ISACA®
Trust in, and value from, information systems
Scottish Chapter

Newsletter - May 2010

After a rather longer delay that usual, to say the least, here is the third all-electronic Chapter newsletter.

Members will almost certainly have noticed that the Chapter has been very quiet over the last year. As with everyone, the Committee have been busy with their professional workloads. As the economic environment appears to settle down, we hope to be able to get Chapter events up and running again. And, as we come up to the summer, we get going with an event covering database auditing, leading up to the annual training day - all free for members, of course.

You may see that there is a slight change in the Chapter logo, as seen at the top of the newsletter. As ISACA now offers a range of certifications and support for IT professionals, the look of the organisation has been updated slightly to reflect this. Members will be seeing a few more changes to ISACA's external face in the next few months, not least of all in the much-anticipated website relaunch (see www.isaca.org/redesign for more information on the new facilities that members will be able to take advantage of).

For future newsletters, the Chapter would like to encourage members to contribute opinion pieces, technical expertise and industry knowledge. One of the great strengths of ISACA is the pool of knowledge in the members, and nobody should forget that sharing knowledge can be worth valuable CPE hours - a comparatively easy way of gaining all-important experience for your recertification, at a time when training budgets are pared to the bone. If any member would like to lead a training event, or write a newsletter article on their area of expertise, then please contact the Committee using the details on the last page.

...news in brief...

ISACA announces "grandfathering" program for the new CRISC certification

...news in brief...

The first annual ISACA Risk/Reward Barometer survey shows that 45% of respondents say that the risks of cloud computing outweigh the benefits

...news in brief...

ISACA releases an exposure draft of COBIT 5, which incorporates the Val IT and Risk IT frameworks

...news in brief...

ISACA Scottish Chapter website awarded Gold Medal for design, content and management

...news in brief...

ISACA launches new Guidelines covering "Return on Security Investment" and "Continuous Assurance"

...news in brief...

ISACA certifies its 75,000th CISA

...news in brief...

Technology researchers Foote Partners identify CISA and CISM as part of the "21 Tech Certifications That Keep IT Workers In Demand"

...news in brief...

Contents

Presidential Cogitations

Tony Povoas

Spring has finally arrived and the economic outlook looks to be improving. In this improved context I am pleased to update that the Chapter has, since the last newsletter, been able to increase it's activity levels. This has included: the upcoming evening educational event on database auditing, the CISM revision school, attendance at the recent international ISACA leadership event and the planned forthcoming AGM, with a free-to-members all-day training event on IT governance and control standards...plus this newsletter. We have even developed agreements with the Council of Higher Education Internal Auditors and the Scottish Society for Computers and Law to share information and events of interest.

The Chapter is, as ever, reliant on volunteer effort for the organisation of these events and we would welcome contact from anyone who would like to get involved in helping further the Chapter and ISACA activities. Website maintenance and training event organisation are just two of the areas we could use assistance with.

If you are interested in getting involved please contact us through the website - you can find contact details for all of the Committee at www.isaca-scotland.org.uk - or through the e-mail addresses at the back of this newsletter. Members with any of the ISACA certifications can claim up to 10 CPEs for attending Committee meetings, plus additional CPEs for any additional work in supporting Chapter activities.

We look forward to seeing you at the forthcoming events and hopefully many more to come.

Tony Povoas
IT Security Manager, Virgin Money
president@isaca-scotland.org.uk

CISM preparation event

Rory Alsop

The 2009 Winter CISM exam preparation day took place on the 29 November 2009, with individuals from a range of banks with a Scottish presence braving the early winter cold with enthusiasm. After introductions and coffee, we began with a quick assessment to identify the areas in which attendees were weakest and focused on these for the rest of the day, through practice questions, roundtable discussions and some lively debate.

After the day the attendees were certainly more confident than at the beginning, and had a better grasp of the types of questions which were likely to turn up in the exam - and this was subsequently reflected in the excellent pass rate.

As this is an interest-driven day, the Chapter will be looking to hold another event in advance of the 2010 Summer CISM exam, if enough individuals are interested. This preparation event will probably be held at the end of May.

Interested candidates should e-mail cism@isaca-scotland.org.uk for more information on this proposed event.

Call for articles

Guy Lomas

This newsletter aims to provide members with a range of articles covering every aspect of IT governance, from IT audit to information security, from governance to risk management and even covering job advice. However, this does depend on the support of Chapter members, who can share their knowledge and experience with other ISACA members.

The Committee would welcome contributions from members on any aspect of information systems management. Technical guidance on some of the more specialist areas of IT would be especially well received.

All contributions qualify for CPEs, based on the time spent preparing the article, to be used against annual CISA, CISM and CGEIT renewals.

If you have any questions on content, format or how to develop an article, please contact newsletter@isaca-scotland.org.uk for more information.

ISACA updates

Brian Frankel

Research Update

The Monitoring of Internal Controls and IT publication provides guidance and tools for enterprises interested in applying IT to support and sustain the monitoring of internal control systems and IT. It provides practical guidance for executing the monitoring process in general and for automating the monitoring process for increased efficiency and effectiveness. Effective IT-enabled monitoring can be of benefit to senior management, which includes governance bodies, the audit committee and the board of directors. Customization of the approaches provided will be necessary to reflect the specific circumstances of each enterprise.

An exposure draft is posted at www.isaca.org/itmonitoring for public comment.

ISACA's New Web Site

ISACA International Headquarters is working with Chapters to better align their online presence. Chapters play a pivotal role in the organization, giving support to members at a local level. ISACA will be supporting Chapters by including the following in the new web site:

- Unified log-in - The ability to use your ISACA login credentials on the local Chapter web sites
- Localised and translated content
- Chapter events and announcements personalised for members
- A map to quickly locate other Chapters around the world

Launching in 2010, the renovated ISACA web site is an exciting advancement. Visit www.isaca.org/redesign for additional information.

Distance Learning Update

ISACA is currently enhancing and restructuring its online training program to meet the training needs of ISACA's global membership. The online COBIT Foundation Exam is now available in English, Spanish, Portuguese, French and Japanese on the ISACA e-Learning Campus. The revised online COBIT Foundation Course, complete with an updated case study, will be available in the second quarter of 2010. Please visit www.isaca.org/elearning for the most current information regarding enhancements and availability dates.

CISA Job Practice Analysis

An analysis is in process to update the Certified Information Systems Auditor (CISA) job practice to reflect the vital and evolving responsibilities of IT auditors and to stay current with the market. The first exam to reflect the results of this analysis will be the June 2011 exam. For more information, please visit www.isaca.org/cisajpa.

CISA, CISM and CGEIT Exam Registration

The final registration deadline for the June CISA, CISM and CGEIT exams was 7 April 2010. Potential candidates should refer to www.isaca.org/cisaboi, www.isaca.org/cismboi or www.isaca.org/cgeitboi, respectively, for more details.

June Exam Changes and Deferrals

For those registered for the June exam, there is no charge for changes to registration information, such as exam site or language, up to 16 April 2010. $50 will be charged for all changes to exam registrations received between 17 and 23 April 2010. No changes will be accepted after this date. Questions or change requests should be directed to exam@isaca.org.

Registered candidates unable to take the exam in June may request a deferral of their registration fees to the next exam date. Deferral requests received on or before 23 April 2010 will be charged a $50 processing fee. From 24 April until 27 May 2010, $100 will be charged. No deferrals will be accepted after this date. Candidates should visit www.isaca.org/examdefer for more information.

CISA, CISM and CGEIT Applications

To process applications more efficiently, exam passers should gather all application documentation and send it in one package to ISACA International Headquarters. Completed applications may be sent via fax to +1.847.253.1443 or via e-mail to certification@isaca.org. Those wishing to send applications via post may use the address listed on the application.

CISA, CISM and CGEIT Certification Renewals

Certificate holders, who have not already done so, should renew and report CPE hours as soon as possible to avoid revocation.

Risk and the business model

Charlie Meehan

The organisation's business model is a framework concept for business strategy, and the concept of mapping the risk in the model has been taken up by Governance, Risk Management and Compliance (GRC) practitioners as a way of holistically identifying and managing risk in relation to IT as the fundamental delivery mechanism for businesses with global reach[1].

The current economic climate is expected to continue to test the robustness of business models and their delivery systems, and this type of risk may not be well-represented in current audit thinking (outside of the rather fuzzy "going concern" test applied in the audit of the statutory accounts). It does offer, however, another way into the conversation with business leadership about potential sources of added value from our audit and control activities, because it allows a common reference point as a starting point for the discussion.

Risk

The basic vocabulary of the risk discussion is commonplace across so many domains - not just audit but HR, Training and management thinking generally - that it can be assumed[2] everyone understands the basic risk equation:

RISK = IMPACT X PROBABILITY

The experience of the recent financial drama has, however, also alerted us to the need to weight this view of risk by taking account of Risk Appetite[3] [4], and it would be better expressed as:

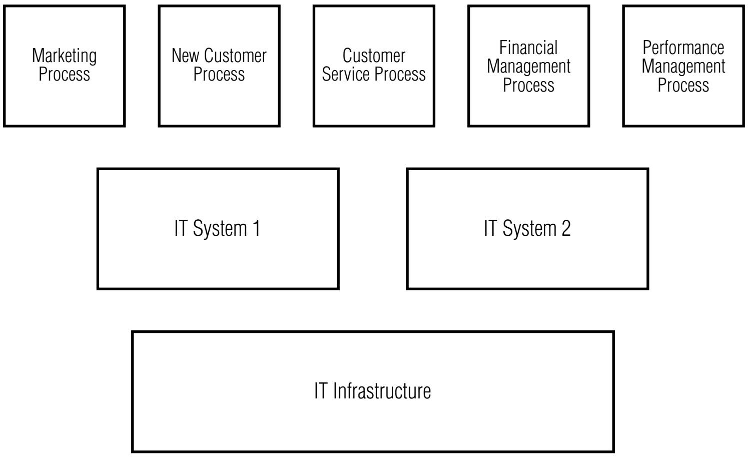
RISK = IMPACT X PROBABILITY X RISK APPETITE

Business model

Although it is often less visible internally than it should be, the business model encapsulates Critical Success Factors (CSF) for the growth of the business. So, for a telecoms provider, the drivers may be acquisition of new subscribers and managing reduced loss of existing subscribers, while in food retail they may be the efficiency of the logistic process and the attractiveness of the prices. Achieving CSFs will, in turn, depend on directly supporting business processes such as marketing, product development and supplier contract negotiation. Underpinning all these will be basic capabilities for the business in terms of people, processes and technology. In order to monitor and measure, there will be Key Performance Indicators (KPIs, for those processes directly linked to the CSF) or performance indicators (for business as usual activities, whose baseline performance is assumed)[5].

For a particular business, the company's strategy and investment priorities can be found in its shareholder communications and statutory reporting, and will reflect the company's CSF and KPIs. Commentary in the business press will often focus on any concerns about perceived shortfalls in capability, as well as delivery against the business model from the perspective of potential impact on shareholder value and prospective dividend performance.

IT will be a key enabler of both the business processes and the KPI reporting, so framing audit plans in terms of risk assurance around these two aspects will align with business priorities at both the strategic and delivery levels. As we auditors like to flowchart, a simple initial mapping between the processes delivering the CSF and the underlying IT systems can be a useful entry point to the planning process:



Risk appetite

How easy is it to get anyone to admit to having a risk appetite, or to specify its parameters?

Risk appetite can be usefully thought of in terms of the trade-offs implicit in choices. All real world systems involve such trade-offs and their absence, in explicit terms of specifications and descriptions, indicates a source of weakness; if not recognised and managed, they suggest either a lack of knowledge or an attempt to ignore what are potential vulnerabilities and threats.

Their explicit recognition, on the other hand, helps to quantify risk appetite as there are opportunity costs in executing low return processes, as well as risk-weighted benefits from engaging in higher risk strategies.

Impact

How well are potential impacts identified and how easy is it to quantify them?

A top-down approach allows us to ensure completeness of coverage while a bottom-up approach draws on the expertise of domain specialists and helps us to avoid overlooking significant consequences that might be well-known to insiders, but not referred to in higher level documentation because they are normally prevented or detected.

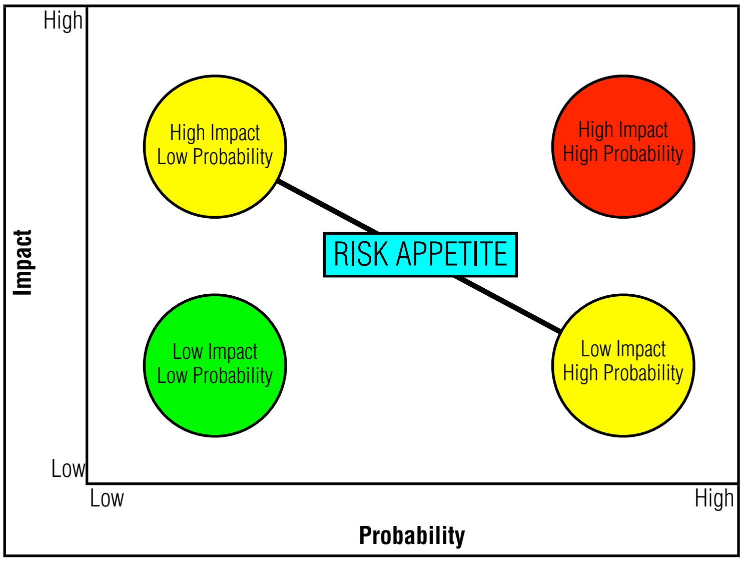
Probability

How much business activity can be described as "duck-like" - the placid surface hiding frantic thrashing around?

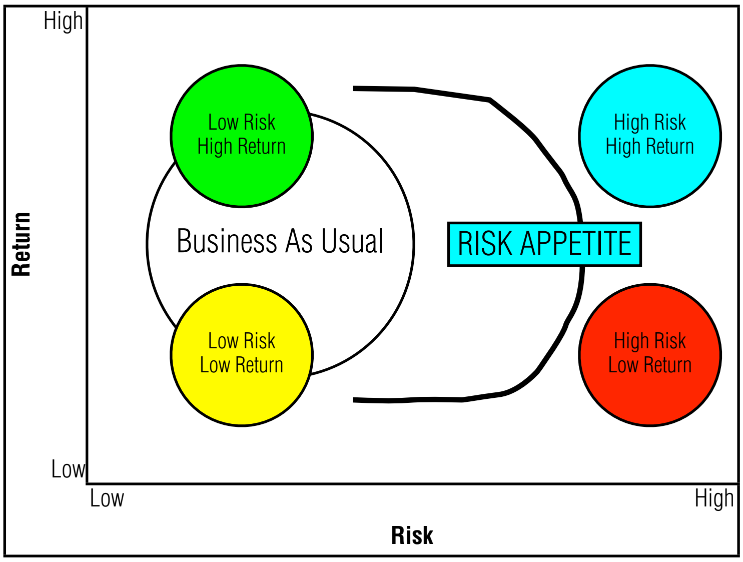
Information based only on recorded frequency can be actively misleading if it excludes near-misses and successful control interventions. This is a universal experience of operational reporting, but may leave us unable to evaluate how often the interventions were "heroic" rather than routine; only the latter can be relied upon to establish a baseline. It can mean, for instance, that the reported frequency of potentially significant impacts is understated - no one boasts about the bad things which nearly happened.

The following simple graphics illustrate some of these relationships.

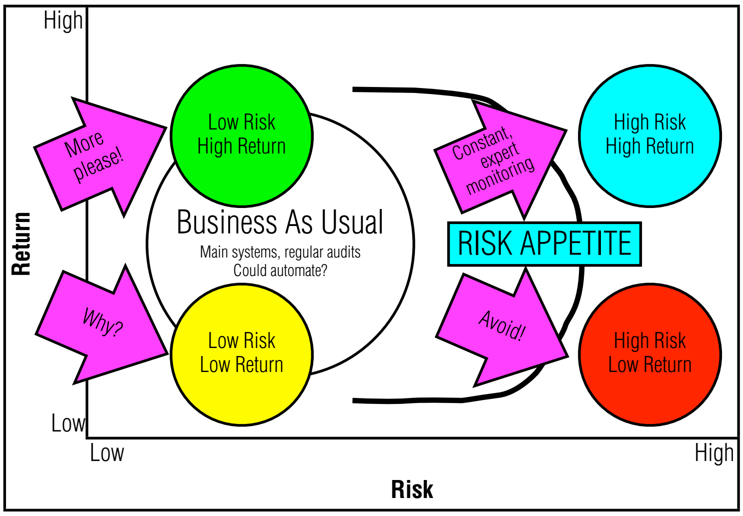
Mapping risk appetite to impact and probability:


High
Impact
Low
High Impact Low Probability
High Impact High Probability
RISK APPETITE
Low Impact Low Probability
Low Impact High Probability
Low
High
Probability

Mapping risk and return to activities:



Mapping activities to strategy:



One point to consider is that all these considerations are filtered through perception processes in individuals and groups, which are already compromised by cognitive biases[6]. After all, many of the financial sector business practices which resulted in "toxic debt" were, even as recently as 2005, regarded as low risk and even a bit nerdish – they had become part of "Business As Usual" , that part of the business that is assumed to be safe and well-controlled, and which becomes the building blocks of the new strategy.

Charlie Meehan
Treasurer, ISACA Scottish Chapter
treasurer@isaca-scotland.org.uk

References

[1] bit.ly/riskbusmodel1 (Search Compliance)
[2] bit.ly/riskbusmodel2 (AuditNet)
[3] bit.ly/riskbusmodel3 (Blogspan - Press Releases)
[4] bit.ly/riskbusmodel4 (IT Governance Institute)
[5] bit.ly/riskbusmodel5 (David Parmenter)
[6] bit.ly/riskbusmodel6 (Social Affairs Unit)

Data security and third party suppliers

Arthur Aitken

The 2009 Chapter AGM and training event took place on 9 June 2009, at The Royal Society Edinburgh, titled "Data Security and Third Party Suppliers".

The event was presented by Stan Dormer of Mindgrove Consulting and, in line with year-on-year trends, was attended by the highest attendance for these events, with just under 70 members and non-members.

The theme of the day was the auditing of third party contracts with the pattern for the event split into three distinct areas, namely:

- Issues – before you sign the contract
- Newly implemented third party contracts
- Mid to late maturity contracts

The presentation asked attendees whether the following statements are familiar:

> *"We wish that we had let the Contract for a shorter period of time, as our business focus changed during the Contract and we required, essentially a more flexible type of service"*
>
> *"We wish that we had investigated the market more thoroughly as we discovered, later, that our Service Provider had more limited experience than we had hoped for"*
>
> *"We wish that we had looked at the Contract in more detail, as we discovered – when the bills started to come in – that we were being billed for activities that, previously, we had never been consciously aware of when we performed the work ourselves"*
>
> *"We wished we had retained more expertise, as we discovered after three years that the Service Provider knew more about the business than we did"*

The bulk of the day was spent discussing the pre-contract phase, simply because this is the most important phase in any contract award: get this right and the rest should be "plain sailing".

Or that is the theory. "Plain sailing" is definitely not a term that can be applied to the operation of a formal agreement between contracted parties. Contracts, particularly between large business entities, can often be lengthy in terms of pages and use a specific type of language in their make up but, as with pretty much everything else in life, a common-sense approach can be applied to reviewing contracts to ensure they include appropriate controls and provisions that will be mutually beneficial to all parties involved.

Once the contract has been signed and is implemented, the main tasks associated with its operation are management and monitoring of performance and service level management. To this end, the right to audit and inspect is a key requirement that should be included in the contract at the outset. Also, in order to enable ongoing monitoring and management of the services being provided, clauses covering the agreed levels of service to be provided (and the implications of failure to deliver), as well as a definition of how the parties communicate and cooperate with each other, should be included. Another important factor is the establishment of ownership of intellectual property (i.e. who owns what).

The event concluded by covering the topic of mid to late maturity contracts, preparation for contract end and contract termination. Included within this were such items as disputes, arbitration and the different termination states and third-party funding withdrawal – all in all, another very interesting and informative day.

I have attended all but one of the annual training days in recent years and I have found every one that I attended to be extremely interesting and informative. The subject matter has been varied and has covered such diverse subjects as Network Auditing, Website Security and Auditing, Security Threats and Trends and even a brief look in 2008 at Espionage and Data Gathering.

The Chapter Committee always manages to deliver the goods when it comes to the annual training day and I would encourage members to try and get along, if not to more of the Chapter events, then certainly the annual training day. Remember, all Chapter events are generally free to members.

Arthur Aitken
Website Manager, ISACA Scottish Chapter
webmaster@isaca-scotland.org.uk

Attack vectors: the user is the weakest link

Charlie Meehan

This item is a round-up of links from the internet on vulnerabilities and the options for protection (as well as the emergent counter-attacks to the protections).

As the title indicates, the main risk lies with the user and their awareness – whether what is advised is heard, understood and implemented.

People Matter the Most
http://jeremiahgrossman.blogspot.com/2008/01/technology-helps-but-people-matter-most.html

Mindgames Continue
http://thesocialgraphofmalware.com/home/mindgames-continue/

Data at Rest, Data in Transit, Data in Use
http://padraic2112.wordpress.com/2007/07/26/data-at-rest-data-in-transit-data-in-use/

Moving on to practicalities, there are many good practices that should be adopted by both corporate entities and private individuals, including full hard disk encryption, management of boot settings in the BIOS, protection of backup media and provision of a recovery path for random hardware failures.

Harden Your Laptop
http://blog.rootshell.be/2009/01/13/new-corporate-laptop-setup/

Hardening Windows Security
http://www.malwarehelp.org/malware-prevention-hardening-windows-security1.html

Late-Breaking Computer Attack Vectors
http://www.pauldotcom.com/LBCAV-SEPTEMBER2008.pdf

http://www.pauldotcom.com/presentations/LBCAV-FEB2008.pdf

Given these good practices, are they be vulnerable to attacks? And, if so, how should we respond?

New Research Result: Cold Boot Attacks on Disk Encryption
http://www.freedom-to-tinker.com/blog/felten/new-research-result-cold-boot-attacks-disk-encryption

Defense-in-Depth vs. BitUnlocker: How to defeat Cold DRAM attacks
http://blogs.technet.com/staysafe/archive/2008/02/24/defense-in-depth-vs-bitunlocker-how-to-defeat-cold-dram-attacks-using-bitlocker-power-options-and-physical-security.aspx

Encrypting Your Hard Disk is Not Safe Anymore
http://www.andhranews.net/India/2008/September/1-Encrypting-Your-Hard-61606.asp

Using Kon-Boot from a USB Flash Drive
http://www.irongeek.com/i.php?page=security/kon-boot-from-usb

http://www.raymond.cc/blog/archives/2009/05/11/burn-iso-image-to-usb-flash-pen-drive-kon-boot-to-usb/

http://www.piotrbania.com/all/kon-boot/

Home PCs, used to provide gateways to the corporate network, have additional vulnerabilities.

Home router hacks, VOIP phishing and drive-by pharming
http://blogs.technet.com/staysafe/archive/2008/01/24/home-router-hacks-voip-phishing-driveby-pharming.aspx

Drive-by pharming in the wild
http://www.symantec.com/connect/blogs/drive-pharming-wild

Protecting Yourself On potentially hostile networks
http://www.irongeek.com/i.php?page=security/hacker-con-handout

The “Cafe Latte” Attack - ToorCon 09
http://www.security-freak.net/toorcon/cafe-latte-wireless-attack.html

http://www.security-freak.net/toorcon/Toorcon.ppt

Those cool wireless headsets keep your hands free - but they also give hackers the ability to eavesdrop on your conversations
http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=208803553

Bluetooth security resources
http://bluetooth.shmoo.com/

Beyond security, there are still concerns with privacy and reputation.

Biometric sensors beaten senseless in tests
http://www.theregister.co.uk/2002/05/23/biometric_sensors_beaten_senseless/

Myspace - an example in cyber insecurity
http://www.shmoo.com/~gdead/pres/WestPoint-Castle-shmoo.ppt

Can short URL sites and Twitter together be attack vectors?
http://blog.red7.com/can-short-url-sites-and-twitter-together-be-attack-vectors/

The biggest security hole on the Web?
http://www.webpronews.com/topnews/2009/08/13/the-biggest-security-hole-on-the-web

This article will self-destruct: A tool to make online personal data vanish
http://uwnews.org/article.asp?articleID=50973

Finally, we need to be aware that the most protected data may end up inaccessible to anyone, including the user! Always remember to prepare backups and, if necessary, a “Rescue CD” that will allow you to get back into your computer.

Charlie Meehan
Treasurer, ISACA Scottish Chapter
treasurer@isaca-scotland.org.uk

Chapter and Local Events

13 May 2010

ISACA Scottish Chapter evening event: Database Auditing: How Does it Protect Me? (2 CPEs)

Ernst & Young, Ten George Street, Edinburgh
Lindsay Hamilton, CEO, Cervello Consultants

20 May 2010

Scottish Society for Computer and Law event: Virtualisation

Burness, 50 Lothian Road, Edinburgh
Neil Davison, Head of Virtualisation, Dell UK
For more information about SSCL events and to register, contact sscl@ccwlegal.co.uk

2 June 2010

ISACA Scottish Chapter: AGM

ISACA Scottish Chapter training event: A Standards-Driven Approach to IT Governance and Control (7 CPEs)

Royal Society of Edinburgh, George Street, Edinburgh
Stan Dormer, Mindgrove

12 June 2010

CISA, CISM and CGEIT exams, to be held in Edinburgh

e-Symposium - available at www.isaca.org/webcasts

27 April 2010

Fighting Security Threats Head On (3 CPEs)

Jeffrey Ritter, CEO, Waters Edge Consulting (Moderator)
Leighton Johnson III, COO & Senior Security Engineer, ISFMT
Richard Hollis, CEO, Orthus Ltd
Larry Seltzer, Security Analyst, VeriSign
Jasvir Gill, CEO, AlertEnterprise Inc
Aleese Eckenrode, Education Coordinator, ISACA

Archived e-Symposia - available at isaca.brighttalk.com/recorded-events

ISACA Events - more details at www.isaca.org/conferences

24-28 May 2010

ISACA International Training Week (up to 38 CPEs)

The Westin Charlotte, Charlotte, North Carolina, USA

6-9 June 2010

ISACA International Conference (up to 40 CPEs)

JW Marriott Cancun Resort & Spa, Cancun, Mexico
Casa Magna Marriott Cancun Resort, Cancun, Mexico

13-15 September 2010

Information Security and Risk Management Conference (up to 32 CPEs)

Caesars Palace, Las Vegas, Nevada, USA

To contact the ISACA Scottish Chapter

Tony Povoas (President) - president@isaca-scotland.org.uk
Rory Alsop (Vice President) - vpresident@isaca-scotland.org.uk
David Meadley (Secretary) - secretary@isaca-scotland.org.uk
Charles Meehan (Treasurer) - treasurer@isaca-scotland.org.uk
Alan Rennie (Membership) - membership@isaca-scotland.org.uk

For more information about this newsletter, or to contribute articles

Guy Lomas (Newsletter Editor) - newsletter@isaca-scotland.org.uk