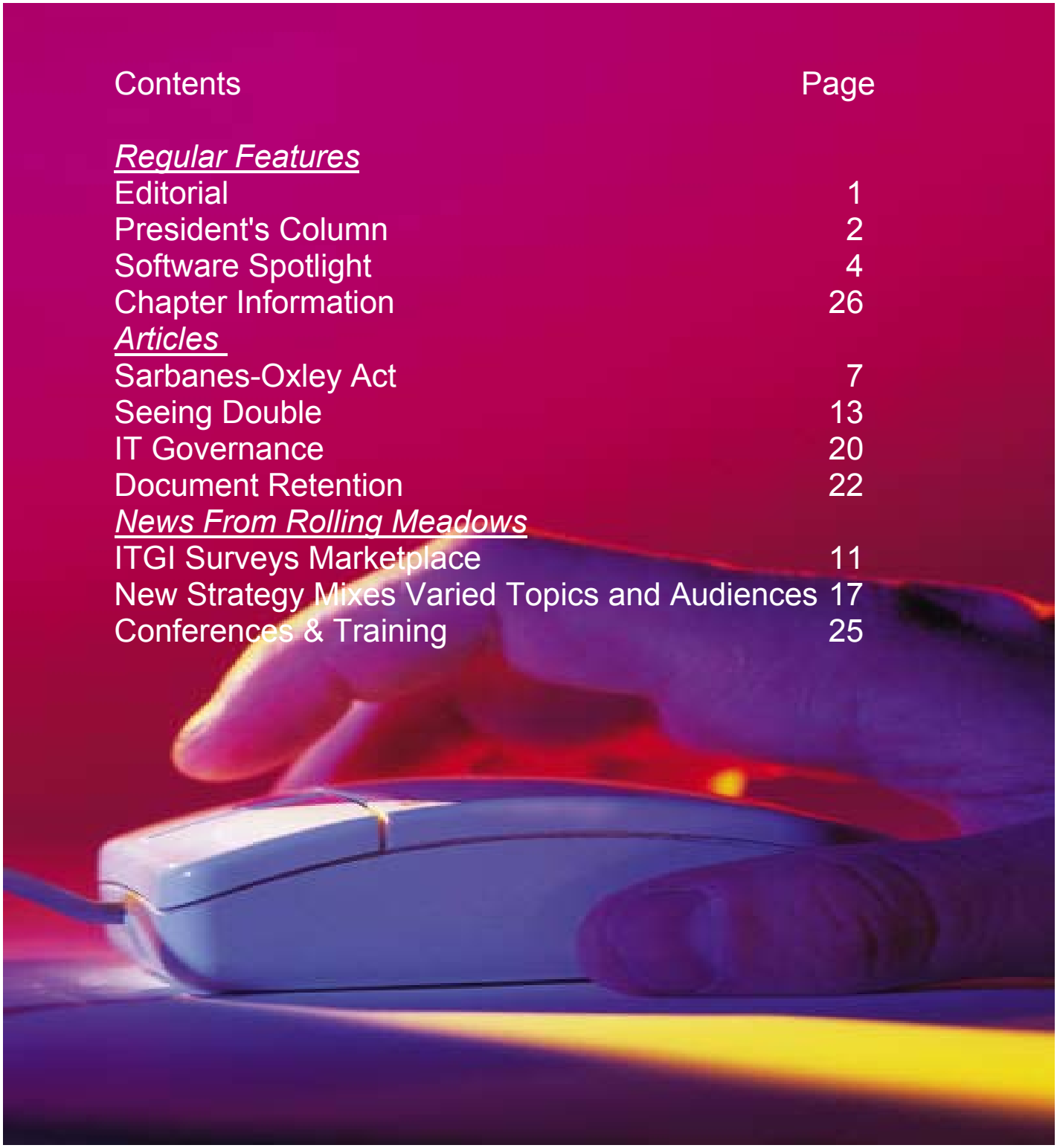
ISACA London Chapter

DATAWATCH

Summer 2004



Contents Page

Editorial Team: David Thirlwall, Allan Boardman, John Hunter

DATAWATCH is published by the ISACA London Chapter. Membership of the Chapter entitles one to receive an annual subscription to DATAWATCH.

Editorial

David Thirlwall

After a long absence, Datawatch is back. Our sincere apologies for the prolonged silence in recent months. We mentioned in the last issue that we were looking for assistance in the production of the magazine, and volunteers can be hard to find. Hopefully these difficulties are now behind us. We have a new editor, and a team determined to deliver.

So here is the first issue of 2004 – and the first issue ever to be delivered electronically. The decision has been taken to publish the magazine only in electronic format from now on. Publishing in this way saves significant cost, and this in turn means that the London Chapter dues can be reduced. Also, the requirement to fill a pre-defined number of pages before an issue can go to the printers becomes a thing of the past.

In this edition Kevin Handscombe writes about the impact of Sarbanes-Oxley. Notwithstanding that this is US domestic legislation, there is no doubt that SOX has achieved worldwide reach in a very short time. Linked to SOX, Thomas Turner reports his research into the take-up of COBIT as a tool for IT Governance. Also, we include a structured approach to testing for duplicated transactions within Accounts Payable. From my own personal observations I concur that duplications remain widespread, and that no amount of sophisticated ERP software can beat this problem. You don't need new systems to start applying tests here, just new invoices - good luck.

Datawatch is alive and kicking, and we intend that it should stay that way. But of course this is only possible if there is material to publish. If you have something that you want to share with colleagues then please get in touch with the editorial team. Remember that all articles published do count for Continuing Professional Education credits.

As well as content, we would like to know what you think about the new format. We cannot pretend that everything will be perfect on the first attempt. So if you would like to see changes to the format, let us know. Electronic publishing is very flexible.

Enjoy the magazine. On behalf of the team,

Dave

President's Column

Allan Boardman

Welcome to the new look Datawatch Online.

How often do new ideas or technologies come along that shape and dominate an industry and truly change the way things are done?

I recently attended the Lovelace lecture, a British Computer Society annual event in honour of Augusta Ada Byron, the Countess of Lovelace and the person who programmed the Babbage Engine. Dr John Warnock, the mastermind and founder of Adobe and the Portable Document Format (PDF), gave this year's lecture. It was a very entertaining and inspiring talk and a fascinating insight into the early beginnings of a technology that today dominates so much of the electronic publishing industry and is used in so many different ways. Acrobat Reader has had upwards of 500 million downloads. Now that's what I call a dominating technology.

Herewith another technology that may change the way we do things. Since Gmail was announced on 1st April 2004, (and turned out not to be an April fool's joke), I have been following with interest the privacy debates linked to introduction of the service. For those not yet familiar with Gmail, it is Google's experiment with a new kind of webmail, built on the idea that you should never have to delete mail and you should always be able to find the message you want. Quickly!

The key features of Gmail are:

- Search, don't sort - Use Google search to find the exact message you want, no matter when it was sent or received;
- Don't throw anything away - 1000 megabytes of free storage so you'll never need to delete another message;
- Keep it all in context - Each message is grouped with all its replies and displayed as a conversation;
- No pop-up ads. No untargeted banners - You see only relevant text ads and links to related web pages of interest.

It is the "relevant text ads" feature that has privacy advocates up in arms, calling for the service to be suspended until the privacy issues have been addressed. The main concerns revolve around Google's plans to scan the text of all incoming messages for the purposes of ad placement, the unlimited period for data retention that Google's current policies allow, and the potential for unintended secondary uses of the information Gmail will collect and store.

Like Google search results pages, Gmail includes relevant text ads on the right side of the browser page based on keywords included in incoming ads. So for example if you received an email from a friend informing you that they had recently been to a Madonna concert, your browser displaying the email (Gmail) may include an ad for a ticket booking agency.

Google has countered criticism of Gmail by highlighting that a computer, not a human, will scan the content of the e-mail, thereby making the system less invasive. However, critics argue that a computer system, with its greater storage, memory, and associative ability than a human's, could be just as invasive as a human listening to the communications, if not more so.

Is this all a storm in a teacup? Maybe. The counter view is that there are already hundreds of millions of users of hosted mail services at AOL, Hotmail, MSN, and Yahoo and the like. These services routinely scan all mail for viruses and spam. In addition, the amount of private data collected and held by credit agencies, retailers and direct marketers dwarfs the personal information that may be gleaned by email.

Perhaps the wider issue is not that Gmail scans your email, or that it might take a while for duplicates of your mails to be deleted off the system. It's that with a gigabyte of storage, user habits with regard to email change entirely, and we

start to keep our entire computing life online, moving massive amounts of personal and private communications and files into cyberspace. The key questions then are who owns the data and how is it controlled and secured?

Email has become the system of choice for exchanging information and has truly become a “killer application”, but it still falls far short of being effective at storing and retrieving information. As the world becomes more connected, with rich, complex data stores, and email simply a tool for passing across messages and notification, and documents and files, technologies such as Gmail may be showing us the way to the future.

I leave you with a response from Google addressed to the various privacy organisations that have requested that Gmail should be suspended.

> *"Let's be clear: there are issues with email privacy, and these issues are common to all email providers. The main issue is that the contents of your messages are stored on mailservers for some period of time; there is always a danger that these messages can be obtained and used for purposes that may harm you. There exists a real opportunity for misuse of your information by governments, as well as by your email provider. Careful consideration of the relevant issues, close scrutiny of email providers' practices and policies, and suitable vigilance and enforcement of appropriate legislation are the best defences against misuse of your information. The only alternative is to avoid new technology altogether, and forego the benefits it provides."*

Hope you enjoy the rest of Datawatch Online

Best wishes

Allan

Software Spotlight

Spam Cop & Spam Inspector

John Mitchell

The Problem

The spammers are closing in on me and spam currently accounts for about 10% of the email I receive and this is increasing monthly. Those of you who attend the London Chapter meeting will know my views on spammers and my belief in not being passive on this matter. Some ISPs now provide spam protection as part of their service, which usually involves them quarantining spam in a special folder on the server which means that it never gets as far as your mail in-box. Those of you who do not have this service are forced to fight back at the in-box level and this is where *Spam Inspector* and *Spam Cop* come in.

How Do *Spam Inspector* and *Spam Cop* Solve the Problem?

These two products tackle the Spam problem in basically the same way, but *Spam Cop* is essential passive while *Spam Inspector* is what I describe as partially active. I will deal with *Spam Cop* first as some of its elements also exist in *Spam Inspector*.

Spam Cop

Spam Cop is basically a reporting engine. Once registered with *Spam Cop* you forward any Spam that you receive to a *Spam Cop* email address where the mail headers are automatically analysed to determine the real source of the mail. Forged headers are detected (and ignored) and *Spam Cop* checks the route to identify the various servers and ISPs that the spammer used. It then generates an abuse report for the ISPs which it emails back to you for checking and sending to the identified ISPs. All you need to do is click the 'Report' button to send the abuse report(s) on their way. *Spam Cop* does not prevent you receiving Spam, but it does provide a fairly easy way of reporting it and leaves you with a 'feel good' factors as you initiate the reporting engine. The basic service is free, although you are exhorted to make a donation if you like it.

Spam Inspector

Spam Inspector is a partially active anti-spam mechanism which integrates into your mail client to inspect every message that comes into your inbox. It then allows you to decide what action you want to take with the spam, ranging from simple quarantine in a specified folder to sending reports to the relevant ISPs and any combination of each. The reason why I describe it as only partially active is that the spam has already arrived and we are now fighting a rearguard action.

Set-up is easy and *Spam Inspector* updates its own spam database automatically, but it also has a learning mode which enables you to specify what you consider to be spam, or not spam as your individual case may be. *Spam Inspector* then learns heuristically and updates its rule base accordingly. However, false positives and negatives will always be around, but in my case only about 5% of spam was not correctly identified.

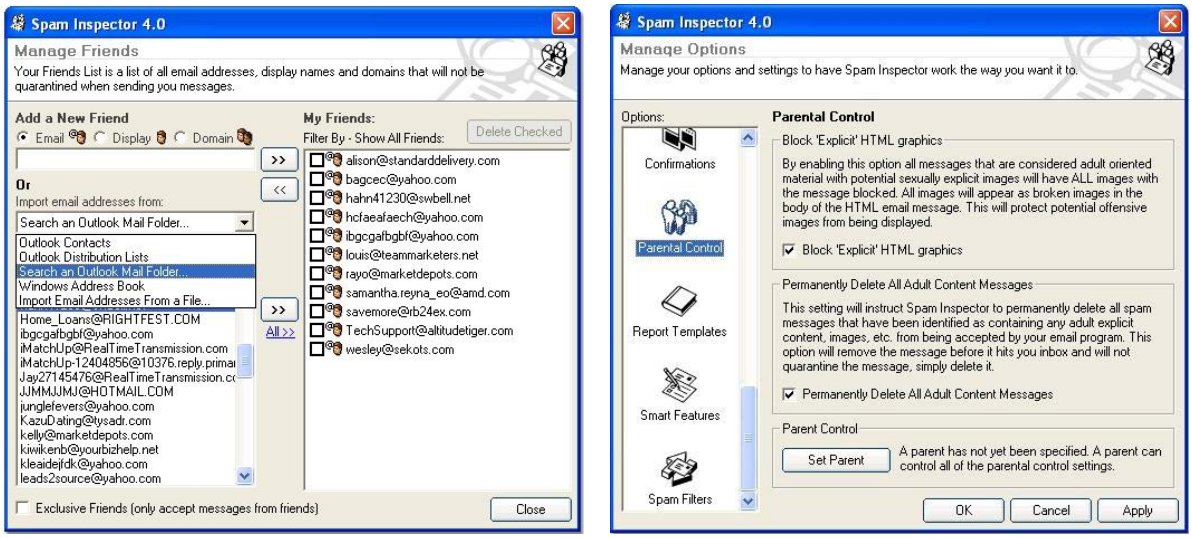
Once you have installed *Spam Inspector* you are given the choice to select which email clients and email accounts you would like to have *Spam Inspector* protection activated for. At anytime in the future, you can easily change these settings, adding or removing email clients or email accounts with one click.

After completing the *Spam Inspector* installation, the next time you open your email client you are guided through a simple getting started process. This process will import all of your local address books to your *Spam Inspector* Friends

List and quickly help *Spam Inspector* make more informed decisions on how to treat your incoming email. However if you choose, you can simply ignore this whole step and *Spam Inspector* will automatically begin filtering your email using its internal database. *Spam Inspector* processes each message against thousands of filtering rules, spam patterns, known spam lists, and checked for spam mutation fingerprints, based on spam reports from other users of *Spam Inspector*'s Global Response Spam Learning Network. These filters are updated regularly and automatically, keeping *Spam Inspector* up to date.

Then based on your incoming email, *Spam Inspector* optimises all of its statistical filters using a patented self learning classifier, calculating the probability that each incoming message is spam and quarantining the junk email away from your Inbox.

The *Spam Inspector* toolbar provides quick access to commonly used *Spam Inspector* features, such as add a friend, a complete domain, or identify an enemy. The first time you use any feature on the toolbar, *Spam Inspector* presents a tips popup window to better explain what exactly the toolbar function does.



The online version of this magazine has links to view twelve screen shots which show the versatility of the Spam Inspector configurations options. Those above are only two examples.

Opinion

Both these packages are working at a disadvantage in that the spammer is already in your in-box. If you are away for a few days your server quota may be exceeded and important messages rejected and returned to the sender, as happened recently to our past President. On the other hand they both allow a degree of fighting back which, when coupled with the strengthening of anti-spamming laws in Europe and the US, may lead to the eventual defeat of the spammers.

Spam Cop is free and requires very little effort on your part to report on spamming activity. *Spam Inspector* quarantines spammed mail to allow you to examine it at your leisure, but does not stop the spam from arriving in the first place. On this issue alone, *Spam Cop* provides the better value for money as both allow the spam to arrive, but *Spam Cop* is free and *Spam Inspector* costs money. I also had the occasional problem of not being able to download any mail from my server until disabling *Spam Inspector*.

Ultimately, *Spam Inspector* is just another rule based filter which does nothing to stop the spam arriving, but may help you keep your sanity by automatically moving the spam to a suitable folder, generating abuse reports and making you feel that you are in control. Your cholesterol may go down, but the spam will still keep coming in.

Ideally, I would like to send the equivalent of a nuclear-tipped cruise missile to the spammer's home address, but as they move around I would probably kill innocent civilians on the way. Ultimately we need better policing of the web, but that involves all sorts of moral, ethical and political considerations … but this is just a software review column!

Spam Cop
Functionality **
East of Use *****
Support ***
Value for Money ****
Platforms: Windows 98/Me/NT4/2000/XP
Vendor: Spam Cop (www.spamcop.net)
Price: Free

Spam Inspector
Version 4.0
Functionality *****
East of Use ****
Support ****
Value for Money **
Platforms: Windows 98/Me/NT4/2000/XP
Supported Mail Clients: *Spam Inspector* can be integrated into Outlook 2000/2002/2003, Outlook Express 5/5.5/6.0, Incredimail, Eudora 5.1,5.2,6.0, and MSN Hotmail (through Internet Explorer 6.0, Outlook, Outlook Express, and Incredimail).
Vendor: Giant Software (www.giantcompany.com)
Price: Currently US$19.95 (normally $29.99)
Evaluation: A free 15 day download is available

Dr John A Mitchell
LHS Business Control
Tel: +44 (0)1707 851454
Fax: +44 (0)1707 851455
Mobile: +44 (0)7774 145638
Email: john@lhscontrol.com
Internet: www.lhscontrol.com
John has no financial or other interests in the software reviewed by him. His views are his own and do not necessarily reflect those of the London Chapter or ISACA. John takes no responsibility for any harm suffered to an individual, organisation, or system as a result of his views.

Is Sarbanes-Oxley the new Y2K?

Kevin Handscombe

The Y2K issue caused a major increase in demand for IT audit skills, the stock-in-trade for the CISA member, to review company systems for problems. The Sarbanes-Oxley Act could be bringing a similar increase in demand. It will not just impact on US companies and not just on the very largest. To find out how it could impact you, read on.

1 What is Sarbanes-Oxley?

There are several articles in the recent issue of the International Managazine[1] (you wait all day for an article on Sarbanes-Oxley and three come along at once!). They provide a good explanation of the history and some of the issues, so I'll keep this bit fairly brief.
The Sarbanes-Oxley Act of 2002 ("SOX" or "the Act") was a response by the US legislature to the major corporate scandals transpiring in 2001 and 2002 (Enron, Worldcom etc) that eroded public confidence in big business. Section 404 of the Act requires Directors of US listed companies to confirm that they have effective systems of control over financial reporting. This seems reasonable enough; after all we have had similar provisions in the UK under 'Turnbull' for some time. But SOX, or at least the Securities and Exchange Commission's (SEC) interpretation of it, goes further than this, because it also says that:

1 Controls have to be documented and tested to prove that they are operating effectively
2 The Directors have to report their conclusion on control effectiveness
3 The external auditors have to review the Directors' approach, test the controls and provide their own opinion on control effectiveness
4 The control assessment work has to be made available for the SEC to review

The Act has raised the stakes to enable the authorities to force individuals and companies to comply. Making wilfully incorrect statements can be punished by substantial fines and prison terms. Needless to say, this caused some consternation in corporate circles, especially amongst the many foreign companies with US listings. Many companies will feel that they have adequate systems of control, but a much smaller number will have documented them fully and still fewer will have tested them and retained the evidence of testing.

2 Why is it like Y2K?

A company's SOX project has certain similarities to the Y2K project that they will probably have been through a few years ago.
Firstly, it is a project that nobody has done before, so there is uncertainty, and no ready-made roadmap of how you do it. There are no easy short cuts. It's down to careful thought and hard graft. It is similar to a large IT implementation as well; a project that you do maybe every twenty years, so you don't carry a lot of in-house knowledge. Unfortunately, there are surveys that show that IT implementation projects have only about a 50% success rate.

Secondly, it has a fixed deadline. The deadline was originally for accounting periods ending after 14 September 2003. When companies realised that they weren't going to make this date, they raised objections and the deadline was moved to give them more time. For US companies the date is now 15 June 2004 and, for non-US companies, 15 April 2005. After getting this extension, woe betide anyone who isn't ready to provide a positive conclusion or able to convince their auditors to do so by the new date!
Lastly the project needs IT specialist expertise, particularly IT audit skills, to be successful (I'll come back to that later). During the Y2K scramble, programmers were a scarce commodity and able to command large salaries. Maybe the CISA fraternity will see a little of that action.

If companies still have the project documentation lying around from their Y2K project, or better still, some of the staff who were involved in it, they would be well advised to make use of that knowledge. Look at how the project was set up, what resources were required, what went well and what went badly, etc.
There is of course one fundamental difference between SOX and Y2K. While Y2K projects came to an end, assuming they had achieved their objectives, on or before 31 December 1999, the requirement to report under section 404 of SOX will, we have to assume, continue for the foreseeable future.

3 What is involved in a SOX project?

A significant amount of work is required in a SOX project and it should not be under-estimated. It is likely to include at least the following steps:

- Develop an internal control approach to design, assess, test, remediate, monitor and track controls
- Analyse existing internal control framework and perform gap analysis against recognised framework
- Project start-up: Determine resourcing needs, scope project and prepare detailed plan
- Document the entity-level business model, risks, processes and associated internal controls over financial reporting
- Test the internal controls that will be relied upon to address key risks and that management will certify as effective
- Provide recommendations for improvement to internal controls and design new controls to address gaps
- Monitor continued compliance with control requirements and update documentation for changes to the control framework

You will notice that many of these are fairly standard steps for most projects, and very similar to the steps within an IT implementation project.

4 Why are CISA skills needed?

A typical SOX project will require a number of skills that a typical CISA possesses:

- Process mapping

  Documenting the significant processes, sub-processes, risks and controls that impact on financial reporting is a crucial part of a SOX project. Process mapping is something that we have been doing for years in relation to IT systems. It's mostly just a matter of extending this to mapping all systems. But, before we launch into doing our flow diagrams, we should recognise that it may also require a slight change in style, because we typically document processes horizontally. That is to say, we usually document across business functions, looking at systems on an end-to-end basis. But for SOX, we need to think vertically. We need to limit ourselves to processes impacting on financial reporting, because that is what section 404 requires, and not get side-tracked into operational processes, no matter how interesting they may be.

- IT technical aspects of systems

  Analysing and documenting processes, risks and controls for a complex ERP system requires technical knowledge of that system. ERP systems will have a large number of controls available as part of the configuration. Many of the risks identified will already be covered off by a system control, so that you don't have to go off and invent a new manual control. The trick is knowing that the control is there, because so many will be invisible to the uninitiated. Another trick is knowing how to use the system to check whether the control is operating effectively.

- Preventative controls

  An extension of the last point is that many of the ERP system controls will be preventative controls; and these can be difficult to audit. In many cases, risk x can't happen, because the system will not let you do it; it was part of the configuration on installation. But auditors don't like auditing preventative controls, because they are so difficult to evidence and so difficult to prove that they have been

operating for the whole period. IT audit expertise can get around the temptation to treat the ERP system as a 'black box' and design good tests, particularly automated monitoring tests.

- Project management/review

  Project management is key to the success of the company's SOX project. There is likely to be a substantial amount of work to do to get a company ready; even more for a distributed international group. Traditional project management skills will be relevant: deciding what has to be done, deciding who will do it and making sure that they do. As already mentioned, nobody has done one of these projects before, so experience with big one-off IT projects will stand project managers in good stead. Experience with IT project risk reviews will also be valuable, to review and identify when SOX projects are going off the rails.

- Expertise in auditing controls

  It is likely that we will have the expertise in testing detailed controls that may be lacking among external and internal audit teams. CISA skills could fill the gap by either carrying out the testing work, or providing a training and coaching role.

External auditors are required to provide an opinion on the truth and fairness of the financial statements. They are not required to report on internal controls directly or explicitly. It is true that, in forming their opinion, they may test and rely on certain controls; but, these controls may be high-level controls. Controls identified for testing in a SOX project may include controls at a much more detailed level. It may also be that it is more efficient for the auditor to check a particular account balance substantively, rather than to rely on controls to produce it.
There seems to have been a trend in recent years for Internal Audit departments to move away from the traditional control testing model to do more risk management work. This may have been partly in response to the encouragement of Cadbury/Greenbury/Turnbull . It may also have been caused by a desire to be more central to the organisation's strategic direction, rather than internal control, which could be perceived as peripheral. Some Internal Audit departments have renamed themselves 'Risk Management'. As a result, Internal Audit seem to spend most of their time running risk workshops, identifying and analysing risk. A recent academic study[2] concluded that they are now communicators and facilitators, rather than auditors. They found that there is "remarkably little traditional auditing ('kicking tyres', 'ticking and bashing') happening".
SOX raises a further problem for Risk Managers because it does not give them the freedom that they may be used to. Their current role can mean that they can manage the identified risks with alternative strategies. The new draft COSO framework[3] lists the risk responses as: avoidance, reduction, sharing or acceptance. For SOX, you don't have this 'luxury', you have to identify a control for each significant risk and then assess whether it's effective.

5 Why could it impact on me?

The requirement is for SEC-registered companies to comply with SOX. Even if your company/audit client doesn't fall into this category, is it a subsidiary in a group that does? If so, you may be required to report upward on financial controls for operations that are significant to the group.
Complying with SOX may come to be regarded as good practice and a means of demonstrating good corporate governance. Foreign companies listed in the US may decide to adopt early and, eventually, we may even see companies that are not listed in the US adopting SOX to meet the perceived standards set by competitor and peer organisations.
There is also continuing speculation that the SOX approach could be adopted in Europe – a development that recent events surrounding Parmalat in Italy will have done nothing to delay. The potential for a shortage of CISA-type skills already mentioned, could improve job prospects for many.

6 What should I do?

If I'm part of Internal Audit:

- Find out if your company is impacted by the regulations and what the state of the project is. If you are directly impacted, offer your services to the project team. This may require a selling job if they don't realise they need you. You could be proactive and suggest a project risk review. If you are indirectly impacted, you could do the same for the head office project team, but it's more likely that you will be pushing for group instructions to plan

for what they will be asking you to do. Also, try to dust down the Y2K project, if you can still find it. It may contain some useful tips.

If I'm part of External audit:

- Find out, if you don't already know, which of your clients are impacted and get on the audit team. Be proactive and suggest a project risk review, or a client readiness review. Identify those clients who are behind schedule and get them back on track, or they may not be clients for a lot longer. It's probably more difficult if your client is a subsidiary of a US parent, and the US office hasn't contacted you yet with group instructions. Keep chasing them.

If I'm a Sole Practitioner:

- If you haven't got any clients who are affected, you might still like to get out there and advise companies who have left it to the last minute. Companies' auditors are precluded from doing certain parts of a SOX project for a client, due to independence rules. So there should be plenty of opportunities to assist.

To find out more
The ISACA website[4] has additional information on the issue. This includes a discussion document issued by the ITGI, IT Control Objectives for Sarbanes-Oxley. Its purpose is to reflect the latest thinking on this topic and is based on COBIT control objectives.

References

1 Information Systems Control Journal Volume 1 2004

2 M Page & L Spira From Compliance to Communication: Perspectives on the Changing Role of Internal Audit, 2003

3 The Committee of the Sponsoring Organizations of the Treadway Commission Enterprise Risk Management Framework, 2003

4 (http://www.isaca.org/)

Kevin Handscombe CISA, ACA is a member of the London Chapter Board, a Senior Manager with KPMG LLP and has nearly 20 years' experience as an IT auditor.

ITGI Surveys Marketplace

In late 2003, the IT Governance Institute commissioned PricewaterhouseCoopers (PwC) to conduct a market research survey to gain a better understanding of the IT governance global marketplace and the opportunities it might contain for the ITGI.

Although the ITGI has identified several targeted audiences—CEOs, COOs, CIOs, CFOs, board members, IT management and practitioners—for its anticipated deliverables, the purpose of the research was to reach members of the C-suite to determine their sense of priority about IT governance and their need for tools and services to help assure effective governance. This high-level objective was translated into the following detailed objectives:

- Survey and analyze the degree to which the concept of IT governance is recognized, established and accepted within boardrooms and with the CIO.
- Research tools and frameworks for IT governance, and determine where organizations look for expertise and services in this domain.
- Obtain direction as to which enhancements could be made to the ITGI's current IT governance products and services to better suit the IT community's needs.

CIOs and CEOs were contacted from the PwC contact databases. The total number of interviews conducted was 335, of which 276 were from a random sample of organizations and 59 were known COBIT purchasers. The main finding in relation to the audience is that although 80 percent of the people contacted were at CEO level, only about one-third of these CEOs felt comfortable enough to talk about IT governance. The remainder referred us back to their CIO, IT manager or, in some limited cases, their auditor.

All continents/regions were represented in the survey, and interviews were conducted in 21 countries. Response rates varied among countries and regions, with high response rates in Europe and lower response rates in North America. This caused a slight over-representation of European countries in the total set of answers, but careful analysis showed that this had a negligible effect on the survey results.

Some of the top messages from the research include:

- **More than 93 percent of business management recognizes that IT is important for delivering the organization's strategy.** There is a worldwide consensus about the importance of IT for delivering the overall strategy of the organization. This is observed across most industries (IT/telecom, financial services, manufacturing and public sector—average 93 percent). The retail sector considers it somewhat less important for the delivery of its overall strategy. Somewhat paradoxically, general management perceives the importance of IT for the delivery of the overall strategy slightly higher than does IT management.
- **Organizations are suffering from IT operational problems.** Respondents were supplied a list of typical IT problems. Only 7 percent of respondents experienced none of the listed problems in the previous year. Most frequently cited were operational failures and incidents and an inadequate view on how it is performing, mentioned by approximately 40 percent of all respondents. Combining this result with the one above begs the question: If IT is so important, why do enterprises still have problems?
- **The top three CIO concerns are operational effectiveness, compliance and better alignment (ROI) with business strategy.** Desk research was conducted in addition to the survey. The desk research, which included the review of recent high-profile articles, other surveys, and PwC's own recent experience and work, led to the conclusion that today's CIO is dealing with following basic issues:
    - The need for better operational effectiveness of IT. How can it be used in the most cost-effective manner, or how can it do things better

- The need for compliance with existing and new regulatory requirements, which are now more than ever affecting it. The most notable example is Sarbanes-Oxley, but other national variants are emerging or have emerged.

- The need for better alignment of IT with the business strategy, and for tools and frameworks to do so

- **CIOs recognize a need for better governance over IT.** A substantial portion—75 percent—of the IT community is aware that IT has issues that need to be resolved. Surprisingly, an even more substantial part (more than 80 percent) recognizes that IT governance or some form thereof is required to resolve the issues they face.

- **IT governance frameworks are used to align IT strategy and manage IT operational risks.** IT governance solutions/frameworks are used mostly for aligning the IT strategy with the overall company strategy (57 percent) and to manage the IT operation's risks (53 percent).

- **Good IT governance helps organizations provide IT value and manage IT risks. (COBIT is a way to implement effective IT governance.)** Process models, such as COBIT, can substantially help in the realization of effective value and risk management. One of the questions asked of the CIOs (Are IT operations running as smoothly, reliably and cost-effectively as possible?) can therefore be looked upon as a valid question, addressed in large part by such process models.

- **COBIT is COSO compatible.** Whether the respondents like it or not, the general consensus is that IT and compliance will have to go together from now on, forced by the regulators. Given that the major corporate governance framework, i.e., COSO, provides few concrete guidelines about IT, it would benefit many organizations enormously to have a framework available that translates COSO into IT language. COBIT does that and is fit for regulatory IT governance purposes.

- **COBIT users are very satisfied.** Eighty percent of those who use COBIT as an IT governance framework are highly satisfied with it.

- **COBIT can be an integrator.** COBIT is quite unique, as it is very broad and encompasses the whole IT domain. If this is agreed to be a key strength, COBIT should not focus on evolving with further detail, but should focus instead on interfaces to other established frameworks.

- **Large IT consulting firms are effective implementers, while ISACA and ITGI provide the expertise.** Large IT consultancy firms, along with ISACA, are considered to have the greatest IT governance expertise (3.8 ranking out of a possible 5), whereas strategic consultants (such as Boston Consulting and McKinsey) score 3.0-3.3 out of 5. Gartner and the Big 4 firms are in the middle (3.6 out of five). When asked about implementation ability, respondents indicated that ITGI and the strategic consultancy firms are rated relatively low, while the large IT and consultancy practices are recognized as being most effective implementers.

The results of the ITGI market research study will be published by the end of the third quarter and will be made available prior to that through articles, webcasts and presentations.

Seeing Double

by a Computer Audit Manager and the Head of Management Audit at a UK company

At first sight, looking for invoices that have been paid twice hardly seems the sort of cutting edge computer audit work to bring the Board to the edge of their seats. However, before dismissing it as unworthy of your attention, bear in mind that if there really is a control problem, recovering previously unnoticed double payments could save your organization several times the cost of the audit. If you ignored this area and significant duplicate payments came to light, would you feel able to justify not having made such a basic check? What if fraudsters had exploited a control weakness to divert and conceal payments to their own accounts? If there is no control problem, at least you can give management assurance on this score based on having reviewed the controls as well as thoroughly testing them.

It is surprisingly easy for invoices to be input and paid twice. Those who authorise invoices for payment are members of line management, who are often not directly concerned with accounting for those invoices. After signing them off, line management assume accounts payable will escort the approved invoices through the system, unaware that accounts payable process hundreds or thousands of supplier invoices each day. Similarly budget controls may not be sufficiently hypersensitive to glitches at individual invoice level. There are numerous snares when it comes to wrongly processing supplier invoices.

One scenario is for an invoice to be put aside or mislaid before it is logged. When the supplier eventually chases for payment, no record of the invoice exists, and the supplier faxes a copy which is then paid. Then the original resurfaces, and if no one remembers paying the copy, that too is input and paid.

Another scenario is where the supplier sends in a draft or pro-forma invoice in advance of the real thing. These can be confused for a legitimate invoice and approved for payment. Even supplier statements can be confused for an invoice requiring payment.

And that is to say nothing of bogus suppliers, invoices which do not match the delivery of goods or services and suppliers who, deliberately or otherwise, charge for the same goods or services more than once.

Once a duplicate payment has been made it can easily remain undetected if creditors do not send statements, or statements are not reconciled.

Over a period of time, processing such invoices can result in over-statement of creditors and expenses, as well as a substantial pot of money which can be recovered from suppliers or offset against future payments.

You might think that the task of finding invoices input twice is laughably simple. After all, surely all you have to do is to run a report to find duplicate supplier invoice numbers (which are usually unique alphanumerics)? When you come to consider it, however, it isn't quite as simple as that, especially if you don't have sophisticated audit software. While a check for duplicate invoice numbers will yield useful information, for a variety of reasons it will also yield plenty of apparent duplicates that aren't (false positives), and ignore many true duplicates. This is because:

1. Suppliers' invoice numbers will have to be input to a free-format field, and therefore can very easily be keyed in slightly differently each time, accidentally or deliberately defeating any process that looks for precise duplicates only.

2. Input staff may interpret the same invoice differently each time it is input, and enter totally different codes for the invoice number on different occasions, defeating even fuzzy matching.

3. Some small suppliers will not use invoice numbers, or will always use the same one.

4. Some invoice numbers will occur frequently, such as 1, 10, 100 etc. resulting in numerous false positives for an audit test which merely attempts to match on supplier invoice number.

5. Some large suppliers send invoices regularly but don't use invoice numbers. Your report could easily be swamped with BT phone bills, if staff input the phone number in the absence of an invoice number.

6. Some duplicate invoices will already have been spotted and reversed with a credit note, put on hold, or a refund obtained. You need to be able to detect whether any of these have happened, and verify that the correct action has been taken. For example, if a refund has been obtained, has the original entry (the credit to the creditors ledger and the debit to the expense account) also been reversed? If not, the accounts will still overstate creditors and expenses.

It is also worth bearing in mind that inputting an invoice twice has implications beyond the unnecessary expense. Even if unpaid, as mentioned above it overstates expenses and creditors, and could therefore distort the accounts. And if there was VAT on the invoice, it means input VAT has been recorded twice, and hence claimed twice from Customs and Excise. It also of course understates profits and leads to underpayment of Corporation Tax.

We found that the most effective way of tackling the problem was to identify the possible combinations of error conditions, and devise reports to detect each. These may be represented as follows:

From our experience, we would suggest the following approach:

First, Home in on the Likely Suspects

Even if you do not have audit software, reporting software should enable you to refine the basic duplicate invoice number report to eliminate many of the false positives, and tease out a few less obvious duplicates. With luck, your accounting software may automatically give reversing transactions the same invoice number as the original transaction. Therefore, grouping transactions by invoice number will show both duplicates and any simple reversing entry. If possible, you should filter out any such groups of transactions which sum to the same as a single transaction (i.e. where one of the duplicate invoices has already been reversed). This will greatly reduce the number of false positives. We then eliminated some of the other large sources of false positives, e.g. rates and phone bills, though this did mean that if any of those had been input twice, we would not have found it. It quickly became apparent in this exercise that it was very much a matter of approximation and trial and error, and that no exception report would ever be perfect. It would always contain some false positives, and fail to pick up some genuine duplicates. If you try to make a report show all invoices input twice, it is likely to be swamped with similar invoices that are not duplicates. However, reports with a moderate number of false positives can be fairly quickly checked by looking at suppliers' accounts.

Second, Use Fuzzy Logic to Increase your Hit Rate

We refined our initial duplicates report by creating our own basic 'fuzzy matching'. We created a calculated field which concatenated other fields, which we then used as a sort key, and we experimented with the components of this field until we found a combination which seemed to work reasonably well for us, in the sense of yielding only a small number of false positives that could be easily eliminated by looking at them. The combination that worked for us was the amount, the invoice date, and the last two characters of the invoice number. Invoices which had all of these in common were either duplicates of the same invoice, or so obviously different that they could be ruled out visually. (E.g. some suppliers have invoice numbers where the serial number is somewhere in the middle and the last few characters are always the same). We could have included the supplier account number in our composite field, but we found that in a number of cases the second invoice had been miscoded to a second supplier account with a similar name, e.g. another

office of the same supplier. Unfortunately our report did not show duplicate invoices input with different dates, but to include these also included large numbers of routine recurring charges such as equipment rentals. As a finishing touch, we used the full invoice number as the second sort key, thereby capturing all items included in the original version of the report. As we still incorporated the logic described above to eliminate reversed duplicates, we now had one report that showed both precise and fuzzy matches.

Third, Eliminate the Double Payments Which Have Already Been Spotted

The next most important area we wanted to cover was to check that where someone had already spotted the duplicate payment, and reversed the invoice entry with a credit note, that the invoice had been deducted from a subsequent payment to the same supplier. For those suppliers who had not been dealt with since, we wanted to see whether a refund had been received. We were lucky that our accounting software made it easy to check this. On our system, all bought ledger transactions have a "matching id" field, and all matching transactions (such as invoices and the corresponding payments) have the same value in this key field. Unmatched transactions have a zero. It is thus easy to see which payments relate to which invoices, and also which invoices have not yet been paid. All we had to do, therefore, was to print a report of all credit notes on the bought ledger which were more than a month or so old and had not yet been matched with cash receipts, or deducted from cash payments. Interestingly, this as a by-product showed which credit notes granted for other reasons had not been realized. Here is another potential pot of money you could recover from suppliers.

Fourth, Look for Wrong Accounting

Related to this, is the situation where the double payment has been spotted and a refund has been received, but the original debit to expenses and credit to supplier transaction has not been reversed. This, of course, would mean that expenses and creditors were still overstated. In our system, this can be found in the same way as unmatched credit notes. That is, by looking for cash receipts posted to supplier accounts that have not been matched to credit notes. It is also easy to produce a slightly different version of this report, which shows what credit notes and cash receipts are unmatched on each supplier account, to see whether there are any obvious cases where the two can be matched off. Although not representing recoverable cash, entries of this type represent a favourable accounting adjustment to profits, as expenses may have been wrongly over-stated.

Fifth, Do a Health Check using Benford's Law

Benford's law can be applied to detect possible recurring irregularities where actual digit frequencies do not correspond to the expected frequencies. Last time we looked, the website http://www.newscientist.com explained Benford's law and how to use it, not just for a supplier payments audit but for any large set of measurements.

Sixth, Look for Uncorrected Double Entered Invoices

Our final check was for any invoices which had been input twice, but spotted, and only paid once. These cannot of course simply be left on hold for ever, as again they overstate expenses and creditors, and lead to underpayment of VAT. We were fortunate again, in that our accounting system had a field for each transaction which contained the date it had been paid. In the report for duplicate invoices which had both been paid, we had filtered out duplicate invoices which had not been paid. It therefore only required a small modification to that report to make it show instances where invoices had been input twice but only paid once. Once verified, these could then be reversed.

Plan B if this is all too Difficult

If your accounting systems do not arrange data in the ways envisaged by the foregoing, or if you've not got the time or resource to find out, we did tackle another area of potential double payments in a different way. Grouping payments data by reference to the amount paid was a relatively straightforward way to identify potentially double paid invoices. Although easy as well as quick to perform, this method had three clear disadvantages:

- Although great for spotting recurring unusual amounts, common amounts re-appear monotonously, especially round figures like £5,000, £10,000, £100,000 etc (or £5,875, £11,750, £117,500 etc if you're analysing the amounts gross of VAT)
- As a result it can result in many more false positives requiring more manual audit time to sift through the chaff
- The resulting exception report is therefore not sufficiently precise to hand over to management at the end of the audit.

The Potentially Awful Consequences of Getting it Wrong

The consequences of multiple-paid invoices could be large. They would include

- the unnecessary cash outflow
- funding costs (overdraft interest, or deposit interest forgone),
- the cost of management and audit time in identifying and recovering overpaid amounts from suppliers,
- accounting errors resulting from the overstatement of expenses and creditors. (Even when suppliers return money overpaid to them, the accounting errors in terms of overstated creditors and expenses can remain unadjusted);
- over claim of input VAT,
- underpayment of corporation tax,
- mis-statement of profit and liabilities in the financial statements
- tarnish of the company's business reputation in the eyes of at least some suppliers and the relevant tax authorities who may assume with some justification that you've made other errors which may result in friendly visits from the tax auditors.

Even where there are no findings, this audit represents an important health check on the system for paying invoices.

Keep up the Good Work!

It also follows that this audit should not be just a one-off exercise. Whatever the state of controls over duplicate payments, it is worth checking whether any invoices input in the last month or so appear to duplicate invoices previously input. In this way there is of course a much greater chance of stopping a second payment, making correction of the error far easier. We therefore set up our reports with run-time parameters, so that they would check just invoices input between specified dates, and compare them with anything input during the previous year. Thus the investment in the reports can give not only a one-off benefit of checking for duplicate invoices accumulated at a point in time, but at minimal extra cost it can provide ongoing benefit as an exception report for management to check for duplicate invoices almost as they occur.

The authors are the Computer Audit Manager and the Head of Management Audit at a UK company. Both have over ten years' experience in their fields, and have published a number of articles in the audit press.

A version of this article was first published in Internal Auditing & Business Risk magazine in February 2004.

ISACA's New Strategy Mixes Varied Topics and Audiences

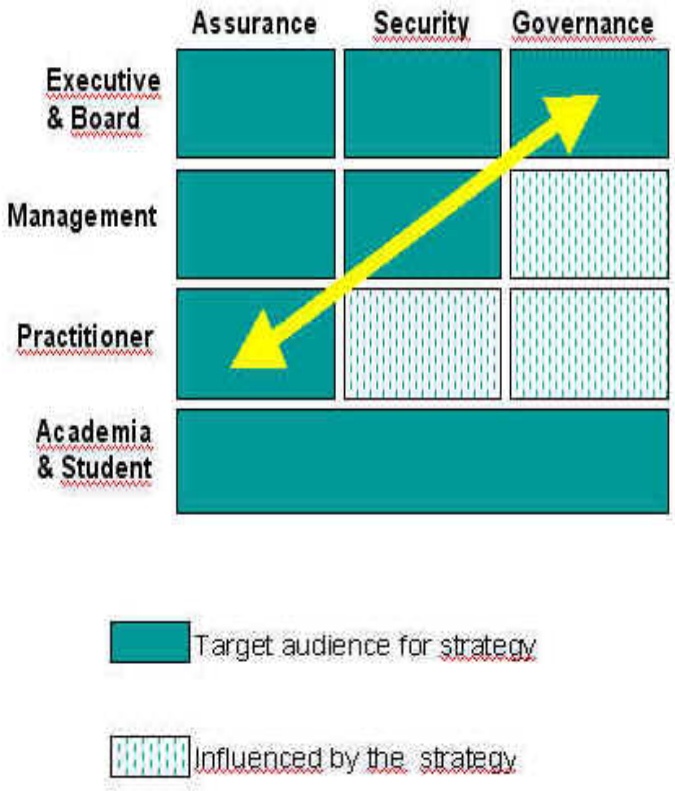
In 2003, Information Systems Audit and Control Association® (ISACA®) announced a new strategy, resulting from a series of meetings of global association leaders. The strategy examines professional topics and targeted audiences to be addressed by the association and the IT Governance Institute® (ITGI), and concludes that ISACA has three strategic thrusts:

1. ISACA is doing well in serving the needs of its traditional audit audiences. It should continue to perform and maximize these activities. This thrust is referred to as *IT Assurance*.

2. ISACA should reach out to the information security market, specifically the management niche. This thrust is referred to as *Information Security*.

3. ISACA should capitalize on its leading position in IT governance, and further expand and emphasize the activities of the IT Governance Institute. This thrust is referred to as *IT Governance*.

Four layers of audience were identified as within the organizations' range: boards/executives, management, practitioners and academia/students. When current level of maturity in each box was considered, ISACA was determined to have the most penetration at the practitioner level in IT Assurance, at the management level in Information Security and at the boards/executive level in IT Governance (see **figure**).



The key boards and committees were provided this information and asked to map their current activities to the chart, identify gaps and suggest activities to fill the gaps. The results of their deliberations were compiled into an 18-month plan, which outlines current and planned new activities for that key board or committee for the next 18 months, the constituency served for each (in accordance with the three professional areas outlined in the strategy and the targeted

audiences identified in the strategy), plus any comments or recommendations on resources required, time schedules, etc. Although space constraints preclude reproducing each key board's entire plan, here are a few highlights of the proposed new activities from each group:

CISA® Certification Board

- Increased program awareness among governmental entities
- Investigation into offering the review course in modules or online
- Investigation into the need for certification programs for assurance management and/or COBIT® practitioners

CISM™ Certification Board

- Increased awareness/recognition among governmental entities and leading organizations/institutions
- Increased program promotion
- Establishment of a CISM Test Enhancement Committee (now completed)
- Development of education courses based on the CISM job practice analysis

COBIT Steering Committee

- Update of the control objectives and audit guidelines
- Alignment of COBIT with the IT governance domains and expansion toward the security domain
- Promotion of new products: *IT Governance Implementation Guide*, COBIT *Quickstart*™, implementation training

Education Board

- Creation of an information security management conference (first one scheduled in third quarter 2004) and courses
- Creation of an executive-level assurance event and an intermediate IS auditing course
- Creation of a COBIT users group convention (first one scheduled for fourth quarter 2004)
- Development of a list or template of minimal educational programs that should be offered at a chapter level

Governmental and Regulatory Agencies (GRA) Board

- Creation of a task force in area 1, initially to address Indian opportunities and later to represent the entire area (now completed)
- Pursuit of representation on the EU Committee on Auditing
- Maintenance of contact with Information Security Interest Group in Australia, with the goal of ISACA being recognized as a certifying body
- Expanded operation of the task force working within area 2

ITGI Steering Committee

- Creation of an executive version of the *Board Briefing on IT Governance*
- Creation of a comprehensive research plan
- Creation of an organizational structure for the IT Governance Institute
- Creation of a stand-alone IT governance educational event aimed at the executive level (now scheduled for October 2004)

Membership Board

- Completion of the job progression study
- Development, in cooperation with the Education Board, of information security education programs for use at chapter level
- Creation of a chapter award for CISM growth
- Administration of a new benchmarking study for assurance professionals

Research Board

- Revision of the research framework
- Initiation of the use of “blue ribbon” panels of experts to create white papers on pertinent topics
- Creation of deliverables directed to development of best practices for information security management and governance
- Creation, in cooperation with the Education Board, of self-assessment questionnaires and work programs

Standards Board

- Development of a harmonization framework to identify existing security guidance
- Adoption of existing security guidance or creation of new guidance in needed areas
- Review of current assurance standards to determine if they meet security management concerns
- Establishment of a security management standards process

Work began on these plans in late 2003 and will continue through year-end 2004, at which time the plans will be updated and continued, or revised and reworked.

IT Governance and the CobiT framework

Thomas Turner

Introduction

The need for internal control of all aspects of the business is more imperative now then ever, especially with changing laws and technologies. Information Technology has long been associated with the failure to deliver the value it has the potential to produce. At extremes, the failure to manage this potential has contributed to the corporate collapses like Enron. IT governance is a new theory, which is understood by many organisations to have powerful advantages. It is important because it aids organisations to conform to ethical and legal standards, like stakeholder accountability and SOX. It is valuable to organisations as it enables them to have a framework that delivers IT value to business activities and to manage IT risks. With the help of John Mitchell and the London ISACA members, I was able to research the usage of this ideology and its principal tool CobiT, by means of a questionnaire and evaluate both frameworks. Because of this the responses are fundamentally bias towards the adoption of IT governance and therefore do not represent a neutral group of responses. It was imperative to contact organisations who had addressed IT governance, as only they would have implemented CobiT. For this reason, I still feel the results present a good assessment of IT governance and the CobiT framework.

Results

My research found that the take-up of IT Governance was very high above 85% though only 23% of organisations reported all five of the key elements of the ITGI framework as definitely impacted. 10% reported that the five key elements had no impact with their organisation. Of the 26 respondents who identified IT governance in their organisation 92.3% of them stated that it has an impact upon value delivery. Of these only 50% reported it to be a definite impact. 100% of organisations stated that IT governance has an impact upon risk management and of these 88.5% reported that IT governance 'definitely' has an impact upon risk management. The results show risk management to be a hugely governed subject in today's organisations. The most impacted area of IT governance was security; at 80% it scored the highest 'definite' connection to IT governance. Technology was the most common IT resource to be governed. 83% of organisations reported IT governance to have an impact upon corporate governance.

I started my research with the intention to asses the take-up of the CobiT framework. I wanted to identify if it was the primary employed IT governance tool. My results showed that CobiT is a very well known tool as 96% of respondents had heard of CobiT. Only ISO 9000 and ISO 17799 were more recognised. CobiT was the second most implemented tool in organisation that used IT governance at 38%. Though my results are not from neutral organisations, nevertheless CobiT is still implemented in over a third of organisations that use IT governance. Top was ISO 17799 at 42%. Therefore, CobiT did not rate as the primary IT governance tool, but a very close second.

My results showed that there was only an 11% difference in the level implementation of the domains. There was an interesting trend for organisations to address the 'Planning and Organisation' and 'Acquisition and Implementation' domains almost identically. This shows that the way organisations implement CobiT is as a united representation of the framework.

CobiT is intended to cover all IT activities and my results showed that it achieved this in practice, as the average percentage of CobiT scope was 80.6%. My results also showed that while the implementation did prove difficult for most organisations once implemented, 64% reported that the ease of operating CobiT was above average. A disappointing result was that organisations found tracking their position through the framework difficult. Although many organisations stated they were at an early stage of implementation and so tracking their progress would not be a priority as many would only be using the framework in 'general terms'.

Conclusions

- Over two thirds of organisations have adopted some form of IT governance
- Risk management is the more addressed outcome of IT governance
- Organisations do not see technology as a commodity but as an asset of significant worth
- Organisations priorities are to protect their primary asset, information, and in doing so apply a principle motive of IT governance, protecting stakeholders interests

- In the majority of organisations that employ IT governance, there is an established strategic alignment between IT and corporate governance
- The 'Planning and Organisation' and 'Acquisition and Implementation' domains are almost identically implemented.
- Organisations implement CobiT as a united representation of the framework
- CobiT covers most of IT activities
- CobiT is difficult to implement
- Many organisations use the CobiT framework in 'general terms'
- CobiT did not rate as the primary IT governance tool, but a very close second
- At present, organisations attention is firmly focused on security
- CobiT is used to define target risk areas
- The CobiT framework is still young and evolving, but will continue to form the central element of IT governance, as over iterations it is likely to be refined

---

Thomas Turner is a final year student at the University of Greenwich, where he is studying Information Systems. His decision to research IT governance stemmed from his industrial placements year. Here he discovered how important an IT strategy is but at the same time how it was based purely on knee jerk reactions. He originally wanted to research why this was and his tutor at Greenwich suggested he research in the CobiT framework.

Contact details

Email: mccallman@hotmail.com

Document Retention - A guide

Susan Wildey, Solicitor, Technology & Outsourcing group, Tite & Lewis

To shred, or not to shred

" ..that evening [Colonel Oliver] North went to his office…he began removing documents, memos and messages from his files…everything was to be shredded. It took an hour."

The Secret Wars of the CIA, Bob Woodward

If this is your company's idea of effective document management, think again. A number of headline-grabbing US cases involving Enron and Arthur Andersen – and then, more recently, Martha Stewart – have recently highlighted the crucial importance of having, and enforcing, an effective document retention policy.
Such a policy will help you comply with day-to-day legal and regulatory obligations to retain documents, but the benefits by no means end there. During litigation it also helps to ensure that the documents you require to enforce, or defend, a claim have indeed been retained. And then there is the question of 'discovery' during litigation; *ie*, the requirement to disclose to your opponent all dispute-related documents, even the damaging ones. By streamlining the discovery process, effective document management not only helps place a limit on discovery- and litigation-related costs, it can also have the indirect benefit of ridding the company of unnecessary or potentially harmful documents.

"Such as what?", you ask. E-mails. Because e-mails are usually written in an informal way, and because they often include opinion and/or unsubstantiated facts, they are more likely to cause problems than any other company document. Typically there isn't even a business need to retain old e-mails for any great length of time. A policy that requires the regular and frequent purging of e-mails can ensure that potentially damaging, but otherwise commercially useless, documents are no longer available for disclosure. The destruction of documents in this way – in good faith and in line with a reasonable document retention policy – is a perfectly valid legal justification for being unable to produce documents during litigation. On the other hand, the seemingly random destruction of documents can, not surprisingly, raise suspicions.

That said, possession of a document retention/destruction policy is not alone enough. It must also be applied sensibly as circumstances change. After all, Arthur Andersen (AA) had a policy but then made the big mistake of continuing to follow it (a) after the firm had become aware that regulatory action against it was about to commence and (b) even though it knew that to do so would result in the destruction of documents of interest to the regulator. In so doing AA left itself open to a barrage of adverse inferences.

To avoid a similar fate, and to avoid the possibility of incurring criminal penalties in the US under the Sarbanes-Oxley Act 2002 (see Table 1 for details), any document retention/destruction policy must be suspended immediately in the event of (actual or potential) dispute, litigation or enforcement action, and all the appropriate staff, including IT people responsible for the electronic purging of data, must be informed immediately.

Beyond compliance

But the full benefits of an effective document destruction policy go well beyond legal compliance, helping an organisation to:

- demonstrate good corporate governance;
- meet the information retention and storage needs of the business;
- manage (and reduce) storage costs;
- ensure a consistent approach across all sites, locations and jurisdictions;
- improve operational efficiency;
- preserve important information; and,
- protect legal rights, such as intellectual property rights.

So what are the main responsibilities of good policy-makers? There's plenty to consider.

- ***One size <u>does not</u> fit all.*** There is no off-the-shelf answer here. The policy required by a large multinational is likely to be very different to the one needed by, say, a small limited company. In fact, the more tailored your policy, the more likely you are to be able to demonstrate that it is valid and that it was drawn up in good faith.
- ***Balance.*** Legal requirements and business needs must be balanced against technological limitations and cost.
- ***Work together.*** The policy must be a joint effort. Business people, the legal department, the records management function and IT specialists should all work together to ensure that the policy meets the needs of the whole organisation. Expert guidance (*eg,* from lawyers, auditors, regulators) should be sought when necessary.
- ***User-friendly.*** The policy should be designed with the 'end-user' in mind. It should be written in straightforward language and have a user-friendly format. The easier the policy is to understand, the more likely it is to be followed.
- ***Purpose.*** The policy should include a statement setting out its purpose and context, and making clear its scope (does it, for example, apply only to particular departments/countries or to the entire organisation?).
- ***Retention.*** Remember: you are writing a document retention policy; not a document destruction policy. It should not be drafted on the basis of the principle "*if in doubt, delete*", and it should set out which categories of documents should be retained and for how long.
- ***Retention periods.*** How long a document is kept depends on the needs of the business? When, and in what circumstances, are the documents likely to be needed? What would the consequences be if they were not available? It is important to consider whatever norms exist for this kind of thing; these might be externally mandated by legislation or the regulatory environment (both in the UK and abroad) or perhaps recommended simply as good industry practice. In the UK pieces of legislation that contain document retention requirements include the Companies Act 1985, the Value Added Tax Act 1994 and the Listing Rules of the Financial Services and Markets Act 2000. If a document retention policy is to serve a worldwide organisation, then it must also consider how best to deal with different, and potentially conflicting, retention periods in various markets; for example, for any given document category should the policy impose different retention periods in different countries, or simply employ the single longest retention period across all jurisdictions? (Table 2 shows UK examples of legal and regulatory, mandatory and recommended, retention periods for certain types of company information).
- ***Data Protection.*** The organisation must consider the impact of data protection legislation when it comes to retention periods, who has the right to access the data, the transfer of data overseas, *etc*.
- ***Media.*** All storage media should be considered and accounted for, including portable devices such as laptops, PDAs, and the like.
- ***Format and location.*** The policy should specify the form in which data is to be retained – hard copy or electronic – and whether documents should be stored on- or off-site and/or by a third party. (Any associated considerations, such as security, will also need to be thought through).
- ***Electronic Retention.*** The organisation should consider any legal, regulatory or other limitations on the electronic retention of data; in some instances electronic documents alone may not be legally sufficient. Data must also be software/hardware-independent if the organisation wants to avoid the expense of maintaining legacy equipment merely to ensure that the information remains readable.
- ***Responsible Staff.*** The retention and management process should have dedicated staff assigned to it.
- ***Destruction.*** The policy should specify the method of document destruction (shredding, incineration, secure waste disposal, *etc.*).
- ***Document Creation.*** Guidance on the creation of documents helps ensure that unnecessary or potentially harmful documents are less likely to be created in the first place.
- ***Suspension of policy.*** And finally, as AA found to its cost, a policy should include a clear statement that emergence of an actual or potential dispute or investigation will automatically trigger suspension of the policy.

Even with the policy properly designed and documented, the hard work is not over yet. An unenforced policy is worse than no policy at all; the organisation must do all it can to create one that it is both usable and used, including:

- obtain buy-in from senior management to ensure that adequate time and resources are available to enforce the policy;
- properly communicate the policy to employees (in writing, via the Intranet, etc.) and train staff (during induction and with regular refereshers, etc.) to understand and use the policy properly;
- carry out regular compliance audits and ensure that penalties are properly enforced;
- create detailed logs of record destruction, retention and back-up activities;
- review and test archiving procedures periodically;

- review the policy regularly to ensure that it is up-to-date and has taken account of any changes to the law and/or regulations (this is often the most onerous implementation-related task); and,
- retain copies of all policies, proof of communication to staff, and audit reports, as well as legal and factual research supporting the policy.

As many organisations are discovering, some of them the hard way, document management can be a huge headache. But done properly it can be a source of peace of mind and useful business benefits. If your senior management is not putting enough time, money and effort into this issue perhaps you should remind them of the fate of Arthur Andersen. That should re-focus even the most pre-occupied among them.

Table 1

Sarbanes-Oxley Act 2002

This act, signed into US law on 30 July 2002, was a response to the Enron scandal. It introduced legislative changes to financial and corporate regulations which are intended (in the words of President Bush) to "*deter and punish corporate accounting fraud and corruption, ensure justice for wrongdoers and protect the interests of workers and shareholders*".

Sarbanes-Oxley introduced the following new requirements and penalties:

- Section 802: Criminal Penalties for Altering Documents – any accountant who conducts an SEC audit/review must maintain all audit/review papers for a period of five years from the end of the fiscal period in which the audit/review took place. Any breach knowingly or wilfully committed risks punishment with a prison term of up to 10 years and/or a fine.
- Section 103: Auditing, Quality Control, and Independence Standards and Rules – Public Company Accounting Oversight Board – new rules require firms to keep audit work papers (and other information related to any audit report) for a period of not less than seven years and in sufficient detail to support the conclusions reached in the report itself.
- Section 802: Criminal Penalties for Altering Documents – makes it an offence to knowingly alter, destroy, mutilate, conceal, cover-up, falsify or make a false entry in any … document … with the intention to impede, obstruct or influence the investigation or proper administration of any matter within the investigation of any department or agency of the US or in respect of any Chapter 11 case. Any breach can be punished with a prison sentence of up to 20 years and/or a fine.
- Section 1102: Tampering With a Record or Otherwise Impeding an Official Proceeding – makes it an offence for any person to corruptly alter, destroy, mutilate, or conceal any document with intent to impair the object's integrity or availability for use in an official proceeding or to otherwise obstruct, influence or impede any official proceeding. Any breach: 20 years in prison and/or a fine.

Table 2

Type of document	Retention period	Source of requirement
Public Company Financial Records	Six years minimum (requirement)/ten years (recommended)	S222 Companies Act 1985/Institute of Chartered Secretaries and Administrators guidance
Private Company Financial Records	Three years minimum (requirement)/ten years (recommended)	S222 Companies Act 1985/Institute of Chartered Secretaries and Administrators guidance
VAT Records	Six years (requirement)	Schedule II Value Added Tax Act 1994
Contractual Documents	Six years minimum (recommended)	Statutory limitation period for contractual claims is six years
Payroll and wage records	Six years (requirement)/ longer than six years (recommended)	Taxes Management Act 1970/Inland Revenue power to investigate for up to 21 years if allegations of fraud/negligence
Incorporation Documents, Board Minutes, Written Resolutions	Indefinitely (requirement)	Companies Act 1985 – various
Various FSA: *eg,* Money Laundering Records	Five years from end of relationship with client	Financial Services & Markets Act 2000/FSA Handbook

Susan Wildey
Solicitor, Technology & Outsourcing group
Tite & Lewis
susan.wildey@titeandlewis.com

Conferences/Training Weeks and Education Updates

International Events 2003/2004

2004 Conference/Training Week Calendar

	IS Audit & Control Training Week	Sarbanes-Oxley Symposium	International Conference	IS Audit & Control Training Week	Network Security Conference	Information Security Management Conference	IS Audit & Control Training Week
Dates	14-18 June 2004	17-18 June 2004	27-30 June 2004	28 June-2 July 2004	13-15 September 2004	13-15 September 2004	20-24 September 2004
Location	Seattle, Washington, USA	Dallas, Texas, USA	Boston, Massachusetts, USA	Boston, Massachusetts, USA	Las Vegas, Nevada, USA	Las Vegas, Nevada, USA	Amsterdam, The Netherlands
CPE Hours	38	12	47	38	25	25	38

For more information or to register, please visit the ISACA web site for the event of your choice.

For ISACA London Chapter events please refer www.isaca-london.org/events.htm

and for UK events providing discounts to ISACA members please refer www.isaca-london.org/conferences.htm

CHAPTER INFORMATION

ISACA London Chapter Board 2004/2005

Allan Boardman *President/Publications/Webmaster* allan@internetworking4u.co.uk	Nick Fellows Vice President/*Events* nick.fellows@barclays.co.uk	Joseph Wright *Secretary* joe-wright@supanet.com
Kevin Handscombe *Treasurer* kevin.handscombe@kpmg.co.uk	Charles Mansour *External Relations* charles.mansour@ntlworld.com	John Mitchell *Academia & Research* john@lhscontrol.com
John Hunter *Membership* jhunter@isaca-london.org	Mark Hughes *Certification* lcac@greenwich-trust.org.uk	Peter Andrews *Marketing* pandrews@isaca-london.org
Roger Southgate *IT Governance/Standards* southgat@nildram.co.uk	David Thirlwall *Datawatch Editor/Volunteers* dave.thirlwall@hmce.gsi.gov.uk	Christine Lyon *Chapter Administrator* admin@isaca-london.org
	Website www.isaca-london.org	

ISACA Northern UK Committee 2004/2005

Alan Rainford *President & Membership* alan.rainford@axa-insurance.co.uk 01253 662782	Robert Newbould *Vice President* bob.newbould@corusgroup.com 01724 402980	Ian Simpson *Treasurer* IanDSimpson@hbosplc.com 01422 334399
Stephen Sykes *Secretary* stephen.sykes@nhs.net 01625 661636	John Moore *CISA/CISM Co-ordinator* & Webmaster john.moore@axa-insurance.co.uk 01253 683504	Ray Butler *Past President* raymond.butler@highways.gsi.gov.uk 0161 930 5662
Mike O'Hara *Academic Relations* m.j.ohara@salford.ac.uk 0161 295 5665	Peter Thompson Committee Member peter.thompson@royalmail.com 01246 546547	Stephen Clark Committee Member stephen.clark@barclays.co.uk 07970 621312
	Website www.isaca.org.uk/northern	

ISACA Central UK Committee 2004/2005

Mike Hughes *President & Membership* *mike.Hughes@kpmg.co.uk* *0121 232 3207*	Jonathan Evans Vice President jonathan.evans@hfcbank.co.uk 0121 265 3832	Geoff Adey *Treasurer* *geoff.adey@kpmg.co.uk* 0121 232 3202
Ken Perry Secretary ken.perry@wolverhampton.gov.uk 01902 555612	Simon Parker *CISA Co-ordinator* *sparker@lowandbonar.com* *01476 564484*	Ross Patel CISM Co-ordinator ross.patel@afentis.com 01246 233893
James Whittaker Past President james.whittaker@bt.com 0121 230 2214	Les Bradshaw Committee Member les.bradshaw@dudley.gov.uk 01384 814853	Andrew Birkbeck Committee Member abirkbeck@deloitte.co.uk 0161 455 6852
Ed Jones Committee Member edward.jones@barclays.co.uk 01605 253 3985	*Website* www.isaca.org.uk/central	Richard Johnson Committee Member Richard@emailrj.freeserve.co.uk

ISACA Scotland 2004/2005

Stuart Middleton President stuart.middleton@morganstanley.com 01236 797872	Glen Bissett Secretary gbissett@audit-scot.gov.uk 0131 624 8447