

The MIS TRAINING INSTITUTE CERTIFICATE in

4 day course

Risk Based IT Auditing

30 November-3 December 2010
Singapore

Use control best practices to ensure the confidentiality, integrity and availability of your information assets

- Plan your IT Audit using risk-based approach, COBIT and COSO control framework
- Determine risk in critical areas of your IT environment, including operating systems, database management systems, business continuity and application controls
- Learn a pro-active audit approach to provide a value-added service to your organisation
- Auditing outsourced IT operations
- Learn why IT governance is critical
- Auditing system development projects

Expert Course Director:

Charles Pask, *CISSP, M.Inst.ISP*

Secure your place!
Register before
2 November 2010 at
www.mistiasia.com

What past delegates have said about this course in other region:

"Very precise and informative"

Past delegate, *Mobiltel EAD*

"Very good course... In 4 days you got an almost complete update of IT risks"

Past delegate,
AON Groep Nederland

WHO SHOULD ATTEND?

- Financial, operational, business applications, information technology, and external auditors
- Quality assurance personnel
- Audit managers and directors
- Information security managers and analysts

LEARNING LEVEL:
Intermediate

PREREQUISITES:
IT Audit School course or equivalent experience. To get the most out of this course, you should have a working knowledge of databases, operating systems and networks.

CPEs: 30



Find out more or register your place today!

Web
www.mistiasia.com

A division of Euromoney Training

FOCUS AND FEATURES

From the European Union Data Protection Directive to Basel II and Sarbanes-Oxley, recent regulations require organisations to ensure appropriate levels of protection for their critical information assets. To be sure, the common thread through these mandates is the requirement for security and effective controls at all levels of the enterprise.

In this practical, four-day course you will immerse yourself in a risk-based approach to IT auditing that will ensure the confidentiality, integrity, and availability of your information assets throughout the enterprise. You will review COBIT, ISO-27002 and a number of other standards / frameworks and learn how they can be applied to your IT audits to provide an appropriate risk focus. You will concentrate on determining risk in critical areas of the IT environment, including operating systems, database management systems, networks, logical security, change management, business continuity planning and application controls. You will learn a proactive audit approach that will provide a value-added service to your organisation. You will leave this intensive course with a thorough understanding of risk-based IT audit and control best practices that you can apply immediately to your next IT audit.

Day 1

Registration commences at 8:30
Programme runs from 9:00 - 5:00 daily

Planning the IT audit

- Risk-based auditing
- Integrated audit approaches
- Developing the audit strategy
- Using the COSO control framework for audit planning
- Planning and executing the audit

Risk assessment

- Risk-based auditing
- Identifying risk factors, vulnerabilities, and threats
- Business and technical risks
- Cost / risk evaluation
- Risk assessment factors
- IT risks in an automated environment

Complying with international regulations

- Risk coverage required by international data protection acts
- European Union Data Privacy
- Basel II
- Sarbanes-Oxley
- Payment Card Industry DSS

Using COBIT

- COBIT control objectives
- COBIT framework and domains
- Utilising COBIT in planning the audit
- Applying COBIT audit guidelines

Applying the ISO-27002 security standard

- ISO 27002 structure overview
- Referencing the standard for auditing
- Security policies
- Information classification
- Physical security
- Access controls
- Security monitoring

Day 2

IT governance

- IT governance defined
- Why IT governance is critical
- Linking enterprise and IT strategies
- IT organisation and management
- Policies and procedures
- IT steering committee
- Information security governance
- Separation of duties
- IIA and ISACA governance audit guidelines

System software

- Software integrity
- Operating system risks and controls
- Controlling privileged access
- Activity logging
- Vendor patch management
- Database management risks and controls
- Utility programmes
- Audit steps

Logical access controls

- Logical access control objectives
- Integrated roles of IT and business process owners
- Authentication objectives: password controls, tokens, and biometrics
- Authorisation
- Audit trail
- Managing user accounts
- Security monitoring
- Single Sign-On (SSO) authentication
- Remote access
- Sensitive data on PCs and workstations
- Social engineering risks
- Centralised vs. decentralised control
- Access control best practices
- Audit steps

Change management

- Change management objectives / risks
- Change requests
- Testing changes
- Implementation approval
- Programme migration
- Contingency plans
- System documentation

Biography

Charles Pask, *CISSP, M.Inst.ISP*

Charles Pask is the Managing Director of his own consultancy firm delivering global IT security and IT audit consultancy services, including training courses, conferences, symposiums and general Infosec consultancy. Previously, he was a Director with MIS Training, and Director of Information Security Institute (ISI) European and Middle East e-Security Services. Charles

has over 25 years' experience in IT, IT audit, and IT security, and was the Information Security Manager for Alliance & Leicester plc prior to joining MIS. More recently Charles was the Global Head of Strategy, Development and Globalisation for the BT Business Continuity, Security and Governance Practice.

Charles has been a member of the ITSEC Common Criteria team working with the DTI, and a committee member of the APACS Security Advisory Group and the LINK Security Group. He has spoken at a number of conferences, including CISO, WebSec, Compsec, the International Security Managers Symposium, and various ISACA events.



Day 4

- Executable and source code integrity
- Emergency changes
- Library control software
- Vendor-supplied source code
- Audit steps

Day 3

Physical and environmental controls

- Physical security objectives, risks, exposures, and controls
- Environmental exposures and risks
- Environmental controls: fire protection, water protection, and power conditioning
- Audit steps

Network perimeter security

- Network security threat / risk analysis
- Network security strategy
- OSI Model
- TCP/IP
- Firewalls
- DMZ
- Intrusion detection systems
- Remote access
- Wireless access
- Audit strategies encryption
- Types of encryption
- Symmetric and asymmetric encryption
- Public key infrastructure
- Network encryption layers
- Secure sockets layer
- Digital signatures

Application controls

- Relationship between general controls and application controls
- Business applications risks
- Transaction life cycle
- Completeness and accuracy of input
- Completeness and accuracy of processing
- Exception reporting
- Output controls
- Application change management
- End user computing
- Business / data warehouses
- Application system audit strategy

Disaster recovery and business continuity

- Disaster recovery planning
- Business continuity planning
- Business impact analysis
- Recovery time objectives
- Continuity plans and procedures
- Off-site data storage and information processing
- Contract requirements
- Auditing disaster recovery and business continuity plans

Auditing outsourced IT operations

- Outsourcing risks
- Offshore outsourcing risks
- Ensuring strong contractual agreements
- How to obtain a right to audit
- Obtaining and assessing SAS-70 reports
- Relationship monitoring
- Audit focus areas

Auditing system development projects

- Audit's role on development projects
- Business risks of development project
- Why auditors should be involved
- Getting involved how, when, who?
- Staffing the audit
- Communicating audit's roles and results
- Assessing project management
- System acquisitions
- Audit strategy

Executing IT audits

- Risk assessment
- Planning the audit
- Developing audit programmes
- Testing controls
- Using CAATs and data analysis
- Workpapers
- Audit report
- IT audit tool kit



Charles delivers a number of MIS Training Institute's IT Audit and Security training program including "IT Auditing and Controls", "IT Audit School", "Risk Based IT Auditing", "How to Manage an Information Security Program" and "Information Security School". He has also previously been a Senior Instructor for ISC2 in for CISSP exam training classes.

SAVE TIME AND MONEY WITH IN-HOUSE TRAINING
MIS Training Institute provides specific, tailor-made in-house training on a wide variety of internal audit, IT audit and information security topics. Clients are able to determine the content, duration, and level of expertise of the course, creating a unique and customised programme. All our in-house consultants are professional trainers and draw on many years of practical experience in the audit and information security area.
To find out more about the special benefits of in-house training, please contact:
Kelli Haynes, Director, Asia Pacific
Tel: +852 2111 6636
Email: kelli.haynes@euromoneyasia.com

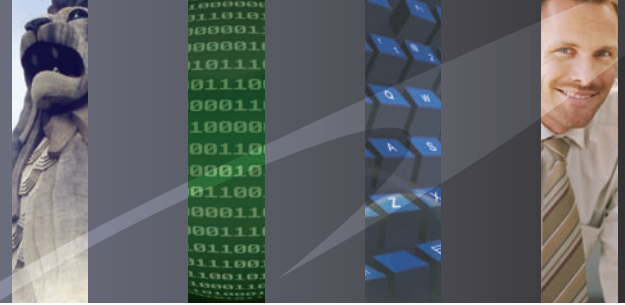


Book by 2 November 2010 to secure your place.

Email
miasia@misti.com

Telephone
+852 2520 1481

Facsimile
+852 2866 7340



Secure your place!

Register before

2 November 2010

5 easy ways to register

Please quote reference WEB

1. Web
www.mistiasia.com
2. Email
miasia@misti.com
3. Telephone
+852 2520 1481
4. Facsimile
+852 2866 7340
5. Mail
GPO Box 11886, Hong Kong

I prefer course updates by **email**.

My email address is _____.

Please fax back to +852 2866 7340 or email your details to update@euromoneyasia.com.

Please include the code that appears on top of the address label above in your email.

Registration form Yes, please register me for:

Risk Based IT Auditing (MS4690)

on 30 November-3 December 2010, Singapore

Can't make this date? We schedule our courses throughout the year. Please contact us to check for alternative dates and locations.

Delegate details (all of the following is required to process your registration)

Surname _____ Mr/Mrs/MS

First name _____

Position _____ Department _____

Company _____

Address _____

Telephone _____ Fax _____

Email _____

IIA Membership No.: _____

ISACA Membership No.: _____

How did you hear about the course? _____

Please tick which best describes your company:

- | | |
|--|--|
| <input type="checkbox"/> Accountancy - 0005 | <input type="checkbox"/> Energy Company - 0193 |
| <input type="checkbox"/> Bank and Financial Institution - 0020 | <input type="checkbox"/> Other _____ |
| <input type="checkbox"/> Corporate - 0149 | |

Course fee: US\$3,850

All fees are net of withholding, business and local taxes.

Delegates registering from Singapore will have to bear the prevailing GST at the date of invoice.

Seat is confirmed only upon receipt of payment.

Payment details (please tick as appropriate)

- Cheque Invoice Credit card[#]

[#]To make this payment by credit card, please call +852 2520 1481.

I have read and understood the booking terms and conditions

Signature _____ Date _____

Membership discount

IIA Hong Kong members save 15% ISACA Hong Kong members save 15%
Other IIA members save 10% Other ISACA members save 10%
This discount cannot be used in conjunction with any other offer.

Group booking discount

When two colleagues from one institution book together on the same course, there is a 5% discount on the second booking. Further discounts are available for larger groups.

Venue

All of our courses are held in 4 – 5 star hotels, chosen for their location, facilities and level of service. You can be assured of a comfortable, convenient learning environment throughout the duration of the course. Due to the variation in delegate numbers, we will send confirmation of the venue to you approximately 2 weeks before the start of the course.

Disclaimer

MIS Training reserves the right to alter any part of the published programme or faculty. In the event of course cancellation by MIS Training due to unforeseen circumstances, MIS Training limits its liabilities to refunding the tuition fee of the course.

Fee includes tuition, documentation, lunch and refreshments. Delegates are responsible for their own flights and accommodation. An invoice will be sent upon receipt of registration form.

A Euromoney Institutional Investor group company

Data protection

The information you provide will be safeguarded by the Euromoney Institutional Investor PLC whose subsidiaries may use it to keep you informed of relevant products and services. We occasionally allow reputable companies outside Euromoney Institutional Investor PLC to contact you with details of products that may be of interest to you. As an international group we may transfer your data on a global basis for the purposes indicated above. If you object to contact by telephone fax or email please tick the relevant box. If you do not want us to share your information with other reputable companies please tick this box

Cancellation policy

If any registered delegate cannot attend our course, a replacement is always welcome for the course. Cancellations must be made in writing (letter or fax) with MIS Training's acknowledgement. Written cancellations must reach this office 30 days before the programme commences. A full refund less an administration charge of US\$150 will be given. For any written cancellation requests that reach us less than 30 days before the event, no refunds will be given. However, if you wish to attend another MIS Training course in the Asia-Pacific region, a 75% discount voucher which values not more than 75% of the initial payment will be issued. Please note that the subsequent course must take place within 1 year of the

initial registration. Discount vouchers are transferable within the same organisation, but not to be used in conjunction with any other discount schemes. Discount vouchers will not be issued for no-shows without cancellation. MIS Training reserves the right to the final decision if any dispute arises.

Incorrect mailing

Please accept our apologies for mail which is incorrectly addressed. Should you wish to amend the address/addressee details, please send or fax us a copy of the relevant mailing label (on the envelope or brochure) and we will update our records accordingly.