AGENDA:
ISO27001:2013, PCI DSS v3 and CES v1.0:
New standards in the global cyber war
(Churchill War Rooms, London, 8 May 2014)

www.itgovernance.co.uk

Time	Session
8:30 - 9:30	Registration Tea and coffee Networking
9:30 - 10:15	**Welcome and introduction**: **Alan Calder, Founder and Executive Chairman of IT Governance,** explains why cyber security matters to the payment card industry and businesses worldwide. Cyber crime is on the rise and represents a serious threat. What are the best ways for an organisation to be cyber resilient, and how can you best address the requirements of PCI DSS? Alan is a leading authority on information security and IT governance. He is also founder and executive chairman of IT Governance, the Cambridgeshire-based, single-source provider of products and services for IT governance, risk management and compliance. His talk will focus on governance of cyber security: people, process and technology, and why organisations need to manage cyber security using best practice to protect data and market share.
10:15 - 11:00	**Keynote speech: Neira Jones** has more than 20 years' experience in the financial services market, directing global change programmes, launching new products/services and managing process reengineering practices. She will be addressing the topical theme of: **"The Global Cyber War: Using ISO27001:2013 and PCI DSS version 3 to drive business, cost and security improvements".**
11:00 - 11:15	**Tea/coffee break** Meet Neira Jones and Alan Calder in the Harmsworth Room
11:15 - 11:30	**Mike Edwards**, BSI Management Systems Tutor, BSI. **Achieving 'Business As Usual' in the Face of Cyber Threats**: Positioning ISO27001:2013 and ISO22301 certifications strategically within your business to achieve 'cyber resilience'. Suzanne will share some best practices observed as companies undergo accredited certification, helping you and your clients derive the maximum cost-effective benefit when implementing two of the most widely adopted management system standards.

11:30	**-**	**12:00**	**Merging Information Security Standards**: Bridget Kenyon, Head of Information Security, University College London, on how to align and reconcile the different information security standards. Organisations already know that they have to adopt these standards (including PCI DSS v3, the IG Toolkit, ISO/IEC 27001:2013, etc.), so the aim is that the resulting approach is greater than the sum of its parts.
12:00	**-**	**12:20**	**Nick Wilding**, Head of Cyber Resilience, AXELOS. **Delivering Business Value Through Cyber Resilience Best Practice.** AXELOS, a global leader in best practice and owner of ITIL® and PRINCE2®, is developing a Cyber Resilience Global Best Practice portfolio. Cyber resilience policies, standards and guidance continue to be published, but organisations are still searching for the right, pragmatic way to ensure these play an integral part of their day-to-day business operations. Nick will outline the approach that AXELOS is taking in developing its new portfolio and how it will help you deliver value across the organisation.
12:20	**-**	**12:40**	**Sarb Sembhi** is the **Chair of ISACA's Government and Regulatory Advocacy Regional Subcommittee for the area of Europe/Africa.** He will present his views on cyber security best practice and how COBIT®5 aligns with ISO27001.
12:40		**13:00**	**Richard Bach, Assistant Director - Cyber Security, Department for Business, Innovation and Skills,** will bring news about the **UK Government Cyber Essentials Scheme.** Following on from the BIS Call for Evidence on a preferred organisational standard for cyber security conducted last year, industry representatives and BIS have collaborated on the development of a scheme for basic technical protection from cyber-attacks. The Scheme comprises a set of requirements for technical controls, and a draft assurance framework on which BIS are seeking feedback. Richard will outline how the Cyber Essentials Scheme identifies the security controls that organisations must have in place within their IT system in order to have confidence that they are beginning to mitigate the risk from internet-based threats. He will answer your questions and be available to speak to delegates over lunch.

13:00	**-**	**14:00**	**Buffet lunch and networking** During the lunch break, delegates will be able to see and join in on live demonstrations of ethical hacking and penetration testing services. (NOTE: There will be a PRESS BRIEFING, 13:15 – 13:45)
14:00	**-**	**14:30**	**Geraint Williams, Senior Consultant and PCI QSA, IT Governance**, on **Security as 'Business as Usual' - a recommendation of the PCI DSS v3**. The PCI SSC said the changes introduced in version 3.0 are designed to help organisations take a proactive approach to protect cardholder data that focuses on security, not just compliance. The changes will make gaining certification to PCI DSS an exercise in security as business-as-usual best practice. Geraint will discuss the changes between v2 and v3 of the PCI DSS, and what you need to know to focus on security as more than just an annual compliance exercise.
14:30	**-**	**15:00**	**Steve Watkins, Director, IT Governance** will discuss **The Cyber Security Challenge**: which standards/methodologies do you need to adopt to be safe? Steve will look at the changing standards environment in which UK businesses find themselves. How can these standards combine to address the existing and further developing cyber security threat? Steve will also discuss the requirements of the ISO27001:2013 information security standard that was published in October 2013 and reflect on the HM Government Cyber Essentials scheme.
15:00	**-**	**15:15**	**Tea/coffee break** Live demo of **penetration testing and ethical hacking**. Relax, sip a cup of tea or coffee, and watch how easy it is to break into a supposedly foolproof security set-up!

15:15	**-**	**15:45**	**Demonstration of Boldon James Classifier** ISO27001-compliant security software. Why use classification software? Email is the primary collaboration tool in most organisations, so it's no surprise that it's a common source of information leakage, with most data loss caused by user error. Piers Chivers, of Qinetiq-owned developer Boldon James, will demonstrate Email Classifier, a product that puts labelling at the heart of data loss prevention by giving users the option to apply relevant visual labels to Microsoft Outlook email messages and embed those labels into the email metadata.
15:45	**-**	**16:00**	**Cryoserver**: Organisations can no longer ignore the importance of information security around email. Cryoserver's recent survey has uncovered some worrying trends in email management that need to be addressed. Jane Cronin of FCS - the Cryoserver people - outlines the issues and explores how Cryoserver enables organisations to better manage the information risk inherent in email and supports ISO27001 compliance. Delegates will be invited to watch demonstrations after the formal presentation.
16:00	**-**	**16:15**	**PolicyHub® for Proactive Policy Management**. Barny Brummell, Business Development Manager at Hitec (Laboratories) Ltd, will demonstrate PolicyHub. This software automates the entire policy management lifecycle, ensuring that only the right employees receive, read, understand and sign-up to corporate policies and procedures. PolicyHub reduces the risk of regulatory fines and reputational damage by achieving a consistent, audited communication with the workforce.
16:15	**-**	**17:30**	**ISO27001:2013 and PCI DSS version 3 Consultancy Advice Surgeries** Confidential one-to-one advice sessions where delegates can ask the experts (see Note 1 below). In addition to the formal talks and workshops, there will be an opportunity to meet IT Governance expert consultants on a one-to-one basis and ask questions that will help you to identify which compliance objective/regime is suitable for your organisation, and how best to support and deliver this. This advice has already helped 150+ organisations to achieve certification to ISO27001 alone.

Please book your advice surgery via the registration desk.

Cyber Security Product Showcase 'Cyber-Security Expo 2014' – the IT Governance roadshow that you need to attend!

IT Governance, in association with our partners Vigilant, Boldon James (a Qinetiq company), BSI, AXELOS, ISACA, and the IISP (the Institute of Information Security Professionals), invite delegates to attend our cyber security exhibition, to watch and take part in live demonstrations of:

- **IT Governance: Cyber Security Risk Assessment Service** – consultants will help you to assess your current level of risk.
- **IT Governance Security Services –** qualified ethical hackers will give live demos of vulnerability scanning and penetration testing.
- **vsRisk** ISO27001 risk assessment software (Vigilant).
- **Classifier™** information classification software products, including Email Classifier (Boldon James – a QinetiQ company).
- **Cryoserver** archiving solution enables organisations to collect emails in a secure, tamper-evident archive repository.
- **IISP (Institute of Information Security Professionals)** – Members will be on hand to discuss the benefits of joining IISP.
- **Hitec (Laboratories) Ltd PolicyHub® (Policy Management Software)** reduces the potential risk of regulatory fines and reputational damage, and demonstrates compliance and best practice to regulators, senior management and auditors.

Representatives from accredited certification body **BSI** will be on hand to discuss the process and costs involved in achieving ISO27001 certification – increasingly important for UK firms that trade with government and international corporations.

Find out more about our speakers:

Alan Calder is a leading authority on cyber security. He is an acknowledged international author on information security and IT governance issues, and is the founder and executive chairman of IT Governance Ltd, the single-source provider of products and services in the IT governance, risk management and compliance sector.

Neira Jones has more than 20 years' experience in the financial services market, directing global change programmes, launching new products and services and managing process reengineering practices. She is an independent advisor on payments, risk, cyber crime and digital innovation, and chairs the Advisory Board for mobile innovator Ensygnia and the Global Advisory Board for Centre for Strategic Cybercrime and Security Science. She is a Fellow of the British Computer Society and was a member of the PCI SSC Board of Advisors for four years. Neira has received numerous awards, including Acquiring Personality of the Year at MPE 2013, Top 25 Female Infosec Leaders to Follow on Twitter in April 2013, the FStech April 2013 Compliance Project of the Year and Anti-fraud/Security Strategy of the Year award, the 2012 SC Magazine Information Security Person of the Year award, and was voted to the Infosecurity Hall of Fame in 2011.

Steve Watkins is a director of IT Governance Ltd, a technical assessor on information security management systems to the United Kingdom Accreditation Service (UKAS) transition to ISO27001:2013, and co-author of IT Governance: An international guide to data security and ISO27001/ISO27002, which was adopted by the Open University as its standard text on information security. Steve is also Chair of the UK ISO27001 User Group.

Bridget Kenyon is building an information security management function for **University College London (UCL)**, in conjunction with the overarching work that the Information Services Division is doing to introduce ITIL. Prior to joining UCL, Bridget led and developed PCI DSS consultancy and assessment practices for two leading technical services companies as a Qualified Security Assessor, dealing with many different environments and types of incidents. CISSP® qualified and an Associate Member of the Institute of Information Security Professionals, she is also editor for ISO/IEC 27013 and participates in revisions/development of other standards in the 27001 series.

Geraint Williams is a Senior Information Risk Consultant and Trainer at IT Governance. Geraint is a PCI QSA and leads the technical services team, as well as being the course leader for the IT Governance CISSP Accelerated Training Programme and the PCI DSS training courses. He has a strong technical background, with experience of ethical hacking, digital forensics and wireless security issues. Geraint has broad technical knowledge of security and IT infrastructure, including high performance computing. He holds certifications in security and digital forensics including CISSP, CREST Registered Tester, CEH and CHFI.

Suzanne Fribbins is EMEA Product Marketing Manager - Risk Portfolio at **BSI**. Suzanne’s role at BSI involves positioning and driving demand for the assessment and certification product range within the risk portfolio, comprising the international standard for information security ISO/IEC 27001, the British standard for health and safety BS OHSAS 18001, the international standard for road traffic safety management ISO 39001, the international standard for business continuity management ISO22301, the British standards for anti-bribery management BS 10500, the CSA STAR Certification Scheme and the international standard for IT service management ISO/IEC 20000.

Mike Edwards is a **BSI** tutor specializing in information security, business continuity and quality management systems. He has extensive security experience and has been a regular speaker at international conferences on information security in the defence sector. Mike has worked closely with the Ministry of Defence (MoD) providing an information security awareness programme, as well as writing a paper on the role of social networking and operational security in the armed forces. Before BSI, Mike spent over 20 years in the Royal Navy in a variety of information security roles. He has worked for the Royal Navy and the MoD on information assurance and business continuity management projects. Mike has been part of and led the MoD technical support teams auditing both classified and non-classified systems, ensuring compliance to ISO/IEC 27001 and HMG Security Policy Framework. Mike has a vocational degree in leadership and management and is a certified information security manager with ISACA as well as a qualified Ethical Computer Hacker and Computer Hacking Forensic Investigator.

Sarb Sembhi is Chair of the **ISACA** Government and Regulatory Advocacy Regional Subcommittee for the area of Europe/Africa, and Director of Consulting Services at Incoming. Sarb is a regular speaker at information security conferences around the world, including EuroCACS, RSA Europe, InfoSec, HITB, BCS, ISACA, ISSA, ASIS, IPSec, IFSec, Gartner, Richmond Events Security Summit and Econique CxO Dialogue.

Nick Wilding is Head of Cyber Resilience Best Practice at **AXELOS**. Nick has spent the last 25 years in senior business development and marketing roles, the last 11 of these at BAE Systems Applied Intelligence, formerly known as Detica. Most recently, Nick has been responsible for all thought leadership across the Applied Intelligence group where he designed and led the successful 'Digital Criminality' programme. Prior to BAE Systems, he was Group Marketing Director for Business Systems Group (now Advanced 365), a London City-based systems integrator, and held senior strategy, product development and operational roles at EULER Hermes UK, part of the world's largest credit insurance provider, and the Automobile Association (AA).

Richard Bach is Assistant Director for Cyber Security at the **Department for Business, Innovation and Skills**. From the age of eight, and inspired by the Enigma story, Richard wanted to break codes or catch spies. Appropriately, his chosen career path has been spent in the UK Government's security community. In earlier years he was a technical advisor on export controls, before moving into international relations, representing the UK's information assurance interests in the EU, the UN and the OECD. In a similar capacity in NATO he was one of the main architects behind NATO's Infosec Framework. For the last six years, Richard has brought his expertise to bear in cyber defence, and in late 2011 he became head of planning and delivery for the Government's operational cyber defence posture for the London 2012 Olympics.

Ethical Hackers/Penetration Testers: Alexandru Apostol, IT Governance Technical Services, will demonstrate penetration testing – a service that can help you evaluate computer and network security by simulating an internal or external threat by attacking a computer system or network. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weakness in process or technical countermeasures.

Product Demonstrators:

Richard Bailey – Chief Development Director, Channel Manager for **Boldon James**, a Qinetiq company – will demonstrate Classifier™ Microsoft document classification software. Richard graduated from UMIST in 1979 with a First Class Honours degree in Electrical and Electronic Engineering, and also gained an MSc in Factory Automation from UMIST in 1986. Richard joined Boldon James in 1987 as a software developer and by 1999 had taken ownership of the Software Development Group, with a responsibility for over 40 software development specialists. He has over 30 years' experience in software engineering across a variety of business sectors including defence, manufacturing, pharmaceutical and retail. Richard has been involved in all aspects of software development within Boldon James over the years, from design, coding and project management through product management and customer-facing activities. Richard has responsibility for driving the Boldon James product development strategy and delivery function of their Microsoft-based messaging and data classification product sets; as the company builds out from the defence sector across its target verticals.

Our sponsors and supporters:

CYBER
ESSENTIALS

AXELOS
GLOBAL BEST PRACTICE

ISACA®
Serving IT Governance Professionals

iisp The Institute of Information Security Professionals

HITEC
LABORATORIES

Cryoserver™

boldonjames
A QinetiQ Company

AGENDA:
ISO27001:2013, PCI DSS v3 and CES v1.0: New standards in the global cyber war (Churchill War Rooms, London, 8 May 2014)

Here are some frequently asked questions … Feel free to ask your own!

Some questions that delegates have asked us recently, but feel free to come up with your own.

How to achieve compliance with ISO 27001:2013 in time and on budget	ISO27001:2013 certification: What are the steps?/What should you expect?
1. How do we engage our senior management, persuading them that the ISMS programme has to be established and that they need to be involved?	1. How do I assess the complexity of my IT systems?
2. Should we aim for ISO27001 conformance, alignment, compliance or certification?	2. What is the key information needed to get a certification quote?
3. How long will it take to implement an ISMS in our situation?	3. How do I decide on a suitable certification scope?
4. Is it possible to restrict the scope of the ISMS to just one department or business unit, at least initially? If so, how do we treat risks that require controls outside the scope?	4. Who is needed to support an external audit?
5. In order to conduct a risk assessment, we need a list of all of our 'information assets'. What kinds of things should be included in the list?	5. How long will the auditors be on site?
6. What are the most challenging aspects of ISO27002 implementation and ISO27001 compliance?	6. What about back-up sites? Must they be included?
7. What are the merits of doing the project work ourselves versus hiring a consultant to help – and how do we maintain our ISMS after certification?	7. We have staff working on a customer's premises. Can they be included within the scope of our certification?