



CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT[®]

2012 Candidate's Guide to the
CGEIT[®] Exam and Certification

Candidate's Guide to the CGEIT® Exam and Certification

CGEIT Exams 2012— Important Date Information

Exam Date—9 June 2012

Early registration deadline:	8 February 2012
Final registration deadline:	4 April 2012
Exam registration changes:	Between 14 April and 20 April, charged a US \$50 fee, with no changes accepted after 20 April 2012
Refunds:	By 13 April 2012, charged a US \$100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 20 April 2012, charged a US \$50 processing fee. Requests received from 21 April through 24 May 2012, charged a US \$100 processing fee. After 24 May 2012, no deferrals will be permitted.

Exam Date—8 December 2012

Early registration deadline:	15 August 2012
Final registration deadline:	3 October 2012
Exam registration changes:	Between 6 October and 12 October, charged a US \$50 fee, with no changes accepted after 12 October 2012
Refunds:	By 5 October 2012, charged a US \$100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 12 October 2012, charged a US \$50 processing fee. Requests received from 13 October through 21 November 2012, charged a US \$100 processing fee. After 21 November 2012 no deferrals will be permitted.

All deadlines are based upon Chicago, Illinois, USA 5 p.m. CT (central time)

ISBN 978-1-60420-231-1
2012 Candidate's Guide to the CGEIT® Exam and Certification
Printed in the United States of America

Table of Contents

Introduction	3
The CGEIT Exam.....	3
Content of the CGEIT Exam	3
Preparing for the CGEIT Exam	3
Administration of the CGEIT Exam.....	4
Scoring the CGEIT Exam.....	5
Types of Questions on the CGEIT Exam.....	6
Application for CGEIT Certification	6
Requirements for Initial CGEIT Certification	6
Requirements for Maintaining CGEIT Certification	7
ISACA Code of Professional Ethics	7
Revocation of CGEIT Certification	7
CGEIT Task and Knowledge Statements	8

ISACA®

With 95,000 constituents in 160 countries, ISACA (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA and the CGEIT Certification Committee have designed the *2012 Candidate's Guide to the CGEIT® Exam and Certification* as a guide to those pursuing the CGEIT certification. No representations or warranties are made by ISACA that use of this guide or any other association publication will assure candidates of passing the CGEIT exam.

Reservation of Rights

Copyright © 2011 ISACA. Reproduction or storage in any form for any purpose is not permitted without ISACA's prior written permission. No other right or permission is granted with respect to this work. All rights reserved.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: exam@isaca.org
Web site: www.isaca.org

Candidate's Guide to the CGEIT® Exam and Certification

Introduction

Boards and executive management have long understood the need for enterprise and corporate governance. As information technology (IT) has become more important to the achievement of enterprise goals and delivery of benefits, there has been an increasing realization that governance must be extended to IT as well. IT governance is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.

ISACA recognized this shift in emphasis in 1998, and formed the IT Governance Institute® (ITGI™) to focus on original research, publications, resources and symposia on IT governance and related topics. To support and promote this significant body of work, in 2007, ISACA developed the Certified in the Governance of Enterprise IT (CGEIT) program for professionals charged with satisfying the IT governance needs of an enterprise.

The CGEIT designation meets the needs of:

- **Individuals** by recognizing and elevating the expertise, skill sets, abilities and experiences of those performing IT governance work
- **Enterprises** by identifying those who have made a tangible commitment to excellence in IT governance practices
- **The profession** by supporting the increasing global trends toward IT governance activities
- **Business** by improving the awareness of IT governance good practices and issues

The certification process has been specifically developed for professionals who have a significant management, advisory, or assurance role relating to the governance of IT. The certification promotes the advancement of professionals who wish to be recognized for their IT governance-related experience and knowledge.

CGEIT Program Accredited Under ISO/IEC 17024:2003

The American National Standards Institute (ANSI) has accredited the CGEIT certification under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons. ANSI, a private, nonprofit organization, accredits other organizations to serve as third-party product, system and personnel certifiers. ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individuals against specific requirements. ANSI describes ISO/IEC 17024 as "expected to play a prominent role in facilitating global standardization of the certification community, increasing mobility among countries, enhancing public safety and protecting consumers. ANSI's accreditation:

- Promotes the unique qualifications and expertise that ISACA's certifications provide
- Protects the integrity of the certifications and provides legal defensibility
- Enhances consumer and public confidence in the certifications and the people who hold them
- Facilitates mobility across borders or industries

Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process. With this accreditation, ISACA anticipates that significant opportunities for CGEITs will continue to present themselves around the world.



The CGEIT Exam

Development/Description of the CGEIT Exam

The CGEIT Certification Committee oversees the development of the exam and ensures the currency of its content. The questions for the CGEIT exam are developed through a comprehensive process designed to enhance the ultimate quality of the exam. The process includes a Test Enhancement Subcommittee (TES) that works with item writers to develop and review questions before they are submitted to the CGEIT Certification Committee for review.

A job practice serves as the basis for the exam and the experience requirements to earn the CGEIT certification. This job practice is periodically updated and consists of six content areas (domains). The domains and the accompanying task and knowledge statements were the result of extensive research and feedback from IT governance subject matter experts from around the world.

The task and knowledge statements depict the tasks performed by CGEITs and the knowledge required to perform these tasks. Exam candidates will be tested based on their practical knowledge associated with performing these tasks.

The exam consists of 120 multiple-choice questions and is administered during a four-hour session. Currently, the exam is offered in English only.

Content of the CGEIT Exam

The CGEIT exam measures an individual's ability and knowledge as it pertains to the performance of his/her job. The content of the exam is modified to reflect changes in technology and practices.

The current job practice contains the following practice areas (domains) and percentages:

- **IT Governance Framework (25%)**
- **Strategic Alignment (15%)**
- **Value Delivery (15%)**
- **Risk Management (20%)**
- **Resource Management (13%)**
- **Performance Measurement (12%)**

Note: The percentages listed with the domains indicate the emphasis or percentage of questions that will appear on the exam from each domain. For a description of each domain's task and knowledge statements, please refer to pages 8-11.

Candidate's Guide to the CGEIT® Exam and Certification

Although knowledge of COBIT® is not specifically tested on the CGEIT exam, the COBIT control objectives or processes are reflected in the CGEIT job practice task statements. As such, a thorough review of COBIT is recommended for candidate preparation for the CGEIT exam. To focus a candidate's attention on the specific COBIT processes that relate to CGEIT practice analysis tasks, go to www.isaca.org/cgeitguide. In 2012, ISACA will release COBIT 5. COBIT 5 is a comprehensive framework of globally accepted practices, analytical tools and models that can help any enterprise effectively address critical issues through governance and management of information and technology. Please see www.isaca.org/cobit5 for more information.

Preparing for the CGEIT Exam

Passing the CGEIT exam can be achieved through an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers a list of IT governance resources at www.isaca.org/cgeitreferences. Most of these resources can be downloaded from the ISACA web site and/or purchased directly from the ISACA bookstore at www.isaca.org/bookstore. In addition ISACA also offers the *CGEIT® Review Manual 2012* and *CGEIT Review Questions, Answers & Explanations Manual 2011 and 2012 Supplement*—visit www.isaca.org/cgeitbooks for complete information. Order early as delivery time can be from one to four weeks depending on geographic location and customs clearance practices. For current shipping information see www.isaca.org/shipping. ISACA maintains a glossary of terms as well as glossaries specific to each certification. These glossaries are available at www.isaca.org/glossary.

No representation or warranties assuring candidates' passage of the exam are made by ISACA or the CGEIT Certification Committee in regard to these or other association publications or courses.

Administration of the CGEIT Exam

ISACA utilizes an internationally recognized professional testing agency to assist in the construction, administration and scoring of the CGEIT exam.

Candidates wishing to comment on the test administration conditions may do so at the conclusion of the testing session by completing the "Test Administration Questionnaire." The Test Administration Questionnaire is presented at the back of the examination booklet and your questionnaire answers should be entered in boxes P through S of the Special Codes section (Grid No. 4) on the front of your Answer Sheet.

Candidates who wish to address any additional comments or concerns about the examination administration, including site conditions or the content of the exam, should contact ISACA international headquarters by letter or by e-mail (exam@isaca.org). These comments or concerns are to be received by ISACA within two weeks after the examination date. Please include the following information in your comments: exam ID number, testing site, date tested and any relevant details on the specific issue. Only those comments received by ISACA during the first two weeks after the exam administration will be considered in the final scoring process of the exam.

Admission Ticket

Approximately two to three weeks prior to the CGEIT exam date, candidates will be sent a physical admission ticket and an e-ticket from ISACA. Exam candidates can also download a copy of the admission ticket at www.isaca.org > MyISACA page of the web site. Tickets will indicate the date, registration time and location of the exam, as well as a schedule of events for that day and a list of materials that candidates must bring with them to take the CGEIT exam. With the exception of contact information changes, candidates are not to write on the admission ticket.

Please Note: In order to receive an admission ticket, all fees must be paid. Admission tickets are sent via hard copy and e-mail to the current postal mailing and e-mail address on file. Only candidates with an admission ticket and an acceptable government-issued ID will be admitted to take the exam, and the name on the admission ticket must match the name on the government-issued ID. The hard copy admission ticket or print out of the e-ticket is valid for admission into the exam. If candidates' mailing and/or e-mail addresses change, they should update their profile on the ISACA web site (www.isaca.org) or contact exam@isaca.org.

It is imperative that candidates note the specific registration and exam time on their admission ticket. NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS READING THE ORAL INSTRUCTIONS, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS. Any candidate who arrives after the oral instructions have begun will not be allowed to sit for the exam and will forfeit his/her registration fee. An admission ticket can only be used at the designated test center specified on the admission ticket. IDs will be checked during the exam administration.

Special Arrangements

Upon request, ISACA will make reasonable accommodations in its exam procedures for candidates with documented disabilities or religious requirements. These candidates may request consideration for reasonable alterations in exam format, presentations, food or drink at the exam site, or scheduling. Requests for food or drink at the exam site must be accompanied by a doctor's note; otherwise, **no food or drinks are allowed at any exam site.** Requests for consideration must be submitted to ISACA International Headquarters in writing, accompanied by appropriate documentation, no later than 4 April 2012 for the June 2012 exam and 3 October 2012 for the December 2012 exam.

Be Prompt

Registration will begin at the time indicated on the admission ticket at each center. All candidates must be registered and in the test center room when the chief examiner begins reading the oral instructions. **NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS READING THE ORAL INSTRUCTIONS, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS.**

Remember to Bring the Admission Ticket

Candidates can use their admission ticket (either their e-ticket or physical admission ticket) only at the designated test center. Candidates will be admitted to the test center only if they have a valid admission ticket and an acceptable form of identification (ID). An acceptable form of ID must be a current and original government-issued ID that contains the candidate's name, as it appears on the admission ticket, and the candidate's photograph. The information on the ID cannot be handwritten. All of these characteristics must be demonstrated by the single piece of ID provided. Examples include, but are not limited

Candidate's Guide to the CGEIT® Exam and Certification

to, a passport, driver's license, military ID, state ID, green card and national ID. Any candidate who does not provide an acceptable form of ID will not be allowed to sit for the exam and will forfeit his/her registration fee.

Observe the Test Center's Rules

- Candidates will not be admitted to a test center after the oral instructions have begun.
- Candidates should bring several sharpened No. 2 or HB (soft lead) pencils and a good eraser. Pencils and erasers will not be available at the test center.
- Candidates are not allowed to bring reference materials, blank paper, note pads or language dictionaries into the test center. As exam venues vary, every attempt will be made to make the climate control comfortable at each exam venue. Candidates may want to dress to their own comfort level.
- Candidates are not allowed to bring or use a calculator in the test center.
- Candidates are not allowed to bring any type of communication devices (i.e., cell phones, PDAs, Blackberries) into the test center. **If exam candidates are viewed with any such device during the exam administration, their exams will be voided and they will be asked to immediately leave the exam site.**
- Visitors are not permitted in the test center.
- No food or beverages are allowed in the test center (without advance authorization from ISACA).

Misconduct

Candidates who are discovered engaging in any kind of misconduct—such as giving or receiving help; using notes, papers or other aids; attempting to take the exam for someone else; using any type of communication device, including cell phones, during the exam administration; or removing the exam booklet, answer sheet or notes from the testing room—will be disqualified and may face legal action. Candidates who leave the testing area without authorization or accompaniment by a test proctor will not be allowed to return to the testing room and will be subject to disqualification. The testing agency will report such irregularities to ISACA's CGEIT Certification Committee.

The complete Personal Belongings Policy is available at www.isaca.org/CGEITbelongings. Neither ISACA nor its testing vendor takes responsibility for the personal belongings of candidates.

Be Careful in Completing the Answer Sheet

- **The multiple-choice answer sheet provided has 200 response areas, but the CGEIT exam is 120 questions long. Please note that candidates are asked to leave blank the last 80 response areas.** Candidates will be reminded of this at the time of the exam.
- Before a candidate begins the exam, the test center chief examiner will read aloud the instructions for entering identification information on the answer sheet. A candidate's identification number as it appears on the admission ticket and all other requested information must be correctly entered or scores may be delayed or incorrectly reported.
- A candidate is instructed to read all instructions carefully and understand them before attempting to answer the questions. Candidates who skip over the directions or read them too quickly could miss important information and possibly lose credit.
- All answers are to be marked in the appropriate circle on the answer sheet. Candidates must be careful not to mark more than one answer per question and to be sure to answer a question in the appropriate row of answers. If an answer needs to be changed, a candidate is urged to erase the wrong answer fully before marking in the new one.
- All questions should be answered. **There are no penalties for incorrect answers. Grades are based solely on the number of questions answered correctly, so do not leave any questions blank.**
- After completion, candidates are required to hand in their answer sheet and test booklet.

Budget One's Time

- The exam is four hours in length. Candidates are advised to pace themselves to complete the entire exam.
- Candidates are urged to immediately record their answers on the answer sheet. **No additional time will be allowed after the exam time has elapsed to transfer or record answers should a candidate mark answers in the test booklet.**

Conduct Oneself Properly

- To protect the security of the exam and maintain the validity of the scores, candidates are asked to sign the answer sheet.
- The CGEIT Certification Committee reserves the right to disqualify any candidate who is discovered engaging in any kind of misconduct or violation of exam rules, such as giving or receiving help; using notes, papers or other aids; attempting to take the exam for someone else; or removing test materials or notes from the test center. The testing agency will provide the CGEIT Certification Committee with records regarding such irregularities for their review and to render a decision.

Reasons for Dismissal or Disqualification

- Unauthorized admission to the test center.
- Candidate creates a disturbance or gives or receives help.
- Candidate attempts to remove test materials or notes from the test center.
- Candidate impersonates another candidate.
- Candidate brings items into the test center that are not permitted.
- Candidate possession of any communication device (i.e., cell phone, PDA, BlackBerry®) during the exam administration
- Candidate unauthorized leave of the test area

If candidates are observed with any communication device (i.e., cell phone, PDA, BlackBerry) during the exam administration, their exams will be voided and they will be asked to immediately leave the test site.

Candidate's Guide to the CGEIT® Exam and Certification

Scoring the CGEIT Exam

The CGEIT exam consists of 120 multiple-choice items. Candidate scores are reported as a scaled score. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. ISACA uses and reports scores on a common scale from 200 to 800. A candidate must receive a score of 450 or higher to pass the exam. For example, the scaled score of 800 represents a perfect score with all questions answered correctly; a scaled score of 200 is the lowest score possible and signifies that only a small number of questions were answered correctly. A score of 450 represents a minimum consistent standard of knowledge as established by the CGEIT Certification Committee. A candidate receiving a passing score may then apply for certification if all other requirements are met.

Approximately eight weeks after the test date, the official exam results will be mailed to candidates. Additionally, with the candidate's consent during the registration process, an e-mail message containing the candidate's pass/fail status and score will be sent to the candidate. This e-mail notification will only be sent to the address listed in the candidate's profile at the time of the initial release of the results. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax. To prevent e-mail notification from being sent to spam folders, candidates should add exam@isaca.org to their address book, whitelist or safe-senders list.

Candidates will receive a score report containing a subscore for each domain area. Successful candidates will receive, along with a score report, details on how to apply for CGEIT certification.

The subscores can be useful in identifying those areas in which the unsuccessful candidate may need further study before retaking the exam. Unsuccessful candidates should note that the total scaled score cannot be determined by calculating either a simple or weighted average of the subscores.

Candidates receiving a failing score on the exam may request a hand score of their answer sheets. This procedure ensures that no stray marks, multiple responses or other conditions interfered with computer scoring. Candidates should understand, however, that all scores are subjected to several quality control checks before they are reported; therefore, rescoring most likely will not result in a score change. Requests for hand scoring must be made in writing to the certification department within 90 days following the release of the exam results. Requests for a hand score after the deadline date will not be processed. All requests must include a candidate's name, exam identification number and mailing address. A fee of US \$75 must accompany each request.

Types of Questions on the CGEIT Exam

CGEIT exam questions are developed with the intent of measuring and testing practical knowledge. All questions are designed with one best answer. Every CGEIT question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. The candidate is cautioned to read each question carefully. A CGEIT exam question may require the candidate to choose the appropriate answer based on a qualifier, such as **MOST** likely or **BEST**. In every case, the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible.

The following questions are representative examples of the CGEIT question format. The option in bold is the correct answer.

1. Which of the following is the **PRIMARY** driver for a commercial enterprise's board of directors when making IT-related investments?
 - A. Alignment with technology plan
 - B. Catch up with leading peers in the industry
 - C. Business opportunity**
 - D. Improve IT service management levels
2. Which of the following is accountable for the IT governance framework?
 - A. IT program manager
 - B. Board of directors**
 - C. IT steering committee
 - D. IT architecture board

Application for CGEIT Certification

Passing the exam does not mean a candidate is a CGEIT. Once a candidate passes the CGEIT exam, he/she has five years from the date of the exam to apply for certification. Successful candidates must complete the application for certification and have their work experience verified using the appropriate forms included in the application. A processing fee of US \$50 must accompany your CGEIT Application for Certification. **Candidates are not certified, and cannot use the CGEIT designation, until the completed application (and fee) is received and approved.** Please note that decisions on applications are not final as there is an appeal process for certification application denials. Inquiries regarding denials of certification can be sent to certification@isaca.org. Once certified, the new CGEIT will receive a certificate and a CGEIT certification pin. At the time of application, individuals must also acknowledge that ISACA reserves the right, but is not obligated, to publish or otherwise disclose their CGEIT status.

Requirements for Initial CGEIT Certification

Certification is granted initially to individuals who have successfully completed the CGEIT exam and met the following work experience requirements.

Five or more years of experience managing, serving in an advisory or oversight role, and/or otherwise supporting the governance of the IT-related contribution to an enterprise. This experience is defined specifically by the domains and task statements described in the CGEIT Job Practice.

Specifically:

- A minimum of one year of experience relating to the development and/or maintenance of an IT governance framework is required. The type and extent of experience accepted is described in CGEIT domain one (1), IT Governance Framework.

Candidate's Guide to the CGEIT® Exam and Certification

- Additional broad experience directly related to any two or more of the remaining CGEIT domains is required. The type and extent of experience accepted is described in CGEIT domains two (2) through six (6). These domains are:
 - Strategic Alignment
 - Value Delivery
 - Risk Management
 - Resource Management
 - Performance Measurement

To recognize other management experience and/or the achievement of specific IT governance-related credentials, advanced (postgraduate) degrees and certificates, up to two years of the five years of required IT governance experience can be substituted. Specifically, each of the following will qualify (substitute) for one year of IT governance experience, with a maximum of two years of substitutions being accepted.

- Other Management Experience—Other management experience that is not specific to IT governance, such as performing consulting, auditing, assurance or security management-related duties will qualify for up to one year of substitution.
- Specific Credentials, Advanced (Postgraduate) Degrees and Certificates—Credentials (in good standing), advanced (postgraduate) degrees and certificate programs which include an IT governance and/or management component or are specific to one or more of the CGEIT domains will qualify for up to one year of substitution.

These include:

- Certified Information Systems Auditor (CISA) issued by ISACA
- Certified Information Security Manager (CISM) issued by ISACA
- ITIL Service Manager certification program
- Chartered Information Technology Professional (CITP) issued by the British Computer Society
- Chartered Information Technology Professional (CITP) issued by the American Institute of CPAs
- Implementing IT Governance Using COBIT certificate issued by ISACA
- Information Systems Professional (I.S.P.) issued by the Canadian Information Processing Society
- Project Management Professional (PMP) issued by the Project Management Institute
- Certified Internal Auditor (CIA) issued by the Institute of Internal Auditors
- Certified Business Manager (CBM) issued by The Association of Professionals in Business Management.
- Prince2—Registered Practitioner certificate from the Office of Government Commerce
- Advanced (postgraduate) degree from an accredited university in governance, information technology, information management or business administration (for example: Master in Corporate Governance, Master of Business Administration, Master in Information and Operations Management, Master of Information Systems Management, Master in Information Technology)

Exception: Two years as a full-time university instructor teaching IT governance related subjects at an accredited university can be substituted for every one year of experience required.

Applicants who have earned/acquired other credentials, advanced degrees and/or certificates that include a significant IT governance and/or information management component and are not listed above are welcome to submit them to the CGEIT Certification Board for consideration.

It is important to note that individuals may choose to take the CGEIT exam prior to meeting the experience requirements. This practice is acceptable and encouraged, although the CGEIT designation will not be awarded until all requirements are met.

Requirements for Maintaining CGEIT Certification

CGEITs must comply with the following requirements to retain certification:

- Attain and report an annual minimum of 20 CPE hours, and attain and report a minimum of 120 CPE hours for a three-year reporting period. For more details visit the CGEIT CPE policy at www.isaca.org/cgeitcpepolicy.
- Submit annual CPE maintenance fees in full to ISACA International Headquarters.
- Respond and submit required documentation of CPE activities to support the hours reported if selected for an annual audit.
- Comply with the ISACA Code of Professional Ethics.

Failure to comply with these general requirements will result in the revocation of an individual's CGEIT designation. All certificates are owned by ISACA. If an individual is approved for certification and subsequently revoked, the individual must destroy the certificate.

ISACA Code of Professional Ethics

ISACA sets forth a Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders. Failure to comply with this Code of Professional Ethics can result in an investigation into a member's and/or certification holder's conduct and, ultimately, in disciplinary measures. The ISACA Code of Professional Ethics can be viewed online at www.isaca.org/ethics.

Revocation of CGEIT Certification

The CGEIT Certification Committee may, at its discretion after due and thorough consideration, revoke an individual's CGEIT certification for any of the following reasons:

- Failing to comply with the CGEIT CPE policy
- Violating any provision of the ISACA Code of Professional Ethics
- Falsifying or deliberately failing to provide relevant information
- Intentionally misstating a material fact
- Engaging or assisting others in dishonest, unauthorized or inappropriate behavior at any time in connection with the CGEIT exam or the certification process

Candidate's Guide to the CGEIT® Exam and Certification

Description of CGEIT Job Practice Areas CGEIT Task and Knowledge Statements

CONTENT AREA (Domain)	
1. IT Governance Framework	—Define, establish and maintain an IT governance framework (leadership, organizational structures and processes) to: ensure alignment with enterprise governance; control the business information and information technology environment through the implementation of good practices; and assure compliance with external requirements.
Task Statements—Develop, or be part of the development of, an IT governance framework that includes the following responsibilities and tasks:	
1.1	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.
1.2	Ensure that an IT governance framework exists and is based on a comprehensive and repeatable IT process and control model that is aligned with the enterprise governance framework.
1.3	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.
1.4	Ensure that the enterprise and IT governance frameworks enable the enterprise to achieve optimal value for the enterprise.
1.5	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.
1.6	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.
1.7	Apply IT best practices to enable the business to achieve optimal value from implementation of IT services and IT-enabled business solutions.
1.8	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.
1.9	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.
1.10	Report IT governance status and issues, and effect transparency in reporting.
1.11	Establish a communications plan to continuously market, communicate and reinforce the need and value of IT governance across the enterprise.
Knowledge Statements	
1.1	Knowledge of how to effect organizational, process and cultural change by translating objectives into actions
1.2	Knowledge of the components of an enterprise governance framework
1.3	Knowledge of how to direct, manage and report on IT governance activities at the enterprise level and collaborating with enterprise governance as appropriate
1.4	Knowledge of business drivers for the use of IT industry practices, standards and frameworks.
1.5	Knowledge of how accountability is established for information requirements, data and system ownership, and IT processes
1.6	Knowledge of COBIT, Val IT and related products.
1.7	Knowledge of the scope, objective and benefits of IT practices, standards and frameworks, such as ITIL, CMMI, PRINCE2, PMBOK, TOGAF, ISO 17799/27000 series, and the IT Balanced Scorecard
1.8	Knowledge of scope, objective and benefits of continuous process improvement, such as Six Sigma, Total Quality Management and the Balanced Scorecard
1.9	Knowledge of IT governance implementation practices
1.10	Knowledge of how IT practices, standards and frameworks relate to, and complement, each other
1.11	Knowledge of the process of selection, customization and integration of IT practices, standards and frameworks, as relevant for the enterprise
1.12	Knowledge of how to align the application of IT practices, standards and frameworks to the needs and culture of the enterprise
1.13	Knowledge of assurance methodologies and techniques
1.14	Knowledge of marketing and communications methods and techniques
1.15	Knowledge of how to utilize mission, vision, guiding principles, critical success factors, etc., in setting the direction for IT governance across the enterprise
1.16	Knowledge of the impact of cultural changes and the need to choose the correct time and way to achieve the desirable results, considering different but possible scenarios
2. Strategic Alignment	—Ensure that IT enables and supports the achievement of business objectives through the integration of IT strategic plans with business strategic plans and the alignment of IT services with enterprise operations to optimize business processes.
Task Statements—Develop, or be part of the development of, an enterprise's IT strategy that includes the following responsibilities and tasks:	
2.1	Define and implement a strategic planning framework, requiring and facilitating collaborative and integrated business and IT management planning.
2.2	Actively support/promote and participate in IT management planning by employing best practice enterprise architecture (EA) frameworks.
2.3	Ensure that appropriate policies and procedures are in place, understood and followed to support IT and business strategic alignment.
2.4	Identify and take action on barriers to strategic alignment.
2.5	Ensure that effective communication and engagement exists between business and IT management regarding shared strategic initiatives and performance.
2.6	Ensure business and IT goals cascade down through the enterprise into clear roles, responsibilities and actions.

Candidate's Guide to the CGEIT® Exam and Certification

CONTENT AREA (Domain)	
2. Strategic Alignment (continued)	
2.7	Assist senior management by aligning IT initiatives with business objectives and facilitating prioritization of business strategies that optimally achieve business objectives.
2.8	Identify and monitor the interdependencies of strategic initiatives and their impact on value delivery and risk.
2.9	Ensure that the strategic planning process is adequately documented, transparent and meets stakeholder needs.
2.10	Maintain and update the IT management plans, artifacts and standards for the enterprise.
2.11	Monitor, evaluate and report on the effectiveness of the alignment of IT and enterprise strategic initiatives.
2.12	Monitor and assess current and future technologies and provide advice on the costs, risks and opportunities that they bring.
Knowledge Statements	
2.1	Knowledge of the enterprise's mission, objectives, culture, economic and business environment, key business processes, and how they are supported by IT
2.2	Knowledge of how an enterprise's structure, operational frameworks, systems, resources, internal and external stakeholder relationships, and culture can impact the enterprise's ability to achieve sufficient strategic alignment
2.3	Knowledge of the strategic planning process and techniques
2.4	Knowledge of enterprise architecture components, principles and frameworks, and their implementation
2.5	Knowledge of how to map strategy to specific, enabling business processes and IT dashboard/balanced scorecard principles to monitor key goal and performance metrics
2.6	Knowledge of benchmarking planned vs. actual strategic performance
2.7	Knowledge of scope, objectives and benefits of investment programs
2.8	Knowledge of portfolio, program and project management techniques
2.9	Knowledge of linking enterprise business strategy with related best practices and selling the value proposition to key stakeholders
2.10	Knowledge of how procedures, monitoring and updating of the IT strategy are impacted and implemented by changes in business strategy
2.11	Knowledge of current and future technology direction to support the business by creation of technological infrastructure plan and architecture board that sets and manages what technology can deliver to achieve business objectives
3. Value Delivery —Ensure that IT and the business fulfill their value management responsibilities: IT-enabled business investments achieve the benefits as promised and deliver measurable business value both individually and collectively, that required capabilities (solutions and services) are delivered on-time and within budget, and that IT services and other IT assets continue to contribute to business value	
Task Statements — <i>Develop, or be part of the development of, a systematic, analytical and continuous value governance process that includes the following responsibilities and tasks:</i>	
3.1	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.
3.2	Ensure that all IT-enabled investments are managed as a portfolio of investments.
3.3	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.
3.4	Ensure that all IT-enabled investments are managed through their full economic life cycle so that value is optimized.
3.5	Recognize that different categories of investments need to be evaluated and managed differently.
3.6	Ensure that all IT solutions are developed and maintained effectively and efficiently through the development life cycle to deliver the required capabilities.
3.7	Ensure that all IT services are delivered to the business with the right service levels.
3.8	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.
3.9	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.
3.10	Engage all stakeholders and assign appropriate accountability for delivery of business and IT capabilities and realization of benefits.
3.11	Ensure that IT investments, solutions and services are aligned with the enterprise strategies and architecture.
Knowledge Statements	
3.1	Knowledge of value governance practices
3.2	Knowledge of IT investment management practices and processes
3.3	Knowledge of business case development and monitoring, portfolio program and project management practices
3.4	Knowledge of managing and reporting the status of IT investments
3.5	Knowledge of IT investment processes, funding models and investment life cycle management, including benefits management
3.6	Knowledge of cost optimization
3.7	Knowledge of solution delivery processes and practices (systems development life cycle)
3.8	Knowledge of service delivery practices and processes
3.9	Knowledge of enterprise, information and IT architecture techniques and frameworks

Candidate's Guide to the CGEIT® Exam and Certification

CONTENT AREA (Domain)
4. Risk Management —Ensure that appropriate frameworks exist and are aligned with relevant standards to identify, assess, mitigate, manage, communicate and monitor IT-related business risks as an integral part of an enterprise's governance environment.
Task Statements — <i>Develop, enhance and maintain a systematic, analytical and continuous enterprise risk management process across the enterprise that includes the following responsibilities and tasks:</i>
4.1 Ensure that IT risk identification, assessment, mitigation, management, communication and monitoring strategies are integrated into business strategic and tactical planning processes.
4.2 Align the IT risk management processes with the enterprise business risk management framework (where this exists).
4.3 Ensure a consistent application of the risk management framework across the enterprise IT environment.
4.4 Ensure that risk assessment and management is included throughout the information life cycle.
4.5 Define risk management strategies and prioritize responses to identified risks to maintain risk levels within the appetite of the enterprise.
4.6 Ensure that risk management strategies are adopted to mitigate risk and to manage to acceptable residual risk levels.
4.7 Implement timely reporting on risk events and responses to appropriate levels of management (including the use of key risk indicators, as appropriate).
4.8 Establish monitoring processes and practices to ensure the completeness and effectiveness of established risk management processes.
Knowledge Statements
4.1 Knowledge of the context of risk management at the strategic, portfolio, program, project and operations level
4.2 Knowledge of risk management frameworks and standards (e.g., COSO ERM, MoR, OCTAVE, ISO31000, AS/NZ 4360:2004)
4.3 Knowledge of the enterprise's business objectives
4.4 Knowledge of the enterprise's risk management framework (including the risk classification model used to support risk identification and assessment)
4.5 Knowledge of the enterprise's external business environment
4.6 Knowledge of the enterprise's internal environment
4.7 Knowledge of how the enterprise defines and executes business strategies to achieve its goals and objectives
4.8 Knowledge of how to map business process down to IT process to understand dependencies and root cause
4.9 Knowledge of the enterprise's risk appetite
4.10 Knowledge of the enterprise's IT resources (applications, information, infrastructure and people)
4.11 Knowledge of the threats, vulnerabilities and opportunities inherent in the enterprise's use of IT
4.12 Knowledge of the types of business risks, exposures and threats that can be addressed using IT resources
4.13 Knowledge of quantitative and qualitative methods to determine sensitivity, criticality and maturity of IT-related contributions to business success
4.14 Knowledge of quantitative and qualitative methods (including enterprise-specific descriptive measurement scales, IT-related asset valuation methods and probability, use of both audit and stream data types, and impact and loss expectancy models/techniques) to assess IT risks
4.15 Knowledge of methods to discover more rare, but high-impact risk types, such as process analysis techniques
4.16 Knowledge of risk mitigation strategies in relation to the use of IT in the enterprise
4.17 Knowledge of risk management techniques that can be applied to affect enterprise risk management, particularly as they relate to IT-related activities
4.18 Knowledge of methods to effectively manage and report the status of identified risks
5. Resource Management —Ensure that IT has sufficient, competent and capable resources to execute current and future strategic objectives and keep up with business demands by optimizing the investment, use and allocation of IT assets.
Task Statements — <i>Develop, or assist in the development of systematic and continuous resource planning, management and evaluation processes that include the following responsibilities and tasks:</i>
5.1 Ensure that the requirements for trained resources with the requisite skill sets are understood and are assessed appropriately.
5.2 Ensure the existence of appropriate policies for the training and development of all staff to help meet enterprise requirements and personal/professional growth.
5.3 Develop and facilitate the maintenance of systems to record the resources available and potentially available to the enterprise.
5.4 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.
5.5 Effectively and efficiently ensure clear, consistent and enforceable human resource allocation to investment programs and services.
5.6 Ensure that sourcing strategies are based on the effective use of existing resources and the identification of those that need to be acquired.
5.7 Ensure that people, hardware, software and infrastructure procurement policies exist to effectively and efficiently fulfill resource requirements.
5.8 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.
5.9 Ensure integration of resource identification, classification, allocation and periodic evaluation processes into the business's strategic and tactical planning and operations.
5.10 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.
5.11 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.

Candidate's Guide to the CGEIT® Exam and Certification

CONTENT AREA (Domain)
5. Resource Management (continued)
Knowledge Statements
5.1 Knowledge of corporate business and IT resources (people, applications, infrastructure and information)
5.2 Knowledge of an enterprise's business and IT resources and acquisition processes (people, application, software, hardware, facilities and outsourced services)
5.3 Knowledge of the skill and technology mixes required to meet the enterprise's business objectives
5.4 Knowledge of human resource management processes and optimization practices needed to meet established technical and business proficiency, competency, and capability requirements
5.5 Knowledge of outsourcing and offshoring processes that may be employed to meet investment program and operation and service level agreements
5.6 Knowledge of the strengths and weaknesses inherent within the enterprise's human and technical business and IT resources and how to identify trainers with the requisite skill sets to maintain work competency and proficiency
5.7 Knowledge of enterprise business strategies
5.8 Knowledge of business and IT resource planning and strategic and tactical planning methods, techniques and processes
5.9 Knowledge of quantitative and qualitative methods used to determine and evaluate business and IT resource utilization and the availability of these resources to effectively meet enterprise objectives
5.10 Knowledge of methods for monitoring and reporting on business and IT resource performance
6. Performance Measurement —Ensure that business-supporting IT goals/objectives and measures are established in collaboration with key stakeholders and that measurable targets are set, monitored and evaluated.
Task Statements — <i>Develop, or assist in the development of, systematic and continuous performance management and evaluation processes that include the following responsibilities and tasks:</i>
6.1 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.
6.2 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.
6.3 Evaluate IT process performance, track IT investment portfolio performance, and measure IT service delivery through the use of outcome measures and performance drivers.
6.4 Use maturity models and other assessment techniques to evaluate and report on the health of the enterprise's performance level.
6.5 Use continuous performance measurement to identify, prioritize, initiate and manage improvement initiatives and/or appropriate management action.
6.6 Report relevant portfolio, program and IT performance to relevant stakeholders in an appropriate, timely and accurate manner.
Knowledge Statements
6.1 Knowledge of the enterprise's business objectives
6.2 Knowledge of strategy mapping and balanced scorecard principles
6.3 Knowledge of the scope, objectives and benefits of commonly used IT maturity models, including their maturity attributes
6.4 Knowledge of data collection techniques for performance measurement
6.5 Knowledge of continuous improvement methodologies
6.6 Knowledge of IT governance implementation practices
6.7 Knowledge of characteristics of, and selection criteria for, measures and metrics
6.8 Knowledge of outcome measures and performance drivers
6.9 Knowledge of accepted practices in performance measurement (e.g., maturity models) and effective industry benchmarking techniques
6.10 Knowledge of tools and techniques that facilitate measurements, good communications and organizational change
6.11 Knowledge of automated monitoring tools and techniques
6.12 Knowledge of root cause analysis techniques
6.13 Knowledge of life cycle cost-benefit analysis techniques
6.14 Knowledge of evaluating and monitoring IT performance and value governance



Prepare for the **2012 CGEIT Exams**

2012 CGEIT Review Resources for Exam Preparation and Professional Development

Successful Certified in the Governance of Enterprise IT® (CGEIT®) exam candidates have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses to exam candidates. These include:

Study Aids

- *CGEIT® Review Manual 2012*
- *CGEIT® Review Questions, Answers & Explanations Manual 2011*
- *CGEIT® Review Questions, Answers & Explanations Manual Supplement 2012*

Review Courses

- Chapter-sponsored review courses (www.isaca.org/cgeitreview)

To order, visit www.isaca.org/cgeitbooks.

