

CISA/CISM/CGEIT

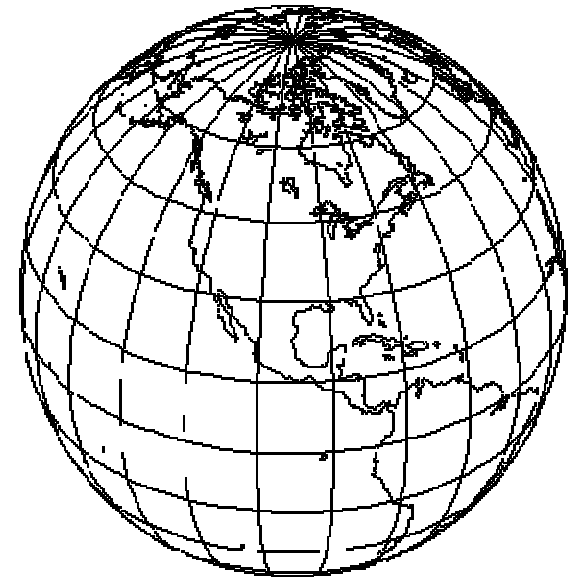
Programs Overview

Prof. Ing. Claudio CILLI

CISA, CISM, CGEIT, CISSP, CSSLP, CIA, M.Inst.ISP

ISACA Facts

- 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 175 chapters in over 70 countries worldwide





ANSI Accreditation

- 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. 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

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 over 60,000 other professionals who have gained the CISA designation worldwide

CISA in the Workplace

- More than 2,000 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
- More than 5,000 serve as CIOs, CISOs, security directors, security managers or consultants
- More than 9,200 serve as audit directors, managers or consultants
- More than 14,000 are employed in managerial or consulting positions in IT operations or compliance
- More than 14,000 auditors (IS/IT and non-IS/IT)



Recent CISA Program Recognition – Top Pay

- CIO Magazine, SC Magazine and Foote Partners research continually cite CISA as a credential earning that earns top pay among other credentials
- In Certification Magazine's 2008 salary survey, both CISA and CISM certifications ranked in the top five highest paying certifications
- Pay for auditing certifications such as the Certified Information Systems Auditor (CISA) will continue to be boosted by stiff compliance requirements and independent auditor control provisions



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)

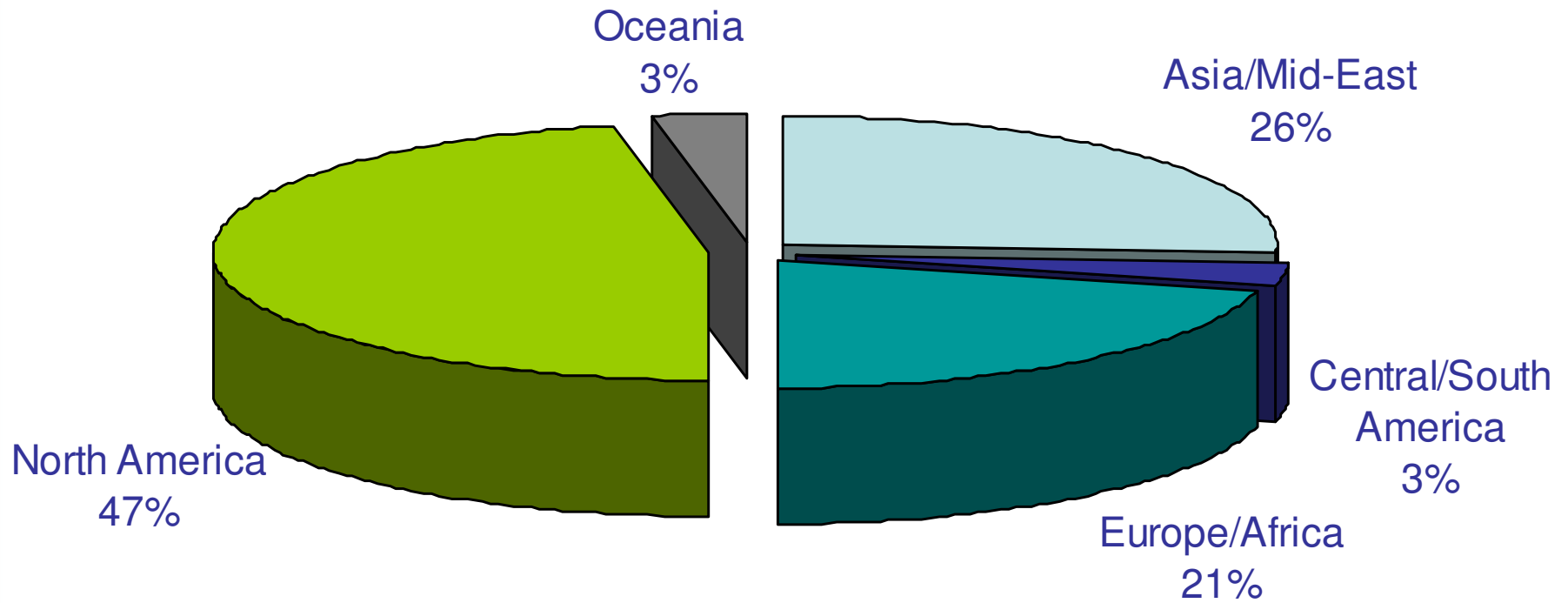
- In Malaysia, the Multimedia Development Corporation (MDEC) provides partial reimbursement for certain CISA and CISM certification and training fees.
- The Canadian Institute of Chartered Accountants (CICA) accredits ISACA as the only body whose designation leads to recognition as a CA-designated specialist 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

- **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.
- **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.



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

CISM Certification Current Facts

- More than 10,000 CISM^s worldwide
- The CISM exam is offered in 4 languages (English, Japanese, Korean and Spanish) in 260+ 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?

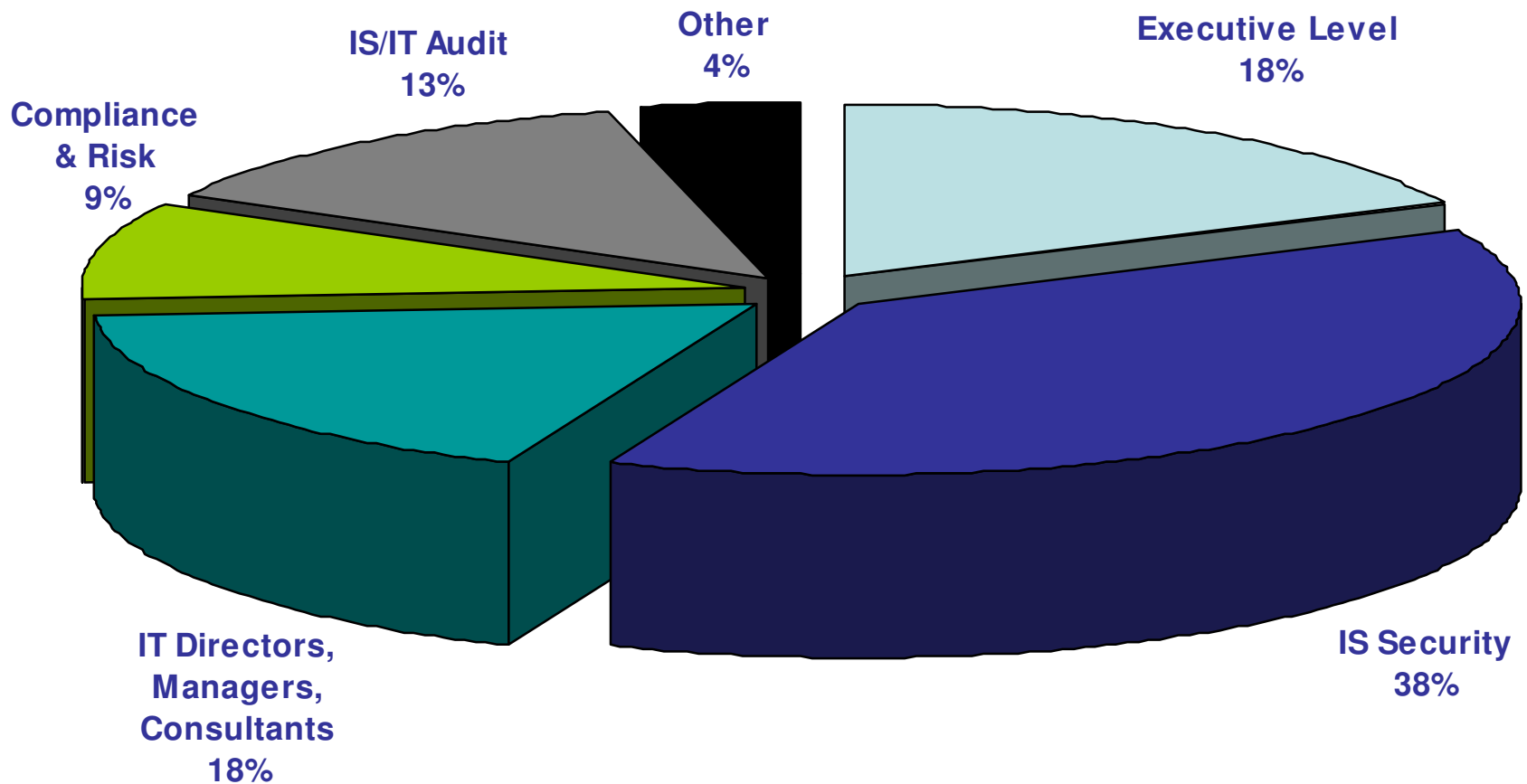
Individuals who design, implement and manage an enterprise's information security program.

- Security managers
- Security directors
- Security officers
- Security consultants
- Security staff

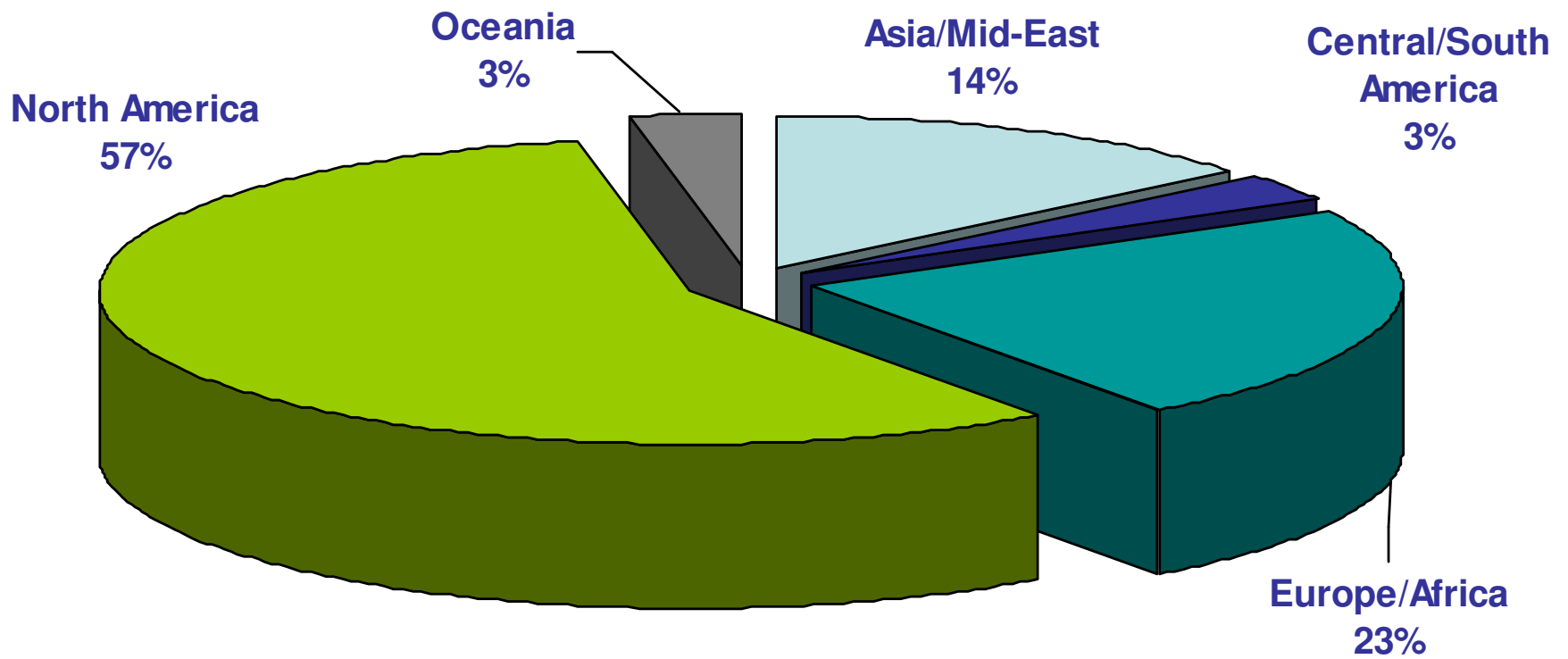
Recent CISM Recognition

- The US Department of Defense (DoD) includes the CISM certification in its list of approved certifications for its information assurance professionals.
- *SC Magazine* selected CISM as a finalist for its 2008 Awards in the "Best Professional Certification Program" category. CISM was chosen as a finalist by a panel of 18 chief information security officers (CISOs) at major corporations and large public-sector organizations.
- CIO Magazine, SC Magazine and Foote Partners research continually cite CISA as a credential earning that earns top pay among other credentials
- In Certification Magazine's 2007 salary survey, CISA and CISM ranked in the top five highest paying certifications.
- CISM recognized in the following publications as a unique security management credential:
 - Information Security Magazine
 - CSO Magazine Online
 - eWeek
 - Computerworld Today (Australia)
 - Security Magazine (Brazil)
 - Cramsession.com

CISMs by Job Title



CISM[®]s by Geographic Area



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*

CISM Job Practice

(Effective December 2007)

- **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.
- **Information Risk Management (22%)** - Identify and manage information security risks to achieve business objectives.
- **Information Security Program Development (17%)** - Create and maintain a program to implement the information security strategy.
- **Information Security Program Management (24%)** - Design, develop and manage an information security program to implement the information security governance framework.
- **Incident Management and Response (14%)** - Plan, develop and manage a capability to detect, respond to and recover from information security incidents.

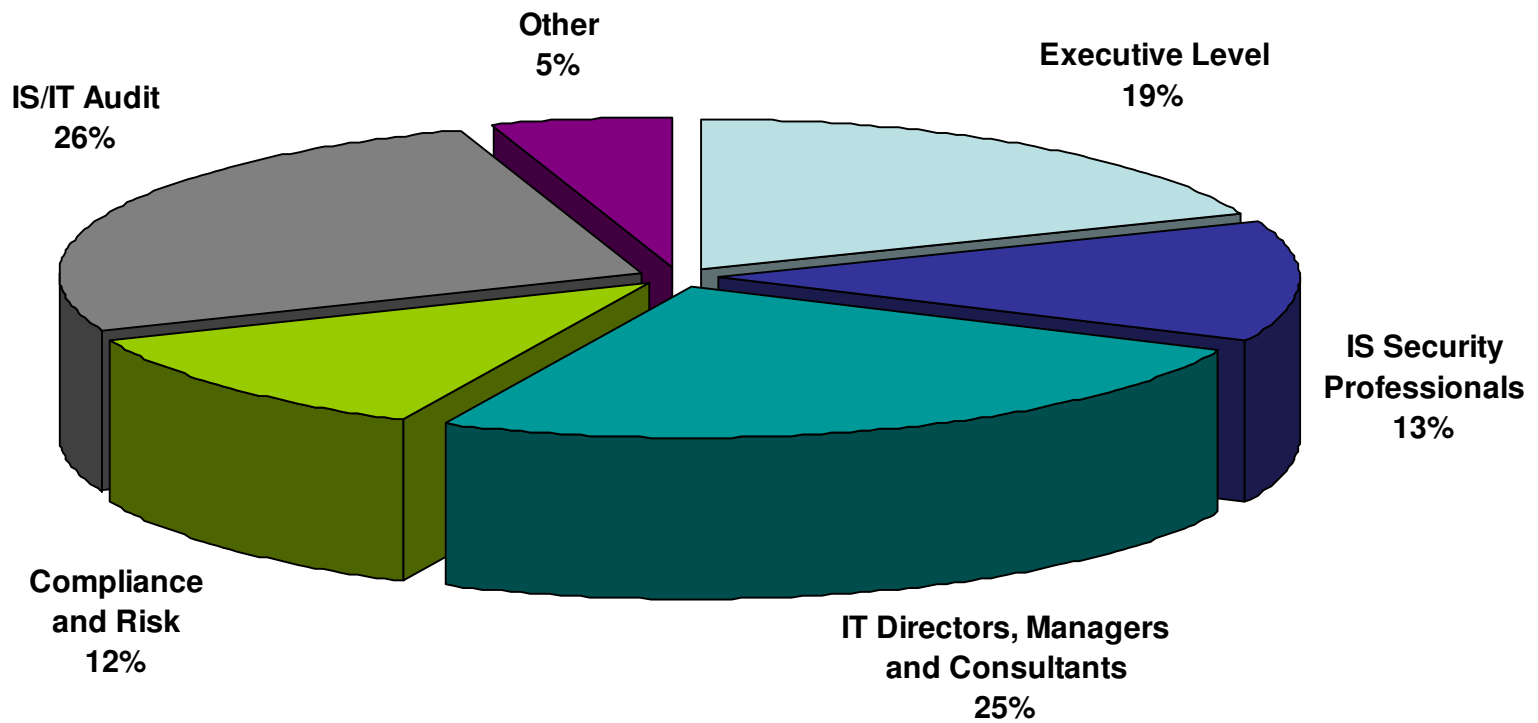


CGEIT Certification Details

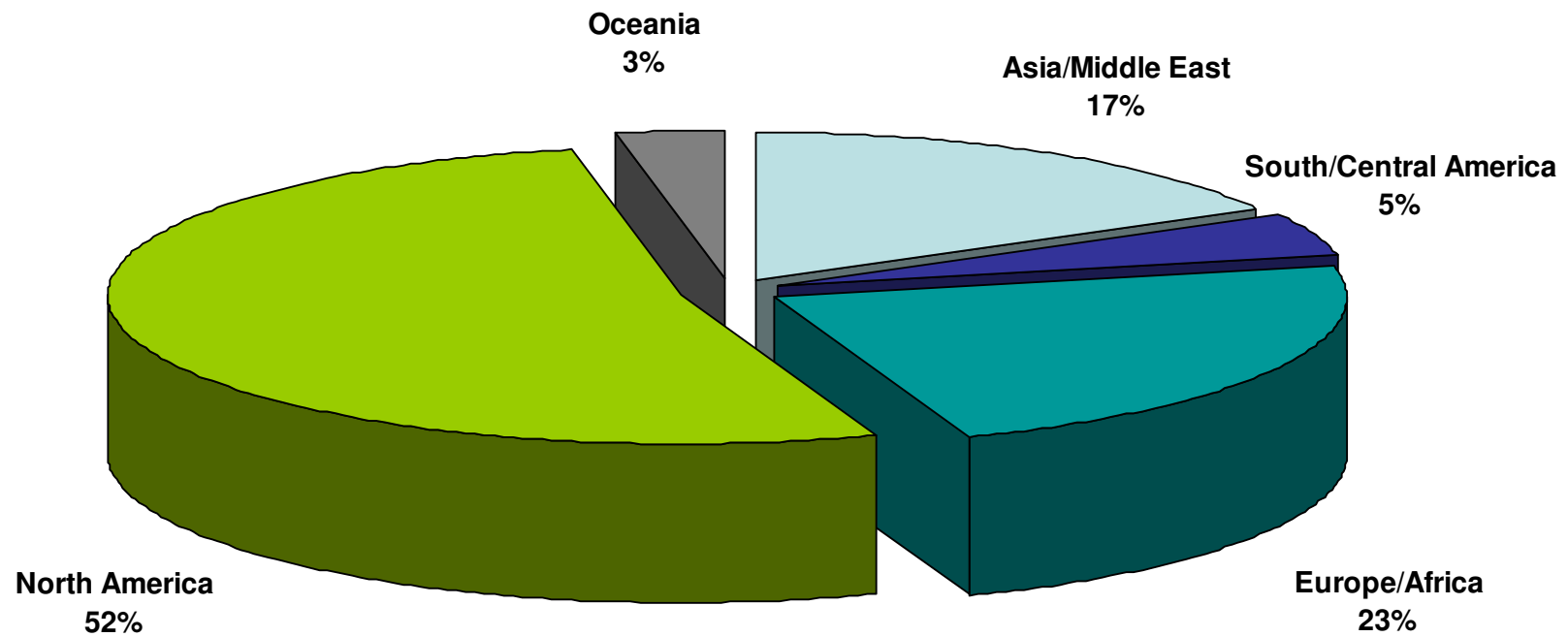
Market Need for CGEIT

- ***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.

Job Practice: A job practice serves as the basis for the exam and the experience requirements to earn the CGEIT certification. Each job practice consists of task and knowledge statements, organized by domains and are intended to depict the tasks performed by individuals who have a significant management, advisory, or assurance role relating to the governance of IT and the knowledge required to perform these tasks. The domains are as follows:

1. IT Governance Framework (required)
2. Strategic Alignment
3. Value Delivery
4. Risk Management
5. Resource Management
6. Performance Measurement

IT Governance Framework

Domain 1 -- IT Governance Framework: Develop, or be part of the development of, an IT governance framework that includes the following responsibilities and tasks.

- Define the requirements and objectives for, and drive the establishment of, IT governance in an enterprise, considering values, philosophy, management style, IT awareness, organization, standards and policies.
- Ensure that an IT governance framework exists and is based on a comprehensive and repeatable IT process and control model that are aligned with the enterprise governance framework.
- Establish appropriate management governance structures, such as an enterprise investment committee, IT strategy committee, IT steering committee, technology council, IT architecture review board, business needs committee and IT audit committee.
- Ensure that the enterprise and IT governance frameworks enable the enterprise to achieve optimal value for the enterprise.
- Confirm that the IT governance framework ensures compliance with applicable external requirements and ethical statements that are aligned with, and confirm delivery of, the enterprise's goals, strategies and objectives.
- Obtain independent assurance that IT conforms with relevant external requirements; contractual terms; organizational policies, plans and procedures; generally accepted practices; and the effective and efficient practice of IT.
- Apply IT best practices to enable the business to achieve optimal value from implementation of IT services and IT-enabled business solutions.
- Ensure the establishment of a framework for IT governance monitoring (considering cost/benefits analyses of controls, return on investment for continuous monitoring, etc.), an approach to track all IT governance issues and remedial actions to closure, and a lessons-learned process.
- Ensure that appropriate roles, responsibilities and accountabilities are established and enforced for information requirements, data and system ownership, IT processes, and benefits and value realization.
- Report IT governance status and issues, and effect transparency in reporting.
- Establish a communications plan to continuously market, communicate and reinforce the need and value of IT governance across the enterprise.

Domain 2 -- Strategic Alignment: Develop, or be part of the development of, an enterprise's IT strategy that includes the following responsibilities and tasks.

- Define and implement a strategic planning framework, requiring and facilitating collaborative and integrated business and IT management planning.
- Actively support/promote and participate in IT management planning by employing best practice enterprise architecture (EA) frameworks.
- Ensure that appropriate policies and procedures are in place, understood and followed to support IT and business strategic alignment.
- Identify and take action on barriers to strategic alignment.
- Ensure that effective communication and engagement exists between business and IT management regarding shared strategic initiatives and performance.
- Ensure business and IT goals cascade down through the enterprise into clear roles, responsibilities and actions.
- Assist senior management by aligning IT initiatives with business objectives and facilitating prioritization of business strategies that optimally achieve business objectives.
- Identify and monitor the interdependencies of strategic initiatives and their impact on value delivery and risk.
- Ensure that the strategic planning process is adequately documented, transparent and meets stakeholder needs.
- Maintain and update the IT management plans, artifacts and standards for the enterprise.
- Monitor, evaluate and report on the effectiveness of the alignment of IT and enterprise strategic initiatives.
- Monitor and assess current and future technologies and provide advice on the costs, risks and opportunities that they bring.

Domain 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.

- Ensure that business takes ownership and accountability for business cases, business transformation, organizational change, business process operation and benefit realization for all IT-enabled business investments.
- Ensure that all IT-enabled investments are managed as a portfolio of investments.
- Ensure that all IT-enabled investments are managed as programs and include the full scope of activities and expenditures that are required to achieve business value.
- Ensure that all IT-enabled investments are managed through their full economic life cycle so that value is optimized.
- Recognize that different categories of investments need to be evaluated and managed differently.
- Ensure that all IT solutions are developed and maintained effectively and efficiently through the development life cycle to deliver the required capabilities.
- Ensure that all IT services are delivered to the business with the right service levels.
- Ensure that IT services enable the business to create the required business value using assets (people, applications, infrastructure and information) to deliver the appropriate capabilities at optimal cost.
- Define and monitor appropriate metrics for the measurement of solution and service delivery against objectives and for the measurement of benefits realized, and respond to changes and deviations.
- Engage all stakeholders and assign appropriate accountability for delivery of business and IT capabilities and realization of benefits.
- Ensure that IT investments, solutions and services are aligned with the enterprise strategies and architecture.

Domain 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.

- Ensure that IT risk identification, assessment, mitigation, management, communication and monitoring strategies are integrated into business strategic and tactical planning processes.
- Align the IT risk management processes with the enterprise business risk management framework (where this exists).
- Ensure a consistent application of the risk management framework across the enterprise IT environment.
- Ensure that risk assessment and management is included throughout the information life cycle.
- Define risk management strategies, and prioritize responses to identified risks to maintain risk levels within the appetite of the enterprise.
- Ensure that risk management strategies are adopted to mitigate risk and to manage to acceptable residual risk levels.
- Implement timely reporting on risk events and responses to appropriate levels of management (including the use of key risk indicators, as appropriate).
- Establish monitoring processes and practices to ensure the completeness and effectiveness of established risk management processes.

Domain 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.

- Ensure that the requirements for trained resources with the requisite skill sets are understood and are assessed appropriately.
- Ensure the existence of appropriate policies for the training and development of all staff to help meet enterprise requirements and personal/professional growth.
- Develop and facilitate the maintenance of systems to record the resources available and potentially available to the enterprise.
- Undertake gap analyses to determine shortfalls against requirements to ensure that the business and IT resources (people, application, information, infrastructure) are able to meet strategic objectives.
- Effectively and efficiently ensure clear, consistent and enforceable human resource allocation to investment programs and services.
- Ensure that sourcing strategies are based on the effective use of existing resources and the identification of those that need be acquired.
- Ensure that people, hardware, software and infrastructure procurement policies exist to effectively and efficiently fulfill resource requirements.
- Through periodic assessment of the training requirements for human resources, ensure that sufficient, competent and capable human resources are available to execute the current and future strategic objectives and that they are kept up to date with constantly evolving technology.
- Ensure integration of resource identification, classification, allocation and periodic evaluation processes into the business's strategic and tactical planning and operations.
- Ensure that the IT infrastructure is standardized; economies of scale are achieved, wherever possible; and interoperability exists, where required, to support the agility needs of the enterprise.
- Ensure that IT assets are managed and protected through their economic life cycle and are aligned with current and long-term business operations requirements to support cost-effective achievement of business objectives.

Domain 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.

- Establish the enterprise's strategic IT objectives, with the board of directors and executive leadership team, categorized into four areas financial (business contribution), customer (user orientation), internal process (operational excellence), learning and growth (future orientation), or whatever areas are appropriate for the enterprise.
- Establish outcome and performance measures, supported by metrics, and targets that assess progress toward the achievement of enterprise and IT objectives and the business strategy.
- Evaluate IT process performance, track IT investment portfolio performance, and measure IT service delivery through the use of outcome measures and performance drivers.
- Use maturity models and other assessment techniques to evaluate and report on the health of the enterprise's performance level.
- Use continuous performance measurement to identify, prioritize, initiate and manage improvement initiatives and/or appropriate management action.
- Report relevant portfolio, program and IT performance to relevant stakeholders in an appropriate, timely and accurate manner.

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

2009 exams:

Saturday, 13 June 2009

Saturday, 12 December 2009

- More than 260 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

CISA
CERTIFIED INFORMATION SYSTEMS AUDITOR

CISM
CERTIFIED INFORMATION
SECURITY MANAGER™



2009 Registration Fees: 13 June 2009

Early Registration: *On or before 11 February 2009:*

- ISACA Member: US \$395.00
- Non-Member: US \$525.00

Final Registration: *After 11 February 2009, but on or before 8 April 2009:*

- ISACA Member: US \$445.00
- Non-Member: US \$575.00

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



2009 Registration Fees: 12 December 2009

Early Registration: *On or before 11 February 2009*

- ISACA Member: US \$395.00
- Non-Member: US \$525.00

Final Registration: *After 11 February 2009, but on or before 8 April 2009:*

- ISACA Member: US \$445.00
- Non-Member: US \$575.00

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



Bulletin of Information and Registration Form

- Sent to potential candidates, as well as to CISAs, CISM's and CGEIT's as part of a mentoring program.
- 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 Policy Details

Certification is renewed annually to those who:

- Report a minimum of 120 hours of continuing professional education for each fixed three-year period, with a minimum of 20 hours in each year.
- Report hours annually, in the year they are earned.
- Pay the continuing professional education maintenance fee
- Comply with the 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.



Want to know more?

Please contact us at:

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

- **Phone: +1.847.660.5660**
- **Fax: +1.847.253.1443**
- **E-mail: certification@isaca.org**
- **Web site: www.isaca.org**