 'out to get you'. Most of the time they are simply trying to gather relevant information and understand complex and ill-defined control systems.

6.2 How much information should I give a computer auditor?

Experienced auditors become adept at filtering large quantities of information and rapidly identifying key facts or concerns. It is difficult for auditees to swamp such an auditor with relevant information, although dumping irrelevant or badly structured information on them just before or after the audit report is due tends to make them somewhat grumpy.

Conversely, auditees who are too terse can also create a problem. It is normally better to offer additional information which you feel may be relevant, than to wait to be asked for it specifically. Auditees who consistently fail to open-up, typically only answering audit questions with highly specific answers, may simply be forgetful or nervous, or may in fact be trying to conceal something important, perhaps concealing a fraud, theft or accident. Similarly, auditors who only ask direct or closed questions (encouraging monosyllabic "Yes" or "No" answers) may themselves limit the breadth of information to the extent that they may miss certain important and relevant facts. In this sense, auditing is a true bidirectional communications process.

Only a small fraction of the information gathered during an audit will ever be formally reported. Computer auditors, in particular, often have access to computerised data analysis tools to help them examine large databases, spreadsheets or other data files provided by auditees. They can select records of interest for further study using a variety of statistical methods ranging from random or stratified sampling (*e.g.* "Identify transactions in the top 5% by value") to highly sophisticated and complex data-correlation techniques (*e.g.* "Find any sales records where the delivery address does not match the cardholder's address" or "What has my manager been up to lately?").

6.3 How can a computer auditor who does not work in my department and has limited knowledge of what I do, possibly criticise our systems and procedures? What on Earth does he/she know?! What gives him/her the nerve to come in here, asking so many ridiculous questions …

Good point! All auditors have a thirst for reliable evidence and the ability to evaluate business situations for control weaknesses. This typically requires having sufficient background knowledge of the auditees' area to ask appropriate questions and understand the answers, coupled with careful observation skills and, at times, the humility to seek help. Interviewing, analytical and reporting skills add to the auditor's armoury, coupled with seriously heavy senior management support and the sheer nerve to ask dumb questions or challenge ridiculous-sounding answers. Blind luck helps sometimes too - but then, the harder I work, the luckier I get.

Computer auditors' favourite phrases	Computer auditees' favourite phrases
"I'm from audit, and I'm here to help"	"It's in the post"
"Trust me, I'm an auditor"	"It's never done that before"
"Your manager said I should speak to you about this"	"Look, I'll show you just how confident I am ... *oh-oh*."
"Show me"	"But that's the way we've always done it"
"Tell me about …"	"I just do what I'm told"
"Call me a cynic, but …"	"Don't be ridiculous, that'll never happen here"
"Go ahead – make my day"	"My manager hasn't a clue what I do"
"Here, hold this wire a moment"	"I'll send it round right away, honest"
"This will only take a second"	"Exactly how many is 'many' control failures?"
"Is there anything else you'd like to tell me?"	"It was working perfectly just a moment ago"
"Is there anything else you feel you want to get off your chest?"	"Which planet do you come from?"
"Can I have a read-only userID to take a little look at your system, please?"	"There's no need to document our strategies/procedures: everyone knows what they are"
"Who else should I speak to about this?"	"Source code comments are for wimps. Real programmers write self-documenting code."
"I don't suppose it's meant to do that"	"I'll email it to you"
"When would you say you'd have this resolved?"	"That is out of scope"
"I need your mobile phone number for the audit file"	"When I said 'next month', I was thinking about the month after"
"Just one more thing ..."	"NO! DON'T PRESS THAT BUTTO..."
"Get a life"	"Mummy!"
"Beam me up Mr. Scott."	
"Cheers"	
"ping"	

7 Setting up (IT) audit

7.1 I've just been invited to establish an Internal Audit function: where do I start?

This is the Institute of Internal Auditors' outline of how to set up an audit department:

- Review the new definition of internal auditing and the International Standards for the Professional Practice of Internal Auditing to become familiar with what is required. This will help you in any discussions with management and the audit committee so you will know what to ask for.
- Interview senior management and board of directors/audit committee chairmen to build rapport, to ensure those at the top have a clear picture of the internal audit function, and to clarify expectations of all. Use this opportunity to quickly learn and address what management and the board view as the greatest risks to the organization, while keeping in mind issues, problems, and opportunities that have already been identified. Develop a system for cataloging such information, including date and name of person interviewed for quick reference in the future. There are many considerations that should be evaluated in determining the optimal structure and source for internal auditing resources. Those responsible for making such determinations should evaluate the additional guidance and considerations outlined in the IIA's position paper "Resourcing Alternatives in the Internal Audit Function".
- Obtain and review the audit committee charter. Of course, no sample charter encompasses all activities that might be appropriate to a particular audit committee, nor will all activities identified in a sample charter be relevant to every committee. Accordingly, this charter must be tailored to each committee's needs and governing rules.
- Understand "benchmarking" needs, *i.e.* industry, specialty groups, organizations with same staff size, *etc*. Ask senior management who they consider to be leaders and laggards in your organization's market niche. Check out IIA's GAIN services and review past GAIN surveys.
- Obtain and review your organization's written policies and procedures, especially those pertaining to governance or management's responsibility to control the organization.
- Discuss with external auditors open and closed internal control issues, which they may have identified during their reviews.
- Start to develop your "audit universe," the list of all auditable entities or the scope of your department.
- Map the major processes/operations within the organization. Meet with operations managers, including those in information technology, in order to understand their risks and concerns.
- Develop a risk assessment for your organization. This should be a macro-level assessment, which includes both external and internal risk factors.
- Develop a charter for the department. Ensure that both senior management and the audit committee review and approve the charter. Examples of audit charters can be found within the IIA Professional Practices Framework or the Internal Auditing Manual Shell on CD. Additional samples are provided below.
- Build your budget, including personnel and travel costs.

- Based on your risk assessment, develop an audit plan. The amount of the plan that can be accomplished in the allotted time period (usually a year) will depend on the risks identified and the internal audit resources and staff. You should always leave time in your audit plan for management requests and contingency (at least 10 percent, perhaps rather more at the start).
- Hire your staff and develop a plan for staff training. Ensure your staff covers the range of expertise needed based on your risk assessment. You may also consider outsourcing portions of your audit plan to outside service providers or using professionals internal to the organization. The IIA Internal Auditing Manual Shell on CD contains descriptions for all professional staff positions.
- Ensure that senior management notifies other departments of your existence and calls for complete cooperation. (The IIA has complimentary brochures, such as "All in a Days Work," "Adding Value Across the Board", and "Guidance for the Profession".) Become familiar with The IIAs Web site and use the search feature on its home page to help you identify valuable resources.
- Work with management to establish best-practice reporting relationships, to ensure internal audit is promoted throughout the organization, and to develop a methodology for following up on audit recommendations and measuring performance.
- Establish a quality assurance program.

The IIA is undoubtedly a valuable source of guidance, advice and assistance on internal audit matters generally, but is not the sole source. ISACA's COBIT method, ISO 20000 (ITIL) and ISO 17799 are well respected standards for example that can usefully be incorporated into the IT audit function's working practices and can influence the way the function plans its work:

COBIT is a rational, structured way to analyze the organization's IT processes from a governance point of view. The latest version, v4, is more usable than all previous versions, thankfully.

ISO 20000 (ITIL) can help IT auditors appreciate the set of idealized or best practice IT operational and management processes characteristic of a well-run IT department.

Standards such as ISO 17799 can help scope the bulk of the technology audit universe, namely the organization's information security management system.

8 Special bonus section

... for the humour impaired.

Computer auditing is a very very boring career frequented by nerds and geeks with extreme personality disorders and BO. It is undervalued and not in the least bit attractive to those of the opposite sex. Only high-school dropouts and those who cannot make it as teachers or accountants become computer auditors.

My advice is very clear. Do not under any circumstances consider becoming a computer auditor. Accountancy the way to go, my son. Learn those tax tables like your life depends on it!

9 The end

9.1 I've finished this FAQ. What other resources are there to help me?

The web is an excellent source of information on computer audit, especially on the technical aspects (*e.g.* information security vulnerabilities). Websites such as www.theiia.org, www.ISACA.org, www.ISSA.org and www.ISC2.org have information relating to their professional membership and qualifications as well as broader topics of interest to practising computer auditors as well as those who have finished practising and started doing.

To swap notes with over 4,000 peers and pose questions not answered in this FAQ, check out the IIA's ITaudit bulletin board (access requires free registration). More IIA links: Professional Practices Framework, Additional Resources, Positions, responses & other IIA resources by topic and the IIA Research Foundation.

"Auditors Sharing Audit Programs" (ASAP) is an excellent collaborative project managed by Jim Kaplan to collect and share audit checklists - often a useful starting point when scoping and preparing for a new audit, but don't expect to just crib one and go straight to work. Engage brain, examine risks, refine checklist – the thought process is a valuable part of the pre-audit phase. There are many portals relating to information security and/or computer audit, although most operate on a commercial basis and are not necessarily unbiased. You may be better-off Googling computer audit or related terms.

For books on computer auditing - try searching Amazon but don't necessarily expect to find the perfect book at your first attempt. The training manuals associated with the qualifications noted above (*e.g.* "CISSP Certification All-In-One Exam Guide" or the "CISM Prep Guide") may be useful, and both ISACA and the IIA offer useful books and other materials. Otherwise refer to the ever increasing body of literature on information security, management, governance, risk, accounting and related topics. Some newer books on auditing recognise and incorporate computer audit as a specialist topic but most seem to concentrate on more traditional accounting-related subjects. Perhaps I should write something: what do you think?

Clement Dupuis' website CCcure is a wonderful resource for certifiable students seeking information security certification, and for that matter those of us who are already certified.

If you employ IT audit or indeed other consultants, "Con tricks - the world of management consultancy and how to make it work for you" is required reading, preferably before you send out your ITT or sign the contract. Forewarned is four armed, as we say.

[NB: we earn a little commission from Amazon if you buy books through the links above. This helps offset our costs for writing, maintaining and hosting this FAQ. If you begrudge us this meager pittance, please leave now. If you want to audit the income, bring a magnifying glass.]

9.2 Feedback

Please let us know what you think of this FAQ (good and bad!). We especially welcome additional relevant questions or topics that you feel should be included, and of course any corrections or extensions to the existing answers, including links to other web resources.

9.3 Who wrote this?

This FAQ was conceived and written by me, Gary Hinson of IsecT Ltd. I maintain and update it from time to time to incorporate feedback suggestions from readers and my own sporadic brainwaves. I am a certified (should that read certifiable?) IT auditor who has experienced or tried most of the things written in the FAQ in the course of my short 17-year career, mostly as an Infernal Auditor. I don't (often) bayonet the wounded. (But I like ((parentheses))). Please forward any complaints, corrections, improvement suggestions, feedback or other comments to me personally by email (info@isect.com). I especially welcome additional FAQ topics (ideally, but not necessarily, with model answers!), and links to other related information sources on the WWW. Or folding money. Gold bullion. Books from my Amazon wishlist. Whatever. If you think I'm desperately wrong about something, tell me. I can take it. I'm an (ex-)auditor with specially thickened skin.

IsecT Ltd. is my consultancy firm specialising in IT governance and related topics, including of course computer auditing and information security awareness. Check out the IsecT website to find out how we might help you but you might like to read the FAQ section on choosing an audit consultant first – we are evidently not the *only* supplier in this market.

9.4 Copyright

9.5 Document change log (I can't help it - it's in my genes. I used to be an IT auditor and before that a geneticist ☺)

October 2006: corrected the spelling of Clement Dupuis' surname. Sorry Clement. Updated the PDF version too.

September 2006: inserted advice on the use of strong access controls to protect often highly sensitive audit evidence.

August 2006: added yet more qualifications/certifications namely PCIP, CEH (and similar) and Symantec's certs. Thinking about offering the CFAQA (Certified FAQ Author) qualification to fellow FAQers. Added a bunch suggestions on the value auditors can bring to development projects, and a link to WizRule CAAT, shamelessly lifted from a discussion thread on the IIA's IT Audit bulletin board. Inserted two missing words (thanks to Winnie, and no thanks to the dumb spellchecker on this PC). Added advice on CISA study guides (good luck Necarti!).

July 2006: added a link to dmeissler.com's list of infosec and audit certifications. Added a link to the CCO qualification from BECCA.

June 2006: the phrase 'All rights reserved' is no longer necessary on our copyright notification, I believe. Let's hope the magic © incantation still works anyway. Thoroughly updated the PDF version. Added a mind map contents index thing (hyperlinked to the text in the online version of this FAQ).

April 2006: added a classic quote from an auditee complaining about 'frequent use of the word "significant"' in an evidently rather uncomplimentary audit report about them.

March 2006: fixed broken links to the BCS. Referred to American English. Updated the PDF version.

December 2005: inserted a rant about the PCAOB, having been prompted to mention them in the FAQ by one of our valued FAQ readers, and updated the Andersen and Enron links (thanks Darian). If anyone disagrees with the rant, by all means tell me.

November 2005: added the extra special bonus section [for the humour impaired] and a few more dodgy jokes.

September 2005: referred to "C&A" (certification and accreditation, apparently). Put some more effort into the setting up an (IT) audit function bit. Added links to the Universities of Nebraska, Texas, Norwich and Colorado Tech who offer IT audit and information security courses (others, anyone?). Added CCE qualification to the list.

August 2005: added advice on setting up an (IT) audit function based on IIA advice sent to the IT Governance mailing list. There's plenty more to say in that section, when I find the time to write it ... Beefed-up the CISA, CISM, SSCP and CISSP write-ups

July 2005: wrote a section on auditing against Best Practice, whatever that means

May 2005: updated the ACL link (thanks Jacqueline).

April 2005: added Q&A about what questions to ask as an auditor (thanks for asking, Maurie). Correctly named the IIA (oops). Added the CCcure recommendation (go Clement go!).

March 2005: made a number of minor amendments. A smattering. A tweak. An indecision maybe. What is the collective noun for minor amendments? Included PMP qualification. Noted that GIAC no longer has a practical bit (shame).

January 2005: updated the PDF a fair bit based on a version issued to IsecT customers as part of the NoticeBored security awareness service. Added a quotation from Bill Royds (thanks Bill!).

October 2004: added a paragraph on careers *vs*. jobs. PDF version updated

September 2004: added yet more qualifications (this is getting silly) plus a snippet of advice for interviewers. SMS/TXT gets a mention. .

August 2004: increased the font size for those with dimensionally-challenged pixels(thanks Anton) and added more about experience. Wrote about compliance auditing. Added CFE and ISSPCS qualifications. Boy Scouts' badge for knots coming soon.

June 2004: expanded on the report-writing sub-process (warning: I'm in an especially cynical frame of mind today. The medication must be wearing off.). Also added a section on choosing audit consultants, a link to the IIA ITaudit bulletin board (thanks for the suggestion Len), and a brief word on getting qualified to earn more money. PDF updated at last.

May 2004: added CAAT section, yet more infosec certifications and the IIA's categories of IT knowledge to this webpage ... although not yet to the PDF. Too busy. Sorry.

Mar 2004: more types of audit added; converted the web page back into a Word document and then to an Acrobat PDF for easier printing. Added the 'rate this paper' link below.

Feb 2004: removed the obvious acronym for Certificate in Information Security Management Principles which is evidently trademarked by someone else; referenced University of Houston.

Jan 2004: linked to CISA article in NetworkMagazineIndia. Expanded on the traits and competencies of auditors.

Dec 2003: added notes about retention of audit evidence; deleted reference to anoraks and things going pear-shaped" as a concession to non-Brits; added feedback section.

Nov 2003: added SSCP qualification.

Sept 2003: narrowed the web version to fit 800x600 displays and printers. Added still more qualifications

August 2003: More minor wording changes. Added CISM and NoticeBored links and contents

June 2003: minor style amendments to match new-look IsecT website - do you like it?

March 2003: various minor amendments

December 2002: first published at www.IsecT.com

If you enjoyed this FAQ, please rate it at the CCcure.org website and put a link to it on your website to help spread the good word about computer auditing. If you hated it, found errors or omissions or know of a better way to put/do something (which is entirely possible), tell me and I'll ~~send the boys round~~ try to do something positive about it.

If you disagree with what's written here, have a better way of putting it, or feel there is something else that needs to be said, please let me know. I am grateful for additional contributions of knowledge, and more questions. Telling me the humour is not appropriate will just make me laugh. Get a life! Auditing is for adults.

I am happy to fund this FAQ through my company in order to give a little back to the Internet community that gives me so much but if you insist on contributing, please consider buying me a book on my Amazon wishlist. As a last resort, please express your gratitude by telling someone else about the FAQ, giving your partner a gratuitous hug, grinning broadly at a complete stranger ... or not stepping on an ant.

Either way, whether you enjoyed it or not, I would love to hear from you.

Thank you,

Gary. gary@isect.com

PS If anyone Out There would care to translate this document into another language, please contact me directly (gary@isect.com). My schoolboy French would make grown Parisians laugh out loud and my Latin skills have a rather limited audience these days. I will gladly sanction good quality "foreign" language translations *provided* that they are released under essentially the same terms as this version *i.e.* PDFs completely free of charge for the public good. Commercial translators please by all means contact me but don't expect to get paid. This project is a labour of love and certainly not a money-spinner.

Gary Hinson is the Chief Executive Officer of IsecT Ltd., an independent IT governance consultancy focused on information security and computer audit. Gary's career stretches back to the mid-1980's and along the way he has collected CISSP, CISM, CISA and MBA qualifications supplementing his PhD in genetics (!).

NoticeBored is IsecT Ltd's innovative security awareness product. NoticeBored delivers a fresh module of high quality security awareness materials on a different information security topic every month. The materials comprise presentations, briefings, newsletters, posters, mind-maps, case studies, policies, white papers, screensavers, awareness surveys, crossword puzzles *etc*. in industry-standard editable file formats (*e.g*. Rich Text Format, PowerPoint, Visio & JPG). Please visit www.NoticeBored.com for more information.