

CISA REVISION WORKSHOP

20th & 21st November 2008



Prepare for the CISA examination on 13 December 2008

Birmingham City University is pleased to announce that we will be offering a two day revision workshop in order to prepare candidates for the 13 December 2008 CISA examination.

The Workshop

The two day workshop focuses on the essential areas covered in the CISA exam. During the workshop you will be given CISA examination questions in groups to create discussion/debates and followed by a review of the correct answers, which will provide you with a better understanding of what the ISACA Certificate Board expects. The intensive course is an ideal way to prepare for the exam.

The workshop aims to provide candidates with a review of the tasks and knowledge requirements for each CISA domain and to help identify any omissions in their knowledge.

The University is easily accessible by car/bus/train/taxi from Birmingham City Centre. Accommodation is not included. However, there is a small local hotel delegates could use which is a 5-10 minute walk from the University. The hotel is called The Park Hotel and can be contacted on 0121 356 0707. Refreshments are included throughout the day but lunch is not provided. There are two canteens/cafes on site and the local shopping centre is a 5 minute walk.

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 20 August 2008
- Final registration deadline 24 September 2008

Website for registration: <http://www.isaca.org>

Who Should Attend

IT, Financial, Operational and External Auditors who are taking or considering taking the CISA examination; anyone seeking an overall understanding of essential IT risks and controls.

Cost and What is Included

The cost for the two day workshop is £375. Included in this cost is:

- Course Revision Manual
- PowerPoint slides
- Refreshments (no lunch)

CISA REVISION WORKSHOP

CONTENT – DAY 1

20 November 2008

IS Audit Process (10% of the Examination)

Provide IS audit services in accordance with IS audit standards, guidelines and best practices to assist the organisation in ensuring that its information technology and business systems are protected and controlled.

IT Governance (15% of the Examination)

Provide assurance that the organisation has structure, policies, accountability, mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT.

Systems and Infrastructure Life Cycle (16% of the Examination)

Provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance and disposal of systems and infrastructure will meet the organisation's objectives

CONTENT – DAY 2

21 November 2008

IT Service Delivery and Support (14% of the Examination)

Provide assurance that the IT service management practices will ensure delivery of the level of services required to meet the organisation's objectives.

Protection of Information Assets (31% of the Examination)

Provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

Business Continuity and Disaster Recovery (14% of the Examination)

Provide assurance that, in the event of a disruption, the business continuity and disaster recovery processes will ensure the timely resumption of IT services, while minimising the business impact.

Course Content

Area 1: IS Audit Process

- 1.1 Develop and implement a risk-based IS audit strategy for the organisation in compliance with IS audit standards, guidelines and best practices.
- 1.2 Plan specific audits to ensure that IT and business systems are protected and controlled.
- 1.3 Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.
- 1.4 Communicate emerging issues, potential risks, and audit results to key stakeholders.
- 1.5 Advise on the implementation of risk management and control practices within the organisation, while maintaining independence

Area 2: IT Governance

- 2.1 Evaluate the effectiveness of IT governance structure to ensure adequate board control over the decisions, directions, and performance of IT so that it supports the organisation strategies and objectives.
- 2.2 Evaluate IT organisational structure and human resources (personnel) management to ensure that they support the organisation strategies and objectives.
- 2.3 Evaluate the IT strategy and the process for its development, approval, implementation, and maintenance to ensure that it supports the organisation strategies and objectives.
- 2.4 Evaluate the organisation IT policies, standards, and procedures; and the processes for their development, approval, implementation, and maintenance to ensure that they support the IT strategy and comply with regulatory and legal requirements.
- 2.5 Evaluate management practices to ensure compliance with the organisation IT strategy, policies, standards, and procedures.
- 2.6 Evaluate IT resource investment, use, and allocation practices to ensure alignment with the organisation strategies and objectives.
- 2.7 Evaluate IT contracting strategies and policies, and contract management practices to ensure that they support the organisation strategies and objectives.
- 2.8 Evaluate risk management practices to ensure that the organisation IT related risks are properly managed.
- 2.9 Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.

Area 3: Systems and Infrastructure Lifecycle Management

- 3.1 Evaluate the business case for the proposed system development/acquisition to ensure that it meets the organisation business goals.
- 3.2 Evaluate the project management framework and project governance practices to ensure that business objectives are achieved in a cost effective manner while managing risks to the organisation.
- 3.3 Perform reviews to ensure that a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- 3.4 Evaluate proposed control mechanisms for systems and/or infrastructure during specification, development/acquisition, and testing to ensure that they will provide safeguards and comply with the organisation policies and other requirements.
- 3.5 Evaluate the processes by which systems and/or infrastructure are developed/acquired and tested to ensure that the deliverables meet the organisation objectives.

- 3.6 Evaluate the readiness of the system and/or infrastructure for implementation and migration into production.
- 3.7 Perform post-implementation review of systems and/or infrastructure to ensure that they meet the organisation objectives and are subject to effective internal control.
- 3.8 Perform periodic reviews of systems and/or infrastructure to ensure that they continue to meet the organisation objectives and are subject to effective internal control.
- 3.9 Evaluate the process by which systems and/or infrastructure are maintained to ensure the continued support of the organisation objectives and are subject to effective internal control.
- 3.10 Evaluate the process by which systems and/or infrastructure are disposed of to ensure that they comply with the organisation policies and procedures.

Area 4: IT Service Delivery and Support

- 4.1 Evaluate service level management practices to ensure that the level of service from internal and external service providers is defined and managed.
- 4.2 Evaluate operations management to ensure that IT support functions effectively meet business needs.
- 4.3 Evaluate data administration practices to ensure the integrity and optimisation of databases.
- 4.4 Evaluate the use of capacity and performance monitoring tools and techniques to ensure that IT services meet the organisation objectives.
- 4.5 Evaluate change, configuration, and release management practices to ensure that changes made to the organisation production environment are adequately controlled and documented.
- 4.6 Evaluate problem and incident management practices to ensure that incidents, problems, or errors are recorded, analysed, and resolved in a timely manner.
- 4.7 Evaluate the functionality of the IT infrastructure (eg network components, hardware, systems software) to ensure that it supports the organisation objectives.

Area 5: Protection of Information Assets

- 5.1 Evaluate the design, implementation, and monitoring of logical access controls to ensure the confidentiality, integrity availability and authorised use of information assets.
- 5.2 Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorised use of the network and the information transmitted.
- 5.3 Evaluate the design, implementation, and monitoring of environmental controls to prevent or minimise loss.
- 5.4 Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded.
- 5.5 Evaluate the processes and procedures used to store, retrieve, transport, and dispose of confidential information assets.

Area 6: Business Continuity and Disaster Recovery

- 6.1 Evaluate the adequacy of back up and restore provisions to ensure the availability of information required to resume processing.
- 6.2 Evaluate the organisation of disaster recovery plan to ensure that it enables the recovery of IT processing capabilities in the event of a disaster.
- 6.3 Evaluate the organisation business continuity plan to ensure its ability to continue essential business operations.

PRIORITY BOOKING FORM

'CISA Revision Workshop'

20th & 21st November 2008

Birmingham City University, Business School
Perry, Barr, Birmingham

Please reserve a place for:

Title: Mr/Mrs/Ms/ Miss _____

Job Title: _____

Name: _____

Telephone Number: _____

Company: _____

Fax Number: _____

Address: _____

Email Address: _____

Special Requirements (eg access) _____

Postcode _____

I agree to pay the costs as highlighted above within the booking conditions.

Name..... Job Title.....

Signature..... Contact Tel

Total Amount
£375

Method of Payment

I enclose a cheque made payable to 'Birmingham City University' for £375

Please send an invoice to the above address and payment will be made promptly.

Please charge my credit/debit card £375

Card Number _____

Start Date __ / __ / __ Expiry Date __ / __ / __

Issue No. __ Security No. __

Signature..... Date.....

For further information and to return booking form:

Angela Reynolds
Centre for Internal Audit, Governance & Risk Management, Postgraduate Office
Birmingham City University Business School
Perry Barr, Birmingham, B42 2SU
Tel: 0121 331 6595
Fax: 0121 331 6366
Email: angela.reynolds@bcu.ac.uk

Booking conditions

If you have requested an invoice please ensure that payment is made within two weeks of receipt of invoice.

Cancellations

To receive a full refund (less £50 administration fee), your cancellation must be received (email or post) by 24 October 2008. No refunds will be paid if cancelled after this date. Substitution of delegates with prior notice is allowed.

