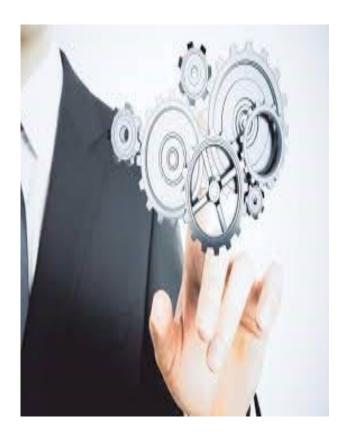


ISACA CISM Boot Camp

The CISM Review Questions, Answers & Explanations Database is a comprehensive 1,000-question pool of items that contains the questions from the CISM Review Questions, Answers & Explanations. The database has been revised according to the recently updated CISM Job Practice.

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CISM candidates to identify their strengths and weaknesses and focus their study efforts accordingly.



Around the world, demand for skilled information security management professionals is on the rise, and the CISM certification is the globally accepted standard of achievement in this area. The uniquely management-focused CISM certification ensures holders understand business, and know how to manage and adapt technology to their enterprise and industry. Since its inception in 2002, more than 30,000 of professionals world-wide have earned the industry-leading CISM to affirm both their high level of technical competence and qualifications for top-caliber leadership and management roles.

IT professionals must have 5 years or more of information security work experience. 2 years of experience requirement is satisfied with CISA/CISSP certification, or Post-graduate degree in information security or a related field (e.g., business administration, information systems, information assurance



CISM Certification Domain 1 - Information Security Governance

Establish and maintain an information security strategy, and align the strategy with corporate governance

Establish and maintain an information security governance framework

Establish and maintain information security policies

Develop a business case

Identify internal and external influences to the organization

Obtain management commitment

Define roles and responsibilities

Establish, monitor, evaluate, and report metrics

CISM Certification Domain 2 - Information Risk Management and Compliance

Establish a process for information asset classification and ownership Identify legal, regulatory, organizational, and other applicable requirements

Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted periodically Determine appropriate risk treatment options

Evaluate information security controls

Identify the gap between current and desired risk levels

Integrate information risk management into business and IT processes Monitor existing risk



CISM Course Goals

Prepare for and pass the Certified Information Security Manager (CISM) exam

Develop an information security strategy and plan of action to implement the strategy

Manage and monitor information security risks

Build and maintain an information security plan both internally and externally Implement policies and procedures to respond to and recover from disruptive and destructive information security events



CISM Certification Domain 4 - Information Security Incident Management

Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents

Establish and maintain an incident response plan

Develop and implement processes to ensure the timely identification of information security incidents
Establish and maintain processes to investigate and document information security incidents
Establish and maintain incident escalation and notification processes
Organize, train, and equip teams to effectively respond to information security incidents

Test and review the incident response plan periodically
Establish and maintain communication plans and processes
Conduct post-incident reviews
Establish and maintain integration
among the incident response plan,
disaster recovery plan, and business
continuity plan about our public and
private training options



CONTACT US: