

Providing Trust and Value Through ISACA's Credentials: CISA, CISM, CGEIT and CRISC

ISACA certification holders, through their expertise and the work they perform, strengthen the trust in information systems to achieve their desired results and provide value to an organization

CGEITs define, establish, maintain and manage a framework of governance as it relates to information systems to ensure:

- business value is achieved from the implementation of information systems
- risk management is integrated into business and planning
- appropriate management structures, roles, responsibilities and accountabilities are established and strategically aligned
- information system processes and controls are comprehensive and repeatable and optimized
- that investments in information systems and resources are appropriate, measurable and managed



CISMs develop, implement and manage information security activities to ensure:

- information security risks are identified and managed
- information security requirements are integrated into, and maintained throughout the organization's information systems processes
- information security controls are monitored and tested for efficiency and effectiveness
- information security roles and responsibilities are defined throughout the organization
- information security incidents are managed efficiently and effectively

Information systems are integral enablers which:

- Help to achieve an organization's strategy and business objectives
- enable the confidentiality, integrity, availability and reliability of information assets
- ensure compliance with applicable laws and regulations

thereby creating unprecedented potential for value creation and risk management to the organization.



CISAs provide assurance by conducting audits and assessments of information systems to ensure:

- information systems risks are measured and managed
- information systems and assets are protected and controlled
- organizational standards, policies, procedures, and processes are adequate and complied with
- information systems controls are efficient and effective
- information systems are acquired, developed, implemented and maintained according to established management policies and practices



CRISCs identify, evaluate, monitor, communicate and manage risk and design, implement, monitor and maintain information systems controls in order to ensure:

- organizational management and stakeholders have a 'common risk view' to assist in making informed business decisions
- information systems controls are aligned with business process objectives and risk tolerance levels
- risks are identified, assessed, evaluated, mitigated and openly communicated in alignment with organizational management vision, strategy and policy
- information systems controls mitigate risk and function effectively and efficiently in accordance with the organization's risk appetite