Certified in the Governance of Enterprise IT (CGEIT)

Overview

The CGEIT qualification is an internationally recognised symbol of excellence in IT governance awarded by ISACA. It is designed for professionals responsible for managing IT governance or with significant advisory or assurance responsibility for IT governance. Achieving CGEIT status will provide you with wider recognition in the marketplace, as well as increased influence at executive level.

Course Objectives

This course has been designed to prepare Delegates for the CGEIT examination by enabling them to supplement their existing knowledge and understanding to be better prepared.

Duration

4 Days

Prerequisites

Our training course is for IT and business professionals, with significant IT governance experience who are undertaking the CGEIT exam.

Certified in the Governance of Enterprise IT (CGEIT)

Domain 1: Framework for the Governance of Enterprise IT (25%)

Ensure the definition, establishment, and management of a framework for the Governance of enterprise it in alignment with the mission, vision and values of the Enterprise.

Course Topics

	Knowledge Statements
Module 1	• Knowledge of components of a framework for the governance of enterprise IT • Knowledge of IT governance industry practices, standards and frameworks (for example, COBIT, Information Technology Infrastructure Library [ITIL], International Organization for Standardization [ISO] 20000, ISO 38500) • Knowledge of business drivers related to IT governance (for example, legal, regulatory and contractual requirements) • Knowledge of IT governance enablers (for example, principles, policies and frameworks; processes; organizational structures; culture, ethics and behaviour; information; services, infrastructure and applications; people, skills and competencies) • Knowledge of techniques used to identify IT strategy (for example, SWOT, BCG Matrix) • Knowledge of components, principles, and concepts related to enterprise architecture (EA) • Knowledge of Organizational structures and their roles and responsibilities (for example, enterprise investment committee, program management office, IT strategy committee, IT architecture review board, IT risk management committee) • Knowledge of methods to manage organizational, process and cultural change • Knowledge of models and methods to establish accountability for information requirements, data and system ownership; and IT processes • Knowledge of IT governance monitoring processes/mechanisms (for example, balanced scorecard (BSC) • Knowledge of IT governance reporting processes/mechanisms • Knowledge of communication and promotion techniques • Knowledge of assurance methodologies and techniques • Knowledge of continuous improvement techniques and processes

Certified in the Governance of Enterprise IT (CGEIT)

Domain 2: Strategic Management (20%)

Ensure that it enables and supports the achievement of enterprise objectives hrough the integration and alignment of it strategic plans with enterprise strategic plans.

Course Topics

	Knowledge Statements
Module 2	• Knowledge of an enterprise's strategic plan and how it relates to IT • Knowledge of strategic planning processes and techniques • Knowledge of impact of changes in business strategy on IT strategy • Knowledge of barriers to the achievement of strategic alignment • Knowledge of policies and procedures necessary to support IT and business strategic alignment • Knowledge of methods to document and communicate IT strategic planning processes (for example, IT dashboard/balanced scorecard, key indicators) • Knowledge of components, principles and frameworks of enterprise architecture (EA) • Knowledge of current and future technologies • Knowledge of prioritization processes related to IT initiatives • Knowledge of scope, objectives and benefits of IT investment programs • Knowledge of IT roles and responsibilities and methods to cascade business and IT objectives to IT personnel

Certified in the Governance of Enterprise IT (CGEIT)

Domain 3: Benefits Realization (16%)

Ensure that it-enabled investments are managed to deliver optimized business benefits and that benefit realization outcome and performance measures are established, evaluated and progress is reported to key stakeholders

Course Topics

	Knowledge Statements
Module 3	• Knowledge of IT investment management processes, including the economic life cycle of investments • Knowledge of basic principles of portfolio management • Knowledge of benefit calculation techniques (for example, earned value, total cost of ownership, return on investment) • Knowledge of process and service measurement techniques (for example, maturity models, benchmarking, key performance indicators [KPIs]) • Knowledge of processes and practices for planning, development, transition, delivery, and support of IT solutions and services • Knowledge of continuous improvement concepts and principles • Knowledge of outcome and performance measurement techniques (for example, service metrics, key performance indicators [KPIs]) • Knowledge of procedures to manage and report the status of IT investments

Certified in the Governance of Enterprise IT (CGEIT)

Domain 4: Risk Optimization (24%)

Ensure that an it risk management framework exists to identify, analyze, mitigate, manage, monitor, and communicate it-related business risk, and that the framework for it risk management is in alignment with the Enterprise Risk Management (ERM) framework.

Course Topics

	Knowledge Statements
Module 4	• Knowledge of the application of risk management at the strategic, portfolio, program, project and operations levels • Knowledge of risk management frameworks and standards (for example, RISK IT, the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management—Integrated Framework (2004) [COSO ERM], International Organization for Standardization (ISO) 31000) • Knowledge of the relationship of the risk management approach to legal and regulatory compliance • Knowledge of methods to align IT and enterprise risk management (ERM) • Knowledge of the relationship of the risk management approach to business resiliency (for example, business continuity planning [BCP] and disaster recovery planning [DRP]) • Knowledge of risk, threats, vulnerabilities and opportunities inherent in the use of IT • Knowledge of types of business risk, exposures and threats (for example, external environment, internal fraud, information security) that can be addressed using IT resources • Knowledge of risk appetite and risk tolerance • Knowledge of quantitative and qualitative risk assessment methods • Knowledge of risk mitigation strategies related to IT in the enterprise • Knowledge of methods to monitor effectiveness of mitigation strategies and/or controls • Knowledge of stakeholder analysis and communication techniques • Knowledge of methods to establish key risk indicators (KRIs) • Knowledge of methods to manage and report the status of identified risk