Why Attend This Course?

- Cover the essential areas you need to know to construct a well-balanced infosecurity framework.
- Define how to organise and oversee a risk-based enterprise infosec programme.
- Drill down to the critical building blocks of infosecurity.
- Explore the respective roles and responsibilities of the key players.
- Learn industry best practices legislation and professional standards based on ISO27000 Series (Previously the ISO17799) and COBIT.
- Course Review Exercises that will help you prepare for information security certification exams including CISSP and CISM.
- Take with you sample security policies, security review checklists, a glossary of computing terminology and much more!

Information Security

5 Day Course:

1–5 June 2015 London
5–9 October 2015 Hong Kong

Course Director: Charles Pask

Leading IT Auditor & Security professional with over 25 years experience and former Global Head of Strategy, Development and Globalisation for the BT Business Continuity, Security and Governance Practice.
Course Focus And Features

Increasing reports of targeted hacker attacks. Data leakage in all directions. Viruses, worms, and other forms of computer crime. Heightened attention to corporate governance. Today’s organizations are under increasing pressure to ensure the effectiveness of their infosecurity efforts and as a result, information security has become a priority business issue. Yet in spite of their far-reaching strategic business implications, security threats and vulnerabilities are still often misunderstood and underestimated by line and IT management. To further add to the confusion, this vital function is often viewed mostly as a technology issue.

In this information-packed, five-day seminar you will cover the essential areas you need to know to construct a well-balanced infosecurity framework. You will gain a business-oriented, architectural perspective that defines how to organize and oversee a risk-based enterprise information security program, blending best management practices with key physical and information technology safeguards. You will cover security policies, awareness, administration, models, mechanisms, and architectures; secure application design and assurance; backup, recovery, fault tolerance, and business continuity planning; user authentication; cryptography; network concepts and security; and much more.

And to ensure that you gain proper familiarity with industry best practices, legislation, and professional standards for information security, key references and yardsticks for the material you learn include, but are not limited to, ISO-27002 Code of Practice for Information Security, Common Body of Knowledge (CBK), Payment Card Industry Data Security Standard (PCI DSS), Common Criteria, Information Technology Infrastructure Library (ITIL).

To reinforce what you learn in the course and to aid anyone preparing for prominent information security certification examinations (including CISSP & CISM), you will be provided with unit and course review exercises. Come prepared for five days of intensive learning and return to your office with the foundation of knowledge and know-how needed to guide your organisation as it develops or revises its information security program.

Who Should Attend

Information Security and IT Managers; Information Security Analysts, Security Architects, Security Administrators; System Administrators, Network Administrators, IT Auditors; and anyone needing a “crash course” in information security concepts and practices.

Prerequisite

This course is geared to individuals with a general familiarity and working knowledge of information technology and other forms of information risk management and security, including those with three or more years of experience and training in IT Audit, Information Security, Quality Assurance, and/or Information Technology.

Advanced Preparation: None

Training Type: Group-Live

Learning Level: Intermediate

CPEs: 37

Price: GBP £2,995+VAT*

*Delegates may be able to claim back VAT. Visit www.mistieurope.com/VAT for more information.

Course Director: Charles Pask

Charles V. Pask is the Managing Director of ITSEC Associates Ltd, responsible for delivering global IT Audit and IT Security consultancy services.

Mr. Pask has 30 years’ experience in IT, IT audit, and IT security, and was previously the IT Audit Manager at Forward Trust Group (subsidiary of HSBC), and also Information Security Manager for Alliance & Leicester (10 years). He was a Director with MIS Training, and Director of Information Security Institute (ISI) European and Middle East e–Security Services (2000–2). More recently Mr Pask was the Global Head of Strategy, Development and Globalisation for the BT Business Continuity, Security and Governance Practice.

Mr Pask provides IT audit and security related consultancy services as well as public training courses, in–house training courses, conferences and symposiums. His clients includes: Royal Court Affairs, Oman; United Nations (Geneva, New York, Brindisi, Nairobi); Lloyds TSB Bank; KPMG; Unisys; Intrum Justitia; and, BT.
Day One:

Session 1: Information security concepts and management practices
- Current trends in information security
- Fundamental principles of information security
- Making the business case for information security
- Information security management cycle
- Risk analysis: threats, vulnerabilities, risks, and countermeasures policies, standards, procedures, and guidelines
- Information classification
- Security awareness
- Roles and responsibilities
- Enterprise information security architecture

Session 2: Laws and standards affecting information security and IT audit
- Ethics affecting information security
- Computer crimes, investigations, and evidence
- Laws, directives, and regulations
  - Types of laws: civil, criminal, administrative
  - Privacy issues and legislation
  - Intellectual property, copyright laws, and software piracy
  - Import and export laws
  - United States / European / International laws
- Information security and auditing standards: IETF, BS7799/ISO17799, NIST publications, GASSP, COBIT
- Information security clearing houses: FIRST, CERT, NIST, NIPC
- Professional certification

Day Two

Session 1: Security models, mechanisms, and architectures
- Overall information security architecture
- Computer architecture
- System architecture
- Security models
- Access controls- access control models, techniques and technologies, and methods
  - Threats to access controls
- Modes of operation open and closed systems
- Security design standards and criteria: “Rainbow Series”, common criteria
- Certification and accreditation
- Threats to security models and architectures
- Change management
  - Tools for the auditor
  - Operating system utilities and vulnerability scanners

Session 2: Access controls
- Common operating system vulnerabilities
- Prominent operating system software and their security features
- User authentication
- Data protection and authorisation
- Privileged authority controls
- Audit logs and monitoring
- Configuration and vulnerability testing
- Workstation security: desktop, mobile
- Operating system security add-ons
- Security administration and operational security

Session 3: Network concepts
- Open Systems Interconnection (OSI) model
- Transmission Control Protocol / Internet Protocol (TCP/IP)
- Wiring
- Type of transmissions
- Local area network (LAN) technologies, topologies and protocols
- Wide area network (WAN) technologies and protocols
- Wireless networks technologies, protocols, and security
- Network addresses and applications
- Networking devices: network cards, hubs, switches, routers, gateways
- Directory services: X.500, LDAP, DNS
- Network management tools: packet sniffers, Simple Network Management Protocol (SNMP), network utility and diagnostic software

Group Booking Discount**

2 delegates - 5% discount
3 delegates - 10% discount
4 delegates - 12% discount
5 delegates - 15% discount

**Available for delegates from one organisation attending the same course
Day Three:

Session 1: Cryptography
- History of encryption
- Key management: asymmetric, symmetric
- Encryption algorithms and hashing functions
- Digital signatures
- Public key infrastructure (PKI)
- Attacks on crypto systems
- Applications of encryption: e-mail, data protection, message concealment, Internet security protocols (SSL/TLS ,SET), virtual private networks (VPNs)

Session 2: User authentication
- Authentication mechanism: passwords, tokens, smart cards, biometrics
- Enterprise authentication systems: RADIUS, TACACS+, Diameter
- Single sign-on (SSO): Kerberos, SESAME, scripting, Web-based SSO, thin-clients

Session 3: Network security
- Network security vulnerabilities, threats, risks, and countermeasures
- Hacker probing and attack techniques
- Firewalls and proxy servers
- Intrusion detection and preventions systems
- Network encryption and VPNS
- Remote access and dial-up access security
- Vulnerability and penetration testing

Day Four:

Session 1: Business application and development security
- Security for different environments
- Data types and structures
- Database management systems
- System development life cycle methodologies
- Configuration management and change control
- Application development tools and methodologies
- Web site attacks and defenses
- Mobile code: Java, ActiveX, JavaScript
- Malicious software: viruses, worms, and Trojan horses
- Hacker attacks on software

Session 2: Physical, personnel and environmental security
- Facilities location, construction, and management
- Physical security threats, vulnerabilities, risks, and countermeasures
- Perimeter security, boundary protection, and facilities access controls
- Electrical, temperature, water, and other environmental controls
- Fire detection, prevention, and suppression
- Information storage media protection and disposal
- Emergency procedures
- Personnel security: hiring practices, badges, personnel records, Terminations and transfers

Day Five

Session 1: Availability, backup, recovery and business continuity planning
- Business impact analysis
- Business continuity planning requirements
- Redundancy and fault tolerance
- Network and computer resource availability
- Backup procedures: on-site and offsite
- Backup resources: processing sites, storage, offices, utilities, equipment and supplies
- Recovery testing procedures
- Emergency response procedures

Wrap-up discussion

TAILORED AND PERSONALISED IN-HOUSE TRAINING

Why Choose In-House Training?

Savings - Running an in-house course in your offices will ensure you avoid the costs of travel and accommodation. Plus we charge per day not per delegate. You can train six or sixteen people for the same price!
Convenience - We can arrange a course that fits your team’s schedule. Any dates, any location, simply tell us what works best for you. Avoid the hassle of coordinating travel arrangements and accommodation for your staff
Tailored training - We have over 150 existing training courses you can mould to fit your exact requirements or if you prefer we can just create a new agenda. You will have complete control over the course content
Confidentiality - You can focus on potentially thorny issues that may be specific to your organization which are best resolved in private with the expert guidance of your course director

IN-HOUSE TRAINING
Save up to 50% with In-House Training

Some Of The Companies We Have Worked With:
- PwC
- International Labour Office
- Barclays
- Capital One
- Legal and General
- Deloitte
- European Court of Auditors
- Lukoil
- Credit Suisse AG
- Euroclear
- AIB
- U.S. Steel, Corp.
- Novartis
- National Commercial Bank
- Qatar National Bank

Visit www.mistieurope.com/inhouse
Call us on 0207 779 8202
Email mis@mistieurope.com

Register online at: www.mistieurope.com