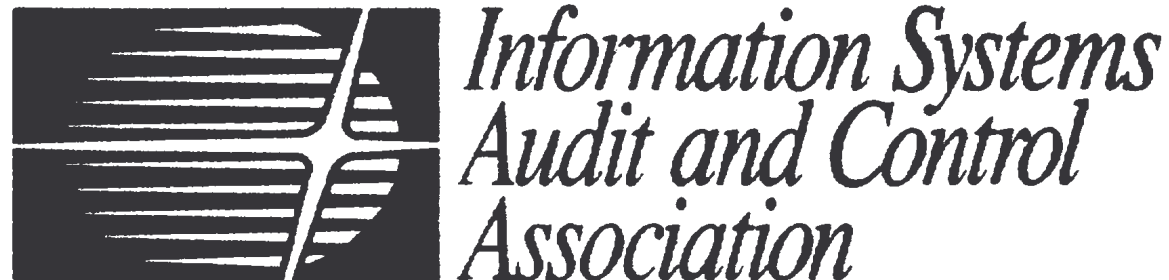


Information Systems Audit and Control Association



Sonja Durnin, KPMG
Fiona Coloe, IIB Bank
25th January 2005



Overview



- Background to ISACA
- Overview of CISA program & exam
- Overview of CISM
- Tips and examination advice
- CISA/CISM Certification Requirements
- Continuing Education Policy Details

Information Systems and Control Association (ISACA)



- Founded in 1969 and presently has more than 28,000 members in 100 countries.
- ISACA is a recognised global leader in IT governance, control and assurance.
- Develops globally applicable information systems auditing and control standards.
- Administers the globally respected Certified Information Systems Auditor (CISA) designation.

Irish Chapter



The ISACA Irish Chapter was established in 1997.

The Chapter currently has approximately 120 members. The Chapter hosts an annual Conference and also regular evening seminars on topics of interest to our members.

For more information on joining the Chapter, or to be included on the ISACA mailing list, please contact jackie.pyatt@kpmg.ie

Overview of the CISA Program and Examination





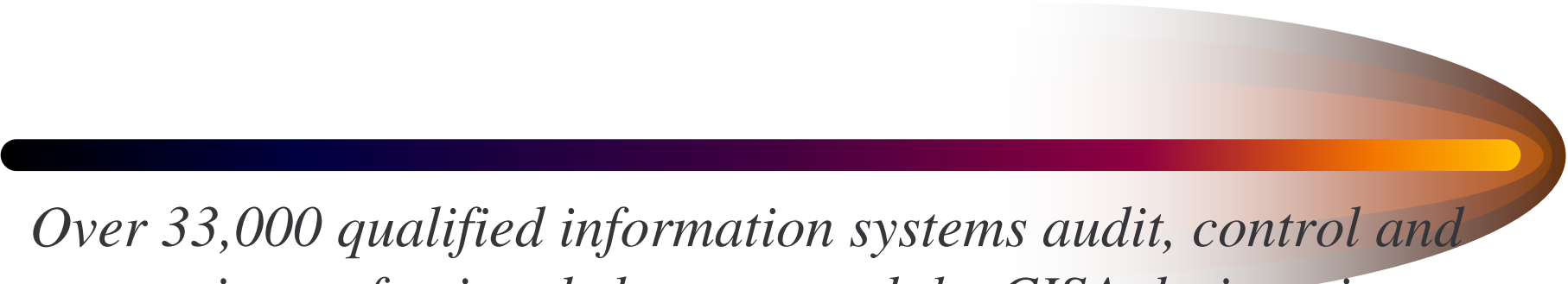
The CISA designation is recognized as the preferred certification for professional information systems audit, control and security professionals!

CISA Certification Background



CISA recognised worldwide as a symbol of excellence since 1978

- Awards expertise in IS audit, control and security
- Requires continuing professional education
- Provides a method for management to evaluate personnel



Over 33,000 qualified information systems audit, control and security professionals have earned the CISA designation worldwide!

The exam is offered in 11 languages in 200+ locations

In 2004 a record number of over 12,000 individuals registered for the exam

In 2005, ISACA expect a record 15,000 individuals to register for the exam!

Why Become A CISA?



- To demonstrate your willingness to improve your technical knowledge and skills.
- To demonstrate to management your commitment toward organizational excellence.
- To obtain credentials that employers seek.
- To enhance your professional image.
- To be included with other professionals who have gained worldwide recognition.

Quality of the Examination



Job Analysis Study:

determines appropriate content of the examination

Test Development Standards:

provide standards for development and review of questions

Review Process:

two reviews of the questions by independent committees before acceptance into pool

Periodic Pool Cleaning:

continuous review of questions in the pool to ensure that questions are up-to-date

Summary of Content Areas



- Domain 1 IS Audit Process (10%)
- Domain 2 Management, Planning and Organisation of IS (11%)
- Domain 3 Technical Infrastructure and Operational Practices (13%)
- Domain 4 Protection of Information Assets (25%)
- Domain 5 Disaster Recovery and Business Continuity (10%)
- Domain 6 Business Application System Development, Acquisition, Implementation and Maintenance (16%)
- Domain 7 Business Process Evaluation and Risk Management (15%)

Overview of IS Audit Process



Chapter objective is to ensure the candidate “has the knowledge necessary to plan and conduct IS audits in accordance with generally-accepted information systems audit standards and audit guidelines to provide a statement of assurance that the organisation’s IT and business systems are adequately controlled , monitored and assessed”

- Audit mission and planning
- Laws and regulations
- ISACA standards and guidelines for IS auditing
- Risk analysis
- Internal controls
- Performing an IS audit

Overview of Management, Planning and Organisation of IS



Chapter objective is to “ensure that the CISA candidate understands and can evaluate the strategies, policies, standards, procedures and related practices for the management, planning and organisation of IS”

- Information Systems Strategy
- Policies and Procedures
- IS Management Practices
- IS Organisational Structure and Responsibilities
- Auditing the Management, Planning and Organisation of IS

Overview of Technical Infrastructure and Operational Practices



Chapter objective is to ensure that the CISA candidate “has the knowledge necessary to evaluate the effectiveness and efficiency of an organisation’s implementation and ongoing management of technical and operational infrastructure to ensure that they adequately support the organization’s business objectives”

- Information Systems Hardware
- Information Systems Architecture and Software
- Information Systems Network Infrastructure
- Information Systems Operations
- Auditing Infrastructure and Operations

Overview of Protection of Information Assets



Chapter objective is to ensure that the CISA candidate “has the knowledge to evaluate the organisation’s logical, environmental and IT infrastructure security”

- Importance of Information Security Management
- Logical access exposures and controls
- Network infrastructure security
- Auditing information security management and logical access issues and exposures
- Auditing network infrastructure security
- Environmental exposures and controls
- Physical access exposures and controls
- Laptop security access issues

Overview of Disaster Recovery and Business Continuity



Chapter objective is to ensure that the candidate “has the knowledge to evaluate the organisation’s ability to restore services to an agreed level of quality, and the process for developing, communicating and maintaining documented and tested plans for the continuity of business operations and IS processing”

- Recovery/Continuity planning process
- Disaster events
- Organisation and assignment of responsibilities
- Components of an effective business continuity plan
- Recovery/Continuity plan testing
- Auditing Recovery/Continuity plans

Overview of Business Application System Development, Acquisition, Implementation and Maintenance



Chapter objective is to ensure that the CISA candidate “has the knowledge to evaluate the methodology and processes by which the business application system development, acquisition, implementation and maintenance are undertaken to ensure that they meet the organisation’s business objectives”

- Business application development
- Alternative software development strategies
- Information systems maintenance practices
- Project management practices
- System development tools and productivity aids
- Software development process improvement practices
- Auditing systems development, acquisition and maintenance

Overview of Business Process Evaluation and Risk Management



Chapter objective is to ensure that the CISA candidate “has the knowledge necessary to evaluate business systems and processes to ensure that risks are managed in accordance with the organisation’s business objectives”

- Business process re-engineering and process change projects
- Risk management
- IT governance
- Application controls
- Business Application Systems

2004 CISA results - Ireland



- 29 people sat the exam in Ireland in 2003
- 23 people passed
- Better than global average (50% pass rate)
- To date 135 people have passed the exam in Ireland – 41 of whom are certified.

CISM Certification

Details



CISM Target Market



- What is the CISM Target Market?

Individuals who design, implement and manage an enterprise's information security program.

- Security managers
 - Security directors
 - Security officers
 - Security consultants
- Over 5,000 CISM certified in first 2 years
 - Certification Magazine, November 2003, recognised CISM among its “top ten” Best New Programs or Certifications

CISM General Requirements



Certified Information Security Manager (CISM)

Criteria

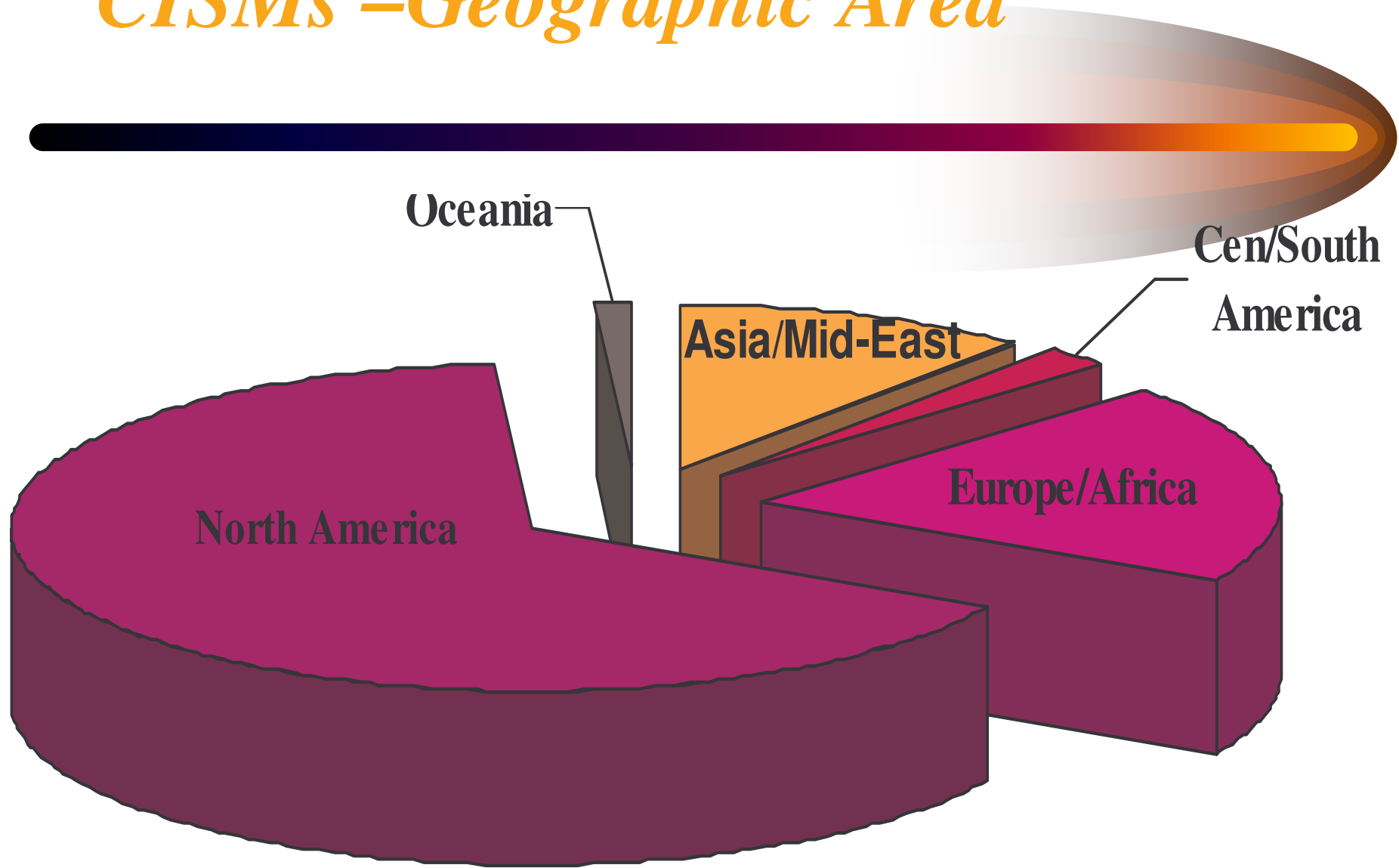
- Pass exam
- Submit verified evidence of a minimum of five years of information security work experience
- Adhere to ISACA *Code of Professional Ethics*
- Comply with continuing education policy

*Prominent CISM*s

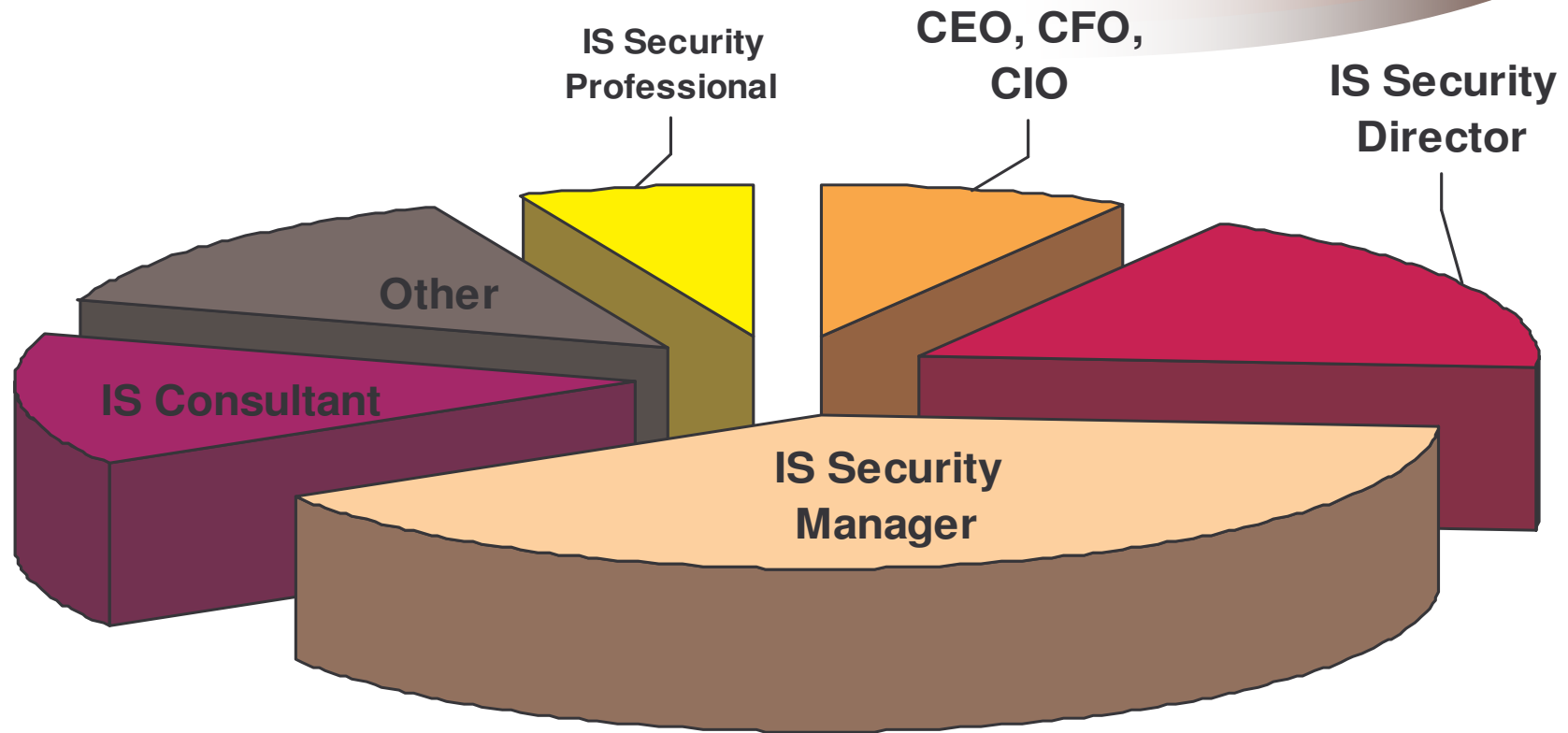


- Howard A. Schmidt, CISM, vice president of security for eBay
- Eugene Schultz, CISM, principal engineer with Lawrence Berkeley National Laboratory
- Fred Piper, CISM, director of the Royal Holloway College (University of London) Information Security Group
- Ted Humphreys, CISM, involved with the development of the British Standard (BS) 7799
- Bill Caelli, CISM, head, School of Data Communications and founder of the Information Security Research Centre, Queensland University
- Robert Clyde, CISM, chief technology officer, Symantec Corporation
- Dorothy Denning, CISM, professor, Department of Defense Analysis, Naval Postgraduate School
- Jae Woo Lee, CISM, professor, Dongguk University IAI
- Bart Preneel, CISM, researcher, Katholieke Universiteit Leuven, Belgium

CISMs – Geographic Area



CISMs by Job Title



Summary of CISM Areas



- ***Information Security Governance (21%)*** – establish and maintain a framework to align IS strategies with business objectives, laws and regulations.
- ***Risk Management (21%)*** – identify and manage IS risks to achieve business objectives.
- ***Information Security Program(me) Management (21%)*** – design, develop and manage an IS programme to implement the IS governance framework.
- ***Information Security Management (24%)*** – oversee & direct IS activities to execute the IS programme.
- ***Response Management (13%)*** – develop and manage a capability to respond to and recover from disruptive IS events.

CISM and CISA Exam Details



Types of questions on the CISM & CISA Exam



- Each exam consists of 200 questions administered over a four-hour period
- Questions are designed to test practical knowledge and experience
- All questions are multiple choice
- Questions require the candidate to choose one best answer
- Every question has a stem (question) and four options (answer choices)

Exam Tips



- Answer all questions
 - No points docked for wrong answers
 - 25% chance of getting it right
- Ensure that the number on the booklet corresponds with the number on the answer sheet

Examination advice



- Be physically prepared
- Read the question carefully
- **Read the question carefully** (not repeated by accident)
 - Don't anticipate what they should be asking. Don't contextualise
- Understand the question – before you read the options
 - There should be no trick questions
- Don't panic
 - If you aren't sure of the answer, move on to the next question

Examination advice



- Take your time
 - But not too long. Pace yourself. Work out the timing “How long do I have per question?”, “How long do I have to review my answers?”
 - Leave time to review your answers after you’ve finished (at least once)
- Remember what they told you in school
 - If you get stuck, move on
 - There’s only one right answer. ALWAYS. If you think that more than one answer is correct, choose the one that’s MOST correct
- Don’t argue. Leave your ego behind
 - It’s not the time while you have work to do
 - Give feedback when you’re finished, if you have time.

Study Advice



- Obtain the CISA & CISM review manual; CISA & CISM review questions, answers; and CISA explanations CD ROM
- Assess your weakest areas, and concentrate on studying for those areas
 - Acquire the leading reference material for the domain
- Practice the test questions
- Don't try and cheat yourself, or don't get too cocky
- Get involved in a project at work that involves your domains of least knowledge (if you can)
 - Learning is so much easier than studying
- Don't panic (You have a life)
- Everyone can only do their best on the day (nobody should expect to get 100%)
- **Enjoy the exam.** It an opportunity for you to challenge your knowledge in your chosen area of expertise

Administration of the Examination



- Administered on Saturday, 11th June 2005
- 200 Multiple Choice Questions
- CISA exam – can be attempted in Dutch, English, French, German, Hebrew, Italian, Chinese, Japanese, Korean, and Spanish languages
- CISM exam – can only be attempted in English at present
- 4 hours
- Approximately 170 Test Sites in 57 Countries
- The examination in Ireland is held in St Patricks college, Drumcondra
- Passing Mark of 75 (scaled score)
- Results received approximately 10 weeks after the exam

Exam Costs



Registration Fees and Payment

- Early registrations received before 2 February 2005:
ISACA Member: US \$335.00
Non-Member: US \$455.00
- Final registrations received by 30 March 2005:
ISACA Member: US \$385.00
Non-Member: US \$505.00
- Application form available at www.isaca.org
Register Online and save US \$ 35 on the Registration Fee

Study aids



- CISA & CISM Review Technical Information Manual 2004
- CISA CD ROM – 600 questions
- CISA & CISM Questions, Answers and Explanations (QAE) Manual (100 sample questions)
- Order when applying for the exam
- For information on other study aids see www.isaca.org

Certification Requirements



Certification CISA Requirements



- Successful completion of the CISA examination
- Minimum of 5 years of Information Systems Audit, Control or Security experience within 10 years of applying and within 5 years of passing exam
- Compliance with the Information Systems Audit and Control Association Code of Professional Ethics

Certification CISA Requirements



Substitutions:

- Work experience can be substituted if:
 - 1 year of data processing or 1 year of auditing experience can be substituted for 1 year of Information Systems Audit, Control or Security experience.
 - Associate or Bachelor's degree (equivalent of 60-120 credit hours) can be substituted for 1 or 2 years.
 - Each 2 years as a full time college or university professor or instructor in a related field (e.g. computer science, accounting, information systems auditing) can be substituted for 1 year Information Systems Audit, Control or Security experience.

Application for CISA Certification



- Sent to all who pass the examination
- Contains:
 - Requirements for Certification
 - Code of Professional Ethics
 - Instructions for Completion of Form
 - Verification of Work Experience for Applicant Form
 - Application for Certification as an Information Systems Auditor

Certification CISM Requirements



- Successful completion of the CISM examination
- Submit verified evidence of 5 years of work experience in the field of Information Security.
 - 3 of the 5 years has to gained performing the role of an IS manager.
 - Experience must be broad and gained in 3 of the 5 job practice areas.
 - Experience gained within 10 year preceding the application for certification or within 5 years of passing CISM exam.

Certification CISM Requirements



Substitutions:

- Max of 2 years of work experience can be substituted if:
 - Post graduate degree in Information Security or related field (e.g. business admin, information assurance, information systems)
 - CISA in good standing
 - CISSP in good standing
- Max of 1 year of work experience can be substituted if:
 - Skills based security certificate held (e.g. SANS GIAC, MCSE, CompTIA Security, CBCP)

CISM & CISA Continuing Education Policy Details



Continuing Education Requirements



Certification is granted annually to those who:

- annually report a minimum of 20 hours of continuing professional education
- annually pay the continuing education maintenance fee
- comply with the *ISACA Code of Professional Ethics*
- report a minimum of 120 contact hours of continuing education for each fixed three-year period

ISACA Code of Professional Ethics



Members and ISACA certification holders shall:

- Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
- Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
- Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.

ISACA Code of Professional Ethics

(cont'd)



Members and ISACA certification holders shall:

- Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
- Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
- Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
- Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Assistance and Information



*For more information on the CISA & CISM
exam, contact:*



Fiona Coloe

IIB Bank

IIB House

Sandwith Street

Dublin 2

+353-1-6646728

fiona.coloe@iibbank.ie

Sonja Durnin

KPMG

1 Stokes Place

St. Stephen's Green

Dublin 2

+353-1-4101512

sonja.durnin@kpmg.ie

For more information...



www.isaca.org

*To join the Irish chapter mailing list, please email
jackie.pyatt@kpmg.ie*