



## ISSIG presents: ***Are you up-to-date? A fresh look at Information Security regulation.***

Wednesday 11<sup>th</sup> May 2011

The May 2011 event will be at Missenden Abbey, Bucks, HP16 0BD

### ***Speakers will cover:***

- ✓ ***“ISO 27001/2” – how can this benefit your organisation? What are the advantages and disadvantages of implementing such a standard?***  
*[Presenter – Mark Towler/Martin Brooks, Deloitte]*
- ✓ ***“PCI - an update” – What are some of the challenges facing the industry today? What methodologies are available to help you? Why audit and maintain so much when you don't have to?***  
*[Presenter – Simon Sharp, illumis]*
- ✓ ***“The Tao of the Data Protection Act” – What is the essence of the Data Protection Act? Where did it come from and why is it important?***  
*[Presenter – Richard Hollis, Orthus Ltd]*
- ✓ ***“But what about the technology?” – What are the typical technologies that an organisation needs to have in place to provide protection from unauthorised attack?***  
*[Presenter - Leon Ward, Sourcefire]*

**Delegate Fee: £65 (£60 for 2 or more delegates)**

*(Fee includes refreshments, lunch, car parking)*

**Please note that places are limited and will be offered on a ‘first come first served’ basis.**

**Location:** Missenden Abbey Conference Centre,  
Great Missenden, Bucks, HP16 0BD

**Date:** Wednesday 11<sup>th</sup> May 2011

**Time:** 9:30 – 4:00

### **Contact Details:**

Email: [issig\\_committee@msn.com](mailto:issig_committee@msn.com)

### **ISSIG Web information:**

[http://www.iaa.org.uk/en/membership/Special\\_Interest\\_Groups/Information\\_Security.cfm](http://www.iaa.org.uk/en/membership/Special_Interest_Groups/Information_Security.cfm)

The Information Security Special Interest Group (ISSIG) provides a forum for internal auditors and security professionals to discuss topics related to information security, ISSIG is affiliated to the IIA - UK and Ireland. We have organised a one-day event that will be of interest to all internal auditors and security professionals. The event will offer an ideal opportunity to network with fellow professionals from both public and private sectors.

09.30 - 10.00	Registration and Refreshments	
10.00 - 10.15	<p><b>Introduction from the Chair</b></p>	<p><b>Arnie Bates, ISSIG Chair</b></p> <p>Arnie is the Information Security Officer for Unum Limited, an income protection insurance provider.</p> <p>Arnie's experience in Information Security spans more than 10 year including IT Audit Manager at Air Products. He holds the CISA, CISM and CGEIT accreditations with the ISACA organisation. He is also a Certified Information Systems Security Professional (CISSP) with the ISC<sup>2</sup> organisation and holds a qualification in forensic investigation techniques from a leading forensics company in Oregon, USA.</p>
10.15 - 11.15	<p><b>Session 1: ISO 27001/2 – The implementation process and how Audit can provide input</b></p> <p>The presentation will cover what is ISO 27001/2 and how can it benefit your organisation. The presentation will give an overview of ISO 27001/2 and consider the advantages and disadvantages of implementing such a standard. It will also look at how it can be implemented in-house and what role Internal Audit can play.</p>	<p><b>Mark Towler / Martin Brooks, Deloitte</b></p> <p>Mark is a General Manager at Deloitte with the responsibility for the provision of IT Audit Services to the Public Sector. He has over 28 years experience in both General and IT Audit and holds the CMIIA and QiCA qualifications. Mark is a Lead Auditor in BS7799 (Original version of ISO27001), which he obtained in 2001.</p> <p>Martin is a Senior IT Audit Manager at Deloitte and has over 14 years experience in IT Audit and holds the CiSA and QiCA qualifications. He has also been a BS7799 Lead Auditor for ten years, which he converted to ISO27001 in 2005.</p>
11.15 – 11.30	<p><b>Break for Refreshments</b></p>	
11.30 – 12.30	<p><b>Session 2: PCI – an update</b></p> <p>This session will cover the PCI Data Security Standard. What are some of the challenges facing the industry? What are the current methodologies to help the organisation and auditor achieve, maintain and validate PCI DSS compliance?</p> <p>Simon will discuss some of the dialogue he is currently involved in, with respect to the VISA TIP (Technology Innovation Programme) bulletin, which was announced in Feb 2011.</p>	<p><b>Simon Sharp, illumis</b></p> <p>Simon has worked in IT for over 15 years, specialising in information risk, protection, security and continuity. Simon is a founding director of illumis, a Qualified Security Assessor (QSA) company established to provide superior assistance in payment security, reducing costs and helping clients achieve compliance with maximum efficiency.</p> <p>Prior to founding illumis, Simon was a senior consultant with three leading information security consultancies delivering innovative solutions to a global client base. As head of information technology at a division of Motivcom plc he took the company through PCI DSS compliance so knows only too well the challenges faced by organisations trying to achieve compliance. Before that Simon has had years of management and consulting experience within financial services. A role as a system architect in the defence sector saw Simon's work shortlisted for a technology innovation award.</p> <p>As well as Simon's role as a consultant and director he is a certified forensic practitioner who actively participates in the Security Standards Council specialist interest groups (SIGs) that are helping to shape emerging compliance standards and technologies.</p>

12.30 – 13.30	<b>Lunch</b>	
13.30 – 14.30	<p><b><u>Session 3: The Tao of the Data Protection Act</u></b></p> <p>What is the essence of the Data Protection Act? Where did it come from and why is it important? What are the real objectives of the 8 Principles that comprise the Act? How do you design, establish and audit a program to achieve these objectives? This presentation plainly states the baseline documentation and day-to-day operational requirements associated with implementing and overseeing a cost-effective DPA compliance program.</p>	<p><b><i>Richard Hollis, CEO Orthus Limited</i></b></p> <p>Richard Hollis is the Chief Executive Officer for Orthus Ltd, a European information security risk management consulting firm specialising in providing effective, independent information risk management services. As a Certified Information Security Manager (CISM), Certified Protection Professional (CPP) and a Payment Card Industry (PCI) Qualified Security Assessor (QSA), Richard possesses extensive hands on skills and experience in designing, implementing and managing and auditing information security programs.</p> <p>Over the course of his career Richard has served as Director of Security for Phillips, Paris, and Deputy Director of Security for the US Embassy Moscow Reconstruction Project as well as a variety of sensitive security positions within the US government and military. In addition to his work with Orthus, Richard serves on several security technology company boards and security industry advisory councils.</p> <p>A celebrated public speaker, Richard has presented to hundreds of audiences across the world on a wide variety of information risk management topics and techniques. As a recognised industry authority, he has published numerous articles and white papers. He has also appeared on national and international broadcast news as well as being cited in a wide range of press including the BBC, MSNBC, Radio 4, the Financial Times, Time magazine and various others.</p>
14.30 – 14.45	<b>Break for Refreshments</b>	
14.45 – 15.45	<p><b><u>Session 4: But what about the technology?</u></b></p> <p>Leon will discuss the typical technologies that an organisation needs to have in place to provide protection from unauthorised attack. In many cases, (especially for PCI), there are regulatory expectations that these technologies are kept up-to-date, but how can an auditor or Information Security professional verify that the end-point technologies are matched to the risk-appetite of the organisation?</p>	<p><b><i>Leon Ward, Sourcefire.</i></b></p> <p>Leon Ward works as a field marketing manager for Sourcefire. Prior to joining Sourcefire, Leon was involved in the design and development of SNORT® based Intrusion Prevention Systems.</p> <p>Leon applies his strong background in UNIX security and protocol analysis to overcome the challenges of network security monitoring in the enterprise, specifically in the areas of network intrusion detection, threat mitigation, event analysis and vulnerability assessment.</p> <p>In the little spare time Leon finds, he is one of the lead contributors to the open source network traffic forensics project OpenFPC (Open Full Packet Capture).</p>
15.45 – 16.00	Closing remarks from the Chair & opportunity for further questions	

**Event:** Are you up-to-date? A fresh look at Information Security Regulation.

**Date:** Wednesday 11<sup>th</sup> May 2011

**Missenden Abbey Conference Centre, London Road,  
Great Missenden, Buckinghamshire, HP16 0BD**

**Venue:** See reception on arrival. Car parking is included in the delegate fee

Please visit the website for travel options and directions to Great Missenden. <http://www.missendenabbey.co.uk/how-to-find-us/>

**Person making booking**

**Title:** Mr/Mrs/Ms/Miss

**Job title:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Department:** \_\_\_\_\_

**Company:** \_\_\_\_\_

**Telephone:** \_\_\_\_\_

**Address:** \_\_\_\_\_

**Fax:** \_\_\_\_\_

\_\_\_\_\_

**E-mail:** \_\_\_\_\_

\_\_\_\_\_

**Post code:** \_\_\_\_\_

**Invoice required:** Yes/No

Please reserve places for the following delegate(s):

	Title	First name	Surname	Job Title	Special requirements (e.g. food/access)
1					
2					
3					
	<b>Payment due:</b>		<b>Cost per person £</b>	<b>Total amount</b>	<b>Paying by (please circle / highlight)</b>
	For 1 attendee		@ £65 Each =		
	For 2 or more attendees		@ £60 Each =		
			<b>Total £</b>		
					Direct Payment / Cheque

**All completed booking forms** should be e-mailed to [ISSIG Committee \[issig\\_committee@msn.com\]](mailto:issig_committee@msn.com)

**Payment Instructions:**

Two payment methods are available:

**Direct payment.** Our preferred payment method is direct payment into the ISSIG bank account (see below for account information) covering the Total amount above plus any applicable bank charges.

*HSBC Bank [Account Number: 61424432. Sort code: 40-04-12]*

*International Bank Account Number [GB93MIDL40041261424432. Branch Identifier Code: MIDLGB2110F]*

**Cheque** payments made payable to 'ISSIG'. Please **post** your cheque and a **copy** of your completed booking form to:

**Maureen Simmons, Audit Manager, Buckinghamshire County Council, Audit and Risk Management, Room 128 Old County Offices, Walton Street, Aylesbury, Buckinghamshire, HP20 1UD.**

**DATA PROTECTION**

By returning this form you consent to our processing your sensitive personal data (such as dietary requirements or health data) for the above purposes. If you have given us information about another/other person/s you confirm that they have appointed you to act for them, to consent to the processing of their personal data, including sensitive personal data, to the transfer of their information abroad (if necessary) and to receive on their behalf any fair collection notices. You (and they) have a right to ask for a copy of your information and to correct any inaccuracies.

**TERMS AND CONDITIONS OF BOOKING**

**Application**

1. These Terms and Conditions apply to the ISSIG Event to be held on 11<sup>th</sup> May 2011. All bookings should be made on ISSIG's booking form and sent with a cheque (or direct payment into the bank account provided) in full payment of the event fee. Bookings must be made by 9<sup>th</sup> May 2011. Companies that require an invoice in order to raise a cheque should forward the completed booking form with a statement of intent to pay the fee on receipt of the invoice.

**Fees**

2. The cost includes lunch, refreshments and all conference documentation provided by ISSIG.
3. Please make cheques payable to "ISSIG" or make a direct payment into the ISSIG bank account (details provided). An email confirmation will be sent to you prior to the event.

**Changes**

4. No refund for event fees will be available after Friday 29<sup>th</sup> April 2011. However, a substitute delegate will be very welcome at any time, at no additional cost.
5. The Committee reserves the right to change the venue subject to reasonable notice and substitute topics or speakers. The ISSIG Committee also reserves the right to cancel the event at their discretion, in which case attendees will be notified and all monies received will be refunded in full.

**Liability**

6. The Members of the ISSIG Committee accept no liability for any loss or damage suffered to delegates or their property.
7. Although the programme has been compiled in good faith, the content of each Speaker's presentation has been created independently and, as such, the ISSIG Committee cannot accept any responsibility for the content and any consequences ensuing from the application of such content. Delegates should take specific advice when dealing with specific situations. Opinions expressed are those of individual speakers and not of the ISSIG Committee.