

CISA / CISM / CGEIT / CRISC Programs Overview

www.isaca.org/certification

- Founded in 1969 as the EDP Auditors Association
- Since 1978, CISA has been a globally accepted standard of competency among IS audit, control, assurance and security professionals
- More than 86,000 members in over 160 countries
- More than 185 chapters in over 75 countries worldwide



- The American National Standards Institute (ANSI) has awarded accreditation under ISO/IEC 17024 to the Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certification programs. ANSI reaccredited these ISACA programs in 2008, and ISACA is currently under review for recertification. ISACA is planning to pursue ANSI accreditation for the CGEIT certification program in the future.
- Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process.



CISA Certification Details

www.isaca.org/cisa

Why Become A CISA?

- ***Enhanced Knowledge and Skills***
 - To demonstrate your willingness to improve your technical knowledge and skills
 - To demonstrate to management your proficiency and commitment toward organizational excellence
- ***Career Advancement***
 - To obtain credentials that employers seek
 - To enhance your professional image
- ***Worldwide Recognition***
 - To be included with nearly 73,000 other professionals who have gained the CISA designation worldwide

CISA in the Workplace

- Almost 2,400 are now employed in organizations as the CEO, CFO or equivalent executive position
- More than 2,000 serve as chief audit executives (CAEs), audit partners or audit heads
- Nearly 6,000 serve as CIOs, CISOs, security directors, security managers or consultants
- More than 10,500 serve as audit directors, managers or consultants
- More than 15,400 are employed in managerial or consulting positions in IT operations or compliance
- More than 14,400 auditors (IS/IT and non-IS/IT)



Recent CISA Program Recognition

- SC Magazine has named CISA the winner of the Best Professional Certification Program. With almost 700 entries submitted in 30 categories, the 2009 SC Awards were the most competitive yet in the program's 12-year history.
- The CISA certification program was awarded the "Best Professional Development Grand Award" and the "Best Professional Development (Scheme) Award" in the 'Hong Kong ICT Awards 2009' presentation ceremony. The Hong Kong ICT Awards were established in 2006 under a collaborative effort amongst the industry, the academia and the Government.
- In a January 2010 study by Mile High Research, ISACA's CISA and CISM certifications made the top 10 in-demand IT certifications for new jobs posted over the last 14 days. The job descriptions specified one or more certifications as minimum or preferred credentials for the job posting. ISACA and other organizations whose credentials made the top 10 "obviously make a connection between their certifications and employers – that connection is value," said Denny Schall, CLO of Mile High Research.

Recent CISA Program Recognition *(continued)*

- According to bankinfosecurity.com, industry recruitment experts and information security professionals noted CISA and CISM as two of the top five certifications for 2009 as they provide assurance that the holder has extensive experience in their fields above and beyond passing a test.
- CISAs qualify for the Disaster Recovery Institute International's (DRII) CBLA (Certified Business Continuity Lead Auditor) certification and get a bypass for the corresponding reference (experience) requirement. In addition, all CISAs are offered a 10% discount on DRII courses.
- The Securities Exchange Board of India requires biannual system audits of all mutual funds to be conducted by an independent auditor who is CISA/CISM-certified or equivalent.
- CISAs are provided an exemption from the CEH (Certified Ethical Hacker) exam and allowed to automatically take the EC-Council Certified Security Analyst (ECSA) exam which leads to the (LPT) Licensed Penetration Tester Certification.



Other CISA Program Recognition

- The US Dept. of Defense includes CISA in its list of approved certifications for its information assurance professionals
- The US Department of Veteran Affairs reimburses exam fees for the CISA exam
- The Department of Information Technology has issued an empanelment of vendors for auditing the Reserve Bank's internal network and IT systems. CISA was listed as one of the pre-qualification criteria for bidding vendors. It was stipulated that the vendor should have a minimum of three CISA/CISSP certified professionals participating in the audit.
- The Payment Card Industry (PCI) data Security Standard (DSS) has named CISA and CISM certifications as validation requirements for qualified security assessors (OSA's); organizations that validate an entity's adherence to PCI DSS requirements.



Other CISA Program Recognition *(continued)*

- All assistant examiners employed by the US Federal Reserve Banks must pass the CISA exam before they are eligible for commissioning
- The Department of Information Technology of the Government of N.C.T. of Delhi sent out an RFP for Website Security Audits of Delhi Government departments. This is the first large scale audit RFP issued by any state government in India. CISA was named as one of the pre-qualification criteria for bidders.
- The National Stock Exchange of India has recognized CISA as a requirement to conduct system audits
- CERT-IN, the Indian Computer Emergency Response Team, has recognized CISA as one of the requirements to be empanelled to conduct security audits

Other CISA Program Recognition *(continued)*

- An information security law in Korea requires that highly skilled professionals, such as CISAs perform information system audits and security services.
- In Romania, banks desiring to implement distance or electronic payment instruments, such as Internet and home banking, are required by law to be certified by CISA certification-holding auditors.
- Article 58 of the Public Finance act in the Republic of Poland (passed in late 2006) acknowledges the CISA certification as one of three designations recognized by the act as an entitlement to be a public-sector auditor.
- The Peruvian government recognizes CISAs for their expertise and specialization which is required for practitioners in internal auditing.



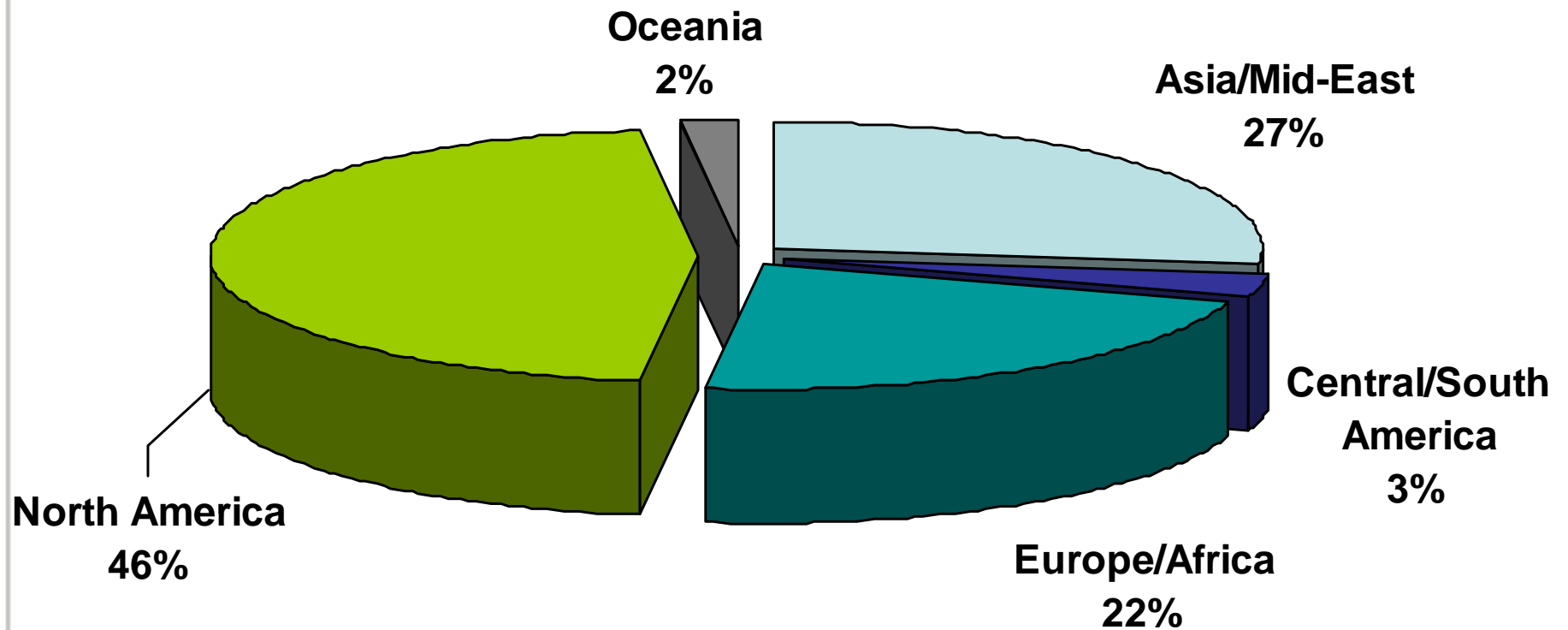
Other CISA Program Recognition *(continued)*

- In Malaysia, the Multimedia Development Corporation (MDEC) provides partial reimbursement for certain CISA and CISM certification and training fees.
- The Canadian Institute of Chartered Accountants (CICA) accredits ISACA as the only body whose designation leads to recognition as a CA-designated specialist in information systems audit, control and security.
- In Hong Kong, ISACA members who have held a CISA certification for at least four years have the right to vote for the city's legislative counselors, as representatives of the IT category among the functional constituencies.
- India's National Information Security Assurance Program, the Department of Information Technology recognizes the CISA designation to assess the information security risks in public sector organizations.

Other CISA Program Recognition *(continued)*

- The Securities and Exchange Commission (SEC) strongly encourages the use of COBIT as a baseline for governance, implementation and planning, and overall IT controls. While certifications are not embedded in guidelines and rules, the CISA certification is strongly encouraged.
- The State Bank of Pakistan offers its employees who earn the CISA credential financial incentives: reimbursement of their examination fees and payment of a cash bonus.
- In Hyderabad, India, the State Bank also offers incentives in the form of exam and maintenance fee reimbursement and a significant honorarium to employees earning and retaining the CISA.
- ISACA worked with the Chinese National Audit Office (CNAO) in 2002 to offer the first CISA exam in the People's Republic of China (PRC). The exam was conducted in four locations in the PRC, in both English and Mandarin Chinese.

CISAs by Area





CISA Job Practice Areas (6)

Note: A CISA job practice analysis is underway to reflect the vital and evolving responsibilities of IT auditors and stay current with the market. Results of this analysis will be incorporated into the June 2011 exam. www.isaca.org/cisa/jpa

- **IS Audit Process – 10%**

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

- **IT Governance – 15%**

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

- **Systems and Infrastructure Lifecycle – 16%**

To provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance, and disposal of systems and infrastructure will meet the organization's objectives.

CISA Job Practice Areas (continued)

- **IT Service Delivery and Support – 14%**
To provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives.
- **Protection of Information Assets – 31%**
To 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%**
To 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 minimizing the business impact.

For complete details visit: www.isaca.org/cisajobpractice

CISA Certification Requirements

- Earn a passing score on the CISA Exam
- Have a minimum of five years of verifiable IS audit, control or security experience (substitutions available)
- Submit the CISA application and receive approval
- Adhere to ISACA's *Code of Professional Ethics*
- Abide by *IS Auditing Standards* as adopted by ISACA
- Comply with *CISA Continuing Professional Education Policy*



CISM Certification Details

www.isaca.org/cism

CISM Certification Current Facts

- More than 12,500 CISM^s worldwide
- The CISM exam is offered in 4 languages (English, Japanese, Korean and Spanish) in 240+ locations

What makes CISM Unique?

- Designed for information security managers exclusively
- Criteria and exam developed from job practice analysis validated by information security managers
- Experience requirement includes information security management

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
- Security staff

Recent CISM Recognition

- In a January 2010 study by Mile High Research, ISACA's CISA and CISM certifications made the top 10 in-demand IT certifications for new jobs posted over the last 14 days. The job descriptions specified one or more certifications as minimum or preferred credentials for the job posting. ISACA and other organizations whose credentials made the top 10 "obviously make a connection between their certifications and employers – that connection is value," said Denny Schall, CLO of Mile High Research.
- CISM gets a bypass for references (experience) for the Disaster Recovery Institute International's (DRII) CBCA (Certified Business Continuity Auditor) certification.
- The Securities Exchange Board of India requires biannual system audits of all mutual funds to be conducted by an independent auditor who is CISA/CISM-certified or equivalent.
- Those who hold the CISM or CISA certification and are in good standing with ISACA can apply for the Level 1 HISPI credential through the prerequisite track and are not required to attend the five-day HISP Certification Course.

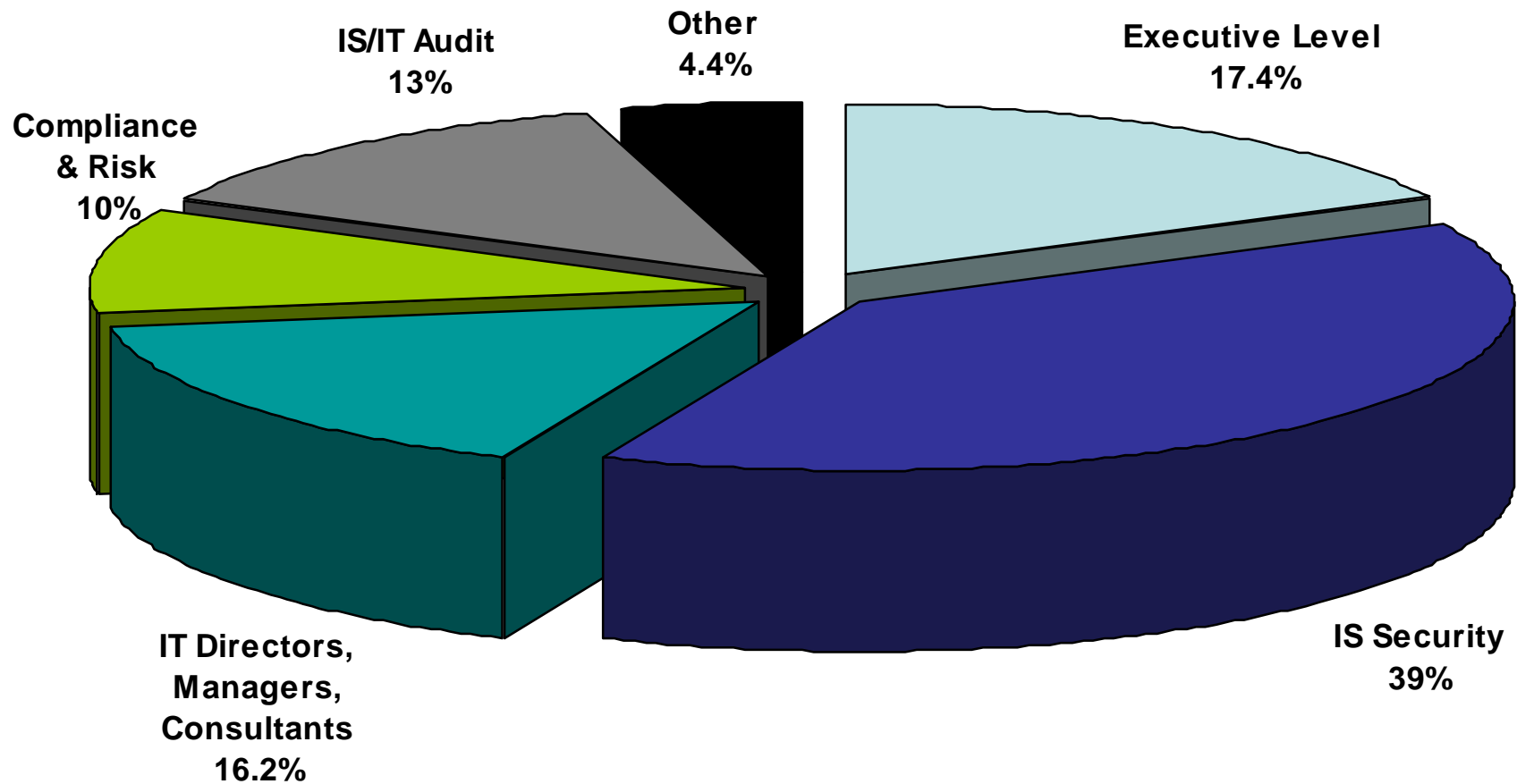
Recent CISM Recognition

(continued)

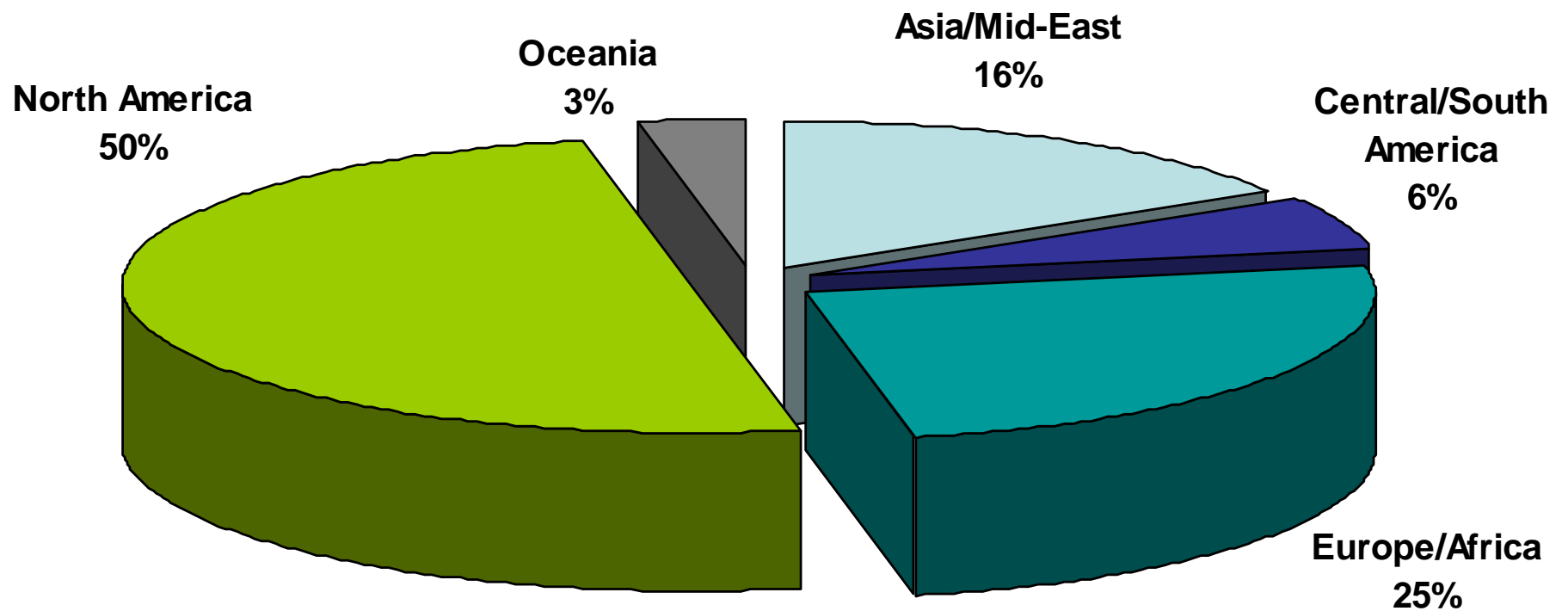
- CIO Magazine, SC Magazine and Foote Partners research continually cite CISM as a credential that earns top pay when compared to other credentials.
 - In April 2009, the Foote Partners “Salary Survey” ranked the CISM certification as the highest paying IT Security certification. CISM was also found to be the only security certification to gain value within the past twelve months.
- Certification Magazine’s 2008 and 2009 salary survey ranked the CISM certification as the third highest paying certification.
- CISM has also been recognized in the following publications as a unique security management credential:
 - Information Security Magazine
 - CSO Magazine Online
 - Computerworld Today (Australia)
 - eWeek
 - Security Magazine (Brazil)
 - Cramsession.com

- CISM was named as a finalist for the 2008 and 2009 *SC Magazine* Best Professional Certification Program.
- The Securities Exchange Board of India requires biannual system audits of all mutual funds to be conducted by an independent auditor who is CISA/CISM-certified or equivalent.
- Those who hold the CISM or CISA certification and are in good standing with ISACA can apply for the Level 1 HISPI credential through the prerequisite track and are not required to attend the five-day HISP Certification Course.
- The Multimedia Development Corporation Sdn Bhd (MDEC) in Malaysia provides reimbursement for certain CISA and CISM certification and training fees. This reimbursement is made possible through the MSC Malaysia Capability Development Program, which was launched to enhance the skills of local information and community technology knowledge workers and assist MSC status companies in human capital development.

CISMs by Job Title



CISMs by Geographic Area



CISM Job Practice (5)

(Effective December 2007)

- 1. Information Security Governance (23%)** - Establish and maintain a framework to provide assurance that information security strategies are aligned with the business objectives and consistent with applicable laws and regulations.
- 2. Information Risk Management (22%)** - Identify and manage information security risks to achieve business objectives.
- 3. Information Security Program Development (17%)** - Create and maintain a program to implement the information security strategy.
- 4. Information Security Program Management (24%)** - Design, develop and manage an information security program to implement the information security governance framework.
- 5. Incident Management and Response (14%)** - Plan, develop and manage a capability to detect, respond to and recover from information security incidents.

For complete details visit www.isaca.org/cismjobpractice

CISM General Requirements

- Earn a passing score on the exam
- Submit verified evidence of a minimum of five years of information security work experience
- Submit the CISM application and receive approval
- Adhere to ISACA *Code of Professional Ethics*
- Comply with ISACA's *CISM Continuing Professional Education Policy*



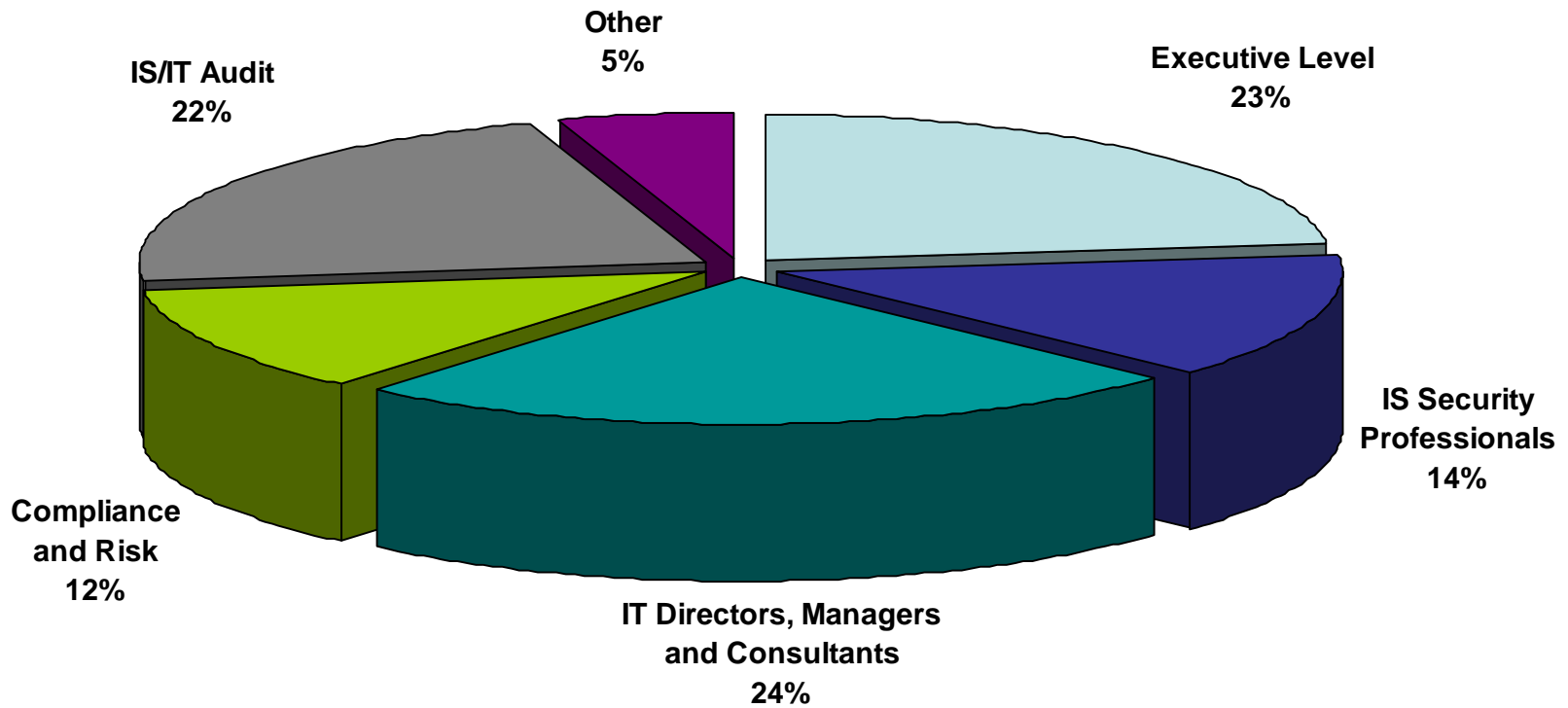
CGEIT Certification Details

www.isaca.org/cgeit

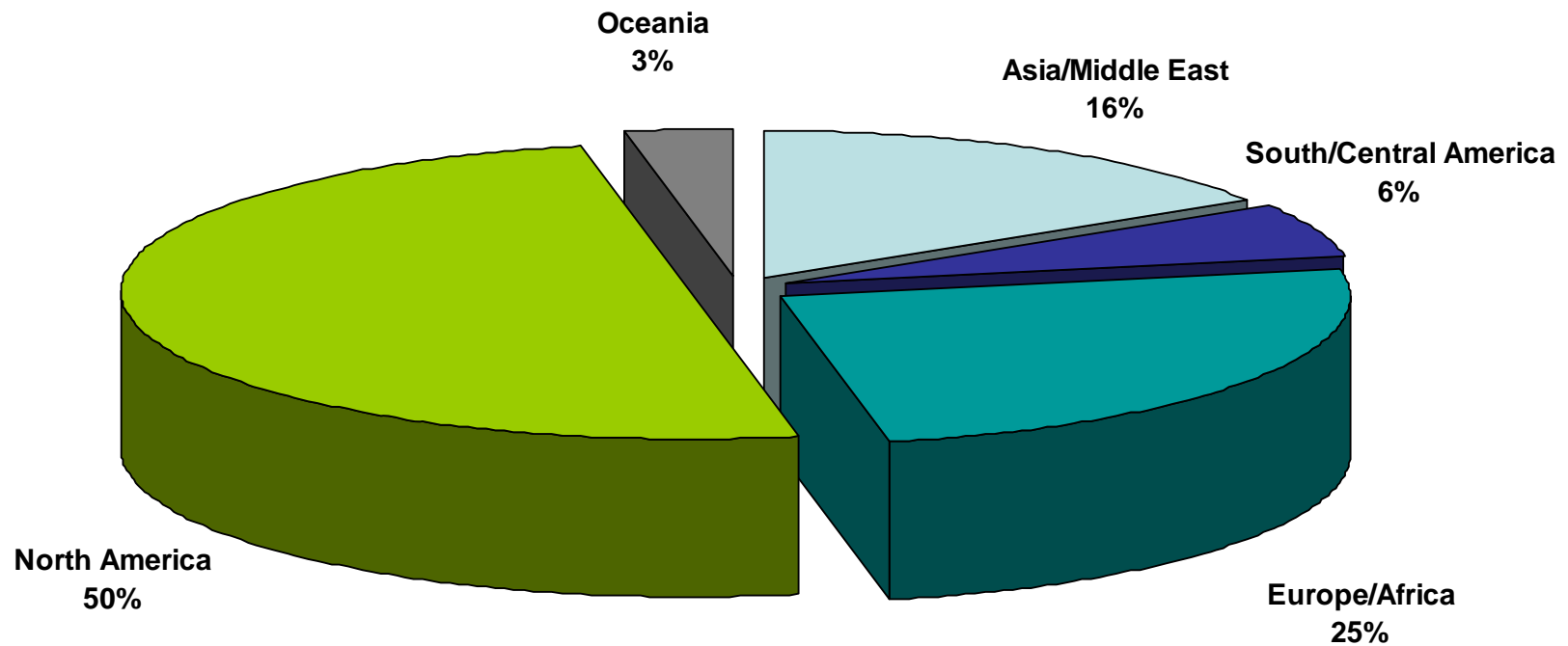
Market Need for CGEIT

- ***Individual***
 - ✓ Defines the roles and responsibilities of professionals performing IT governance work and recognizes their professional knowledge and competencies; skill-sets; abilities and experiences
- ***Enterprise***
 - ✓ Supports through the demonstration of a visible commitment to excellence in IT governance practices
- ***Business***
 - ✓ Increases the awareness of IT governance good practices and issues
- ***Profession***
 - ✓ Supports those that provide IT governance management, advisory or assurance direction and strategy

CGEITs by Job Category



CGEITs by Geographical Area



CGEIT: Who is it for?

The CGEIT certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. It is designed for professionals who have management, advisory, or assurance responsibilities as defined by the CGEIT Job Practice consisting of IT governance related task and knowledge statements.

CGEIT Job Practice (6)

- 1. IT Governance Framework** - Develop, or be part of the development of, an IT governance framework that includes the following responsibilities and tasks.
- 2. Strategic Alignment** - Develop, or be part of the development of, an enterprise's IT strategy that includes the following responsibilities and tasks.
- 3. Value Delivery** - Develop, or be part of the development of, a systematic, analytical and continuous value governance process that includes the following responsibilities and tasks.

- 4. Risk Management** - Develop, enhance and maintain a systematic, analytical and continuous enterprise risk management process across the enterprise that includes the following responsibilities and tasks.

- 5. Resource Management** - Develop, or assist in the development of systematic and continuous resource planning, management and evaluation processes that include the following responsibilities and tasks.

- 6. Performance Measurement** - Develop, or assist in the development of, systematic and continuous performance management and evaluation processes that include the following responsibilities and tasks.

For more complete details visit www.isaca.org/cgeitjobpractice

CGEIT Experience Requirements

- Earn a passing score on the CGEIT exam
- Submit verified evidence of the five year experience requirement as defined by the *CGEIT Job Practice*
- Submit the CGEIT application and receive approval
- Adhere to the *ISACA Code of Professional Ethics*
- Comply with the *CGEIT Continuing Education Policy*
- Comply with *Information Systems Auditing Standards*



CISA, CISM and CGEIT Exam Details



Administration of the CISA, CISM and CGEIT Exams

Next exams:

Saturday, 12 June 2010

Saturday, 11 December 2010

- More than 240 test sites offered for each exam administration
- Offered in every city where there is an ISACA chapter or a large interest by individuals to sit for the exam
- Passing mark of 450 on a common scale of 200 to 800





2010 Registration Fees:

12 June 2010

Early Registration: *On or before 10 February 2010:*

- ISACA Member: US \$415.00
- Non-Member: US \$545.00

Final Registration: *After 10 February 2010, but on or before 7 April 2010:*

- ISACA Member: US \$465.00
- Non-Member: US \$595.00

Register Online at www.isaca.org/examreg

- Online registration via the ISACA web site is encouraged, as candidates will save US \$50.
- Non-members can join ISACA at the same time, which maximizes their savings.

Exam registration fees must be paid in full to sit for the exams. Those whose exam registration fees are not paid will not be sent an exam admission ticket and their registration will be cancelled.



2010 Registration Fees: 11 December 2010

Early Registration: *On or before 18 August 2010*

- ISACA Member: US \$415.00
- Non-Member: US \$545.00

Final Registration: *After 18 August, but on or before 6 October 2010:*

- ISACA Member: US \$465.00
- Non-Member: US \$595.00

Register Online at www.isaca.org/examreg

- Online registration via the ISACA web site is encouraged, as candidates will save US \$50.
- Non-members can join ISACA at the same time, which maximizes their savings.

Exam registration fees must be paid in full to sit for the exams. Those whose exam registration fees are not paid will not be sent an exam admission ticket and their registration will be cancelled.

Bulletin of Information and Registration Form

- There is a *Bulletin of Information* for each exam administration for each exam.
- Can be downloaded from ISACA web site – www.isaca.org/cisaboi, www.isaca.org/cismboi or www.isaca.org/cgeitboi.
- Is available in the languages offered for CISA, CISM or CGEIT exam

Bulletin Includes:

- | | |
|----------------------------------|-------------------------|
| ✓ Requirements for certification | ✓ Test date procedures |
| ✓ Exam description | ✓ Score reporting |
| ✓ Registration instructions | ✓ Test center locations |
| | ✓ Registration form |

Types of Questions on the CISA, CISM and CGEIT Exams

- The CISA and CISM exam consists of 200 multiple choice questions administered over a four-hour period.
- The CGEIT exam consists of 120 multiple choice questions administered over a four-hour period.
- Questions are designed to test practical knowledge and experience
- Questions require the candidate to choose one best answer
- Every question or statement has four options (answer choices)

Quality of the Exam Ensured by:

- ***Job Analysis Study***: determines content
- ***Test Development Standards***: ensures high standards for the development and review of questions
- ***Review Process***: provides two reviews of questions by independent committees before acceptance into pool
- ***Periodic Pool Cleaning***: ensures that questions in the pool are up-to-date by continuously reviewing questions
- ***Statistical Analysis of Questions***: ensures quality questions and grading by analyzing exam statistics for each language



CISA, CISM and CGEIT Continuing Professional Education (CPE) Policy Details



Continuing Professional Education (CPE) Requirements

Certification is renewed annually to those who:

- Report a minimum of 120 hours of continuing professional education (CPE) for each fixed three-year period, with a minimum of 20 hours in each year.
- Report hours annually, in the year they are earned. Hours are reported annually during the renewal process.
- Pay the continuing professional education maintenance fee
- Comply with the ISACA Code of Professional Ethics

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.
- 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.

Members and ISACA certification holders shall:

- 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.

First CRISC Exam will be in 2011

- The Certified in Risk and Information Systems Control™ certification (CRISC™) is intended to recognize a wide range of professionals for their knowledge of enterprise risk and their ability to design, implement, monitor, and maintain IS controls to mitigate such risk. It is particularly designed for IT professionals who have hands-on experience with risk identification, assessment, and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance.
- The CRISC designation will not only certify professionals who have knowledge and experience identifying and evaluating entity-specific risk, but also aid them in helping enterprises accomplish business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls
- The grandfathering program will run April 2010 through March 2011



ISACA Winnipeg Chapter Support

- **The ISACA Winnipeg Chapter encourages it's members to work toward the ISACA designations available though:**
- The chapter sponsors and subsidizes review courses to help members prepare for the Exams
- The chapter will reimburse ISACA Winnipeg Chapter members registered to write the exams, up to \$160 (Cdn) toward the cost of study materials. This one time benefit is only available to those who have been ISACA Winnipeg Chapter members since March 31 of the reimbursement year and are not receiving reimbursement from their employer. An acceptable receipt is required in support of a claim for reimbursement.
- The Chapter Directors arrange to have designation certificates framed (at chapter expense) for ISACA Winnipeg Chapter members granted their designation each year. The framed Certificates are presented at annual recognition luncheon.



ISACA Membership Pays

- Save on the cost of Exams
- Save on the cost of books and study materials
- Save on the cost of CPEs and Review Courses
 - Save on the cost of Conferences

CISA/CISM & CGEIT videos can be viewed at:

<http://www.isaca.org/Template.cfm?Section=Certification&Template=/ContentManagement/ContentDisplay.cfm&ContentID=51252>

Want to know more? Please contact us at:

ISACA
3701 Algonquin Road
Suite 1010
Rolling Meadows, IL 60008 USA

Phone: (847) 660-5660
Fax: (847) 253-1443
E-mail: certification@isaca.org
membership@isaca-wpg.org
Web site: www.isaca.org
www.isaca-wpg.org