



University of Salford
A Greater Manchester University



CISM Revision Course

4th – 6th November 2009



Prepare for the CISM examination early December 2009
Delivered by Vernon Poole of Sapphire Technologies
Gain 19 CPE Credits

Salford Business School at The University of Salford are pleased to announce that, in association with ISACA Northern England Chapter, we will be offering a 3 day training course in order to prepare candidates for early December 2009 CISM examination.

The Course

- This three day seminar focuses on the essential areas covered in the CISM exam, completely revised for 2007 by the ISACA Certification Board. You will cover the core knowledge bases included in the examination 'Common Body of Knowledge'.
- At the end of the course there is a mock examination and review session including a review of the correct answers that will provide you with a better understanding of what the ISACA Certification Board expects. This intensive course is an idea way to prepare for the exam.

“The Salford Business School’s CISM training proved to be a real advantage when I came to take my exam. Their experienced instructors and links to ISACA allowed thorough preparation”

Gavin White, Management Auditor

Who Should Attend:

- Experienced information security managers and those who have information security management responsibilities and are taking or considering taking the CISM examination. The CISM certification is for the individual who manages, designs, oversees and/or assesses an enterprise's information security strategy.

Course Director

- Vernon Poole: Vernon is a European leader in the field of information security management and is qualified as a ISO27001 Lead Auditor and CLAS consultant, apart from being a world-renowned speaker and founder member of the UK & International 7799 User Groups.

He is a recognised adviser to senior management on the importance of 'Information Assurance' and a European representative on the global IT Governance Institute - where he is recognised as one of the thought leaders on Information Governance.

Vernon is CISM certified and presents CISA/CISM workshops for these qualifications; and after 12 years with Deloitte's, he joined Sapphire Technologies - which is one of the UK's leading independent information security companies - and the company celebrates its 10th

Anniversary this year by being one of the first companies to become ISO 27001 certified Vernon develops highly respected Information Security Benchmarking methodologies based on ISO 27001; he works closely with the UK's DTI (Department of Trade & Industry) and the Cabinet Office's CSIA (Central Sponsor for Information Assurance) – who jointly worked on the Standard's Revision.

Overview of the Course:

- The course aims to provide candidates with a review of the tasks and knowledge requirements for each CISM domain and to help identify any omissions in their knowledge. Therefore, candidates are expected to be familiar with the content of the CISM domains and already have 1-2 years Information Security experience.
- The course includes a review of the examination format and aims to improve candidates' examination techniques.
- The course includes a mock examination, each candidate's answers will be reviewed followed by a discussion on how to identify the most appropriate answers.
- Refreshments and lunch are included in the price, together with a full delegate pack. The University is easily accessible by car/taxi/public transport from Manchester City Centre.
- Accommodation is not included, however we recommend delegates stay at The Castlefield Hotel (www.castlefield-hotel.com), this hotel is reasonably priced, close to all amenities and, we hope that if delegates stay in the same hotel they will have the opportunity to discuss the course and socialise in the evenings.

Registering for the Exam

- **All delegates are responsible for registering on the exam themselves and must contact ISACA directly by their specified deadlines to be eligible to take the examination.**
 - Early registration deadline mid August 2009
 - Final registration deadline mid September 2009



Course Content

- The areas may be subject to change as they are defined centrally by ISACA in the USA.

Information Security Governance

- Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.
- Develop the information security strategy in support of business strategy and direction.
- Obtain senior management commitment and support for information security throughout the enterprise.
- Ensure that definitions of roles and responsibilities throughout the enterprise include information security governance activities.
- Establish reporting and communication channels that support information security governance activities.
- Identify current and potential legal and regulatory issues affecting information security and assess their impact on the enterprise.
- Establish and maintain information security policies that support business goals and objectives.
- Ensure the development of procedures and guidelines that support information security policies.
- Develop business case and enterprise value analysis that support information security program investments.

Risk Management

- Identify and manage information security risks to achieve business objectives.
- Develop a systematic, analytical and continuous risk management process.
- Ensure that risk identification, analysis and mitigation activities are integrated into life cycle processes.
- Apply risk identification and analysis methods.
- Define strategies and prioritise options to mitigate risk to levels acceptable to the enterprise.
- Report significant changes in risk to appropriate levels of management on both a periodic and event-driven basis.

Information Security Programme Management

- Design, develop and manage an information security programme to implement the information security governance framework.
- Create and maintain plans to implement the information security governance framework.
- Develop information security baseline(s).

- Develop procedures and guidelines to ensure business processes address information security risk.
- Develop procedures and guidelines for IT infrastructure activities to ensure compliance with information security policies.
- Integrate information security programme requirements into the organisation life cycle activities.
- Develop methods of meeting information security policy requirements that recognise impact on end users.
- Promote accountability by business process owners and other stakeholders in managing information security risks.
- Establish metrics to manage the information security governance framework.
- Ensure that internal and external resources for information security are identified, appropriated and managed.

Information Security Management

- Oversee and direct information security activities to execute the information security programme.
- Ensure that the rules of use for information systems comply with the enterprise's information security policies.
- Ensure that the administrative procedures for information systems comply with the enterprise's information security policies.
- Ensure that services provided by other enterprises, including outsourced providers, are consistent with established information security policies.
- Use metrics to measure, monitor and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
- Ensure that information security is not compromised throughout the change management process.
- Ensure that vulnerability assessments are performed to evaluate effectiveness of existing controls.
- Ensure that non-compliance issues and other variances are resolved in a timely manner.
- Ensure the development and delivery of the activities that can influence culture and behaviour of staff, including information security education and awareness.
- **Response Management**
- Develop and manage a capability to respond to and recover from disruptive and destructive information security events.
- Develop and implement processes for detecting, identifying and analysing security related events.
- Develop response and recovery plans including organising, training and equipping the teams.
- Ensure periodic testing of the response and recovery plans where appropriate.
- Ensure the execution of response and recovery plans as required.
- Establish procedures for documenting an event as a basis for subsequent action, including forensics when necessary.
- Manage post-event reviews to identify causes and corrective actions.

CISM Revision Course

4th – 6th November 2009

Name:			
Company:			
Address:			
Email:			
Telephone no:			
Email:			
ISACA Member?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Member No: <input type="text"/>

Circle as appropriate:

Member Non-member
Course £650 £700

Group Discounts:

£50 per delegate for 5 - 10 delegate groups

£80 per delegate for 10+ delegate groups

Payment is by cheque and must be received with your registration form. Please make cheques payable to: University of Salford.

Send your registration form and cheque to: Sarah Christie, Salford Business School, Maxwell Building, University of Salford, The Crescent, Manchester, M5 4WT, email: s.christie@salford.ac.uk.
Should you require an alternative method of payment please contact Sarah Christie.

**Any questions please contact Prof. Elaine Ferneley
0161 295 5507 email: E.Ferneley@salford.ac.uk**

Cancellation Policy: to receive a full refund (less £50 administration fee), your cancellation must be received (by email or post) within 61 days of the course date. The penalty after that is 60-31 days 30% 30-15 days 60%, less than 14 days 100%. If you are unable to attend a substitute is welcome. Substitution of a non-member in place of an ISACA member is subject to the additional non-member fee.

Please note: If you fail to attend without the due cancellation notice, you will be liable for the entire fee