KnowledgeWoods
Education . Training . Consulting

Aligned to Global Standards


HD Quality Audio/Video Sessions


Storyline Driven Learning


Course end Assessment

Email Based Query Support

24/7 Access

Certified Information Security Manager (CISM) 2013

Estimated Duration (30 Hrs.)

skillsoft | Project Management Institute | Microsoft Partner Silver Project and Portfolio Management Silver Learning | PRINCE2 APPROVED EXAMINATION ORGANIZATION | ITIL TRAINING ORGANIZATION ACCREDITED BY PEOPLECERT | PEARSON VUE-Authorized Test Center

CISM: Information Security Governance (Part 1)

Duration: 2 Hour

- Identify the tasks within the information security governance job practice area
- Recognize the outcomes of information security governance
- Recognize the difference between corporate governance and information security governance
- Match senior management roles with their corresponding responsibilities related to information security governance
- Identify the elements of the information security business model
- Recognize the interconnections between the elements of the information security business model
- Recognize key concepts related to information security governance
- Identify the optimal reporting relationship between senior management and the information security manager
- Label examples of reports about information security according to their intended recipients within an organization
- Identify the goal of converging security-related functions
- Identify categories of key goal indicators
- Recognize key concepts related to information security management

CISM: Information Security Governance (Part 2)

Duration: 2 Hour

- Match the key participants in developing an information security strategy with their corresponding responsibilities
- Recognize appropriate models for developing an information security strategy
- Label examples of pitfalls that organizations may encounter as they develop an information security strategy
- Assess the effectiveness of a given management team's efforts to develop an information security strategy
- Recognize questions that an information strategy should answer
- Recognize two types of objectives an information security strategy should have
- Identify the key elements of a business case for an information security program
- Recognize key concepts related to approaches for determining the desired state of security
- Identify the aspects of security that must be assessed when determining the current state
- Identify the components of a roadmap for achieving security objectives
- Match constraints that must be considered when developing an information security strategy to their corresponding descriptions

CISM: Information Security Governance (Part 3)

Duration: 2 Hour

- Match organizational resources with descriptions of how they are used in developing an information security strategy
- Distinguish between policies, standards, procedures, and guidelines
- Match employee-related resources with descriptions of how they impact development of an information security strategy
- Identify risk-related resources that become part of an information security strategy
- Match strategies for addressing risk to corresponding examples
- Recognize key concepts related to information security strategy resources
- Match the components of an information security action plan with their corresponding roles within the strategy
- Identify types of metrics used to monitor progress toward achieving information security objectives
- Match indicators that security objectives have been met with their corresponding descriptions
- Recognize the key facts about the components of an information security strategy

- Assess the efforts of a given management team to create a roadmap for its information security strategy

CISM: Information Risk Management and Compliance (Part 1)

Duration: 2.5 Hour

- Identify the tasks within the information risk management job practice area
- Identify the outcomes of risk management
- Sequence the steps in planning a risk management program
- Recognize the qualities of a good risk management plan
- Match roles in risk management program development with their corresponding responsibilities
- Recognize the steps of the risk management process
- Distinguish between the concepts of risk management, risk analysis, and risk assessment
- Recognizing activities of the risk management program planning process
- Associate steps in the risk management process with specific outcomes of an effective risk management program
- Label examples as either threats or vulnerabilities
- Recognize examples of risk categories
- Recognize the process for conducting a semiquantitative risk analysis
- Match quantitative risk analysis methods with their corresponding descriptions
- Match common risk assessment methodologies with corresponding descriptions

CISM: Information Risk Management and Compliance (Part 2)

Duration: 2.5 Hour

- Identify examples of information assets that should be valuated
- Match valuation methods with corresponding examples
- Recognize how to classify information assets
- Match disaster recovery terms with their corresponding definitions
- Recognize considerations related to outsourcing security services to a third-party provider
- Determine information asset valuation methodologies used by a given information security manager
- Perform information asset classification
- Distinguish between examples of rtos and rpos
- Match risk treatment options with corresponding examples of their use
- Classify examples of controls
- Identify types of controls
- Recognize considerations when planning controls and countermeasures
- Identify the key responsibilities of an information security manager related to risk monitoring and communication
- Recognize methods of integrating risk management processes with other life-cycle processes within an organization
- Determine appropriate actions to effectively manage a given risk

CISM: Information Security Program Development and Management (Part 1)

Duration: 1.5 Hour

- Define the purpose of the information security program development and management domain
- Describe the tasks within information security program development and management job practice area
- Describe the fundamentals of an information security program
- Recognize how an information security program supports the objectives of information security governance
- Identify the defining goals of the information security program
- Identify key information security program concepts
- Develop an information security program
- Develop an information security program

- Recognize risk assessment concepts
- Perform quantitative risk analysis, given a scenario

CISM: Information Security Program Development and Management (Part 2)

Duration: 1.5 Hour

- Describe the function of COBIT 5 in the information security management framework
- Identify the objectives of the information security management framework
- Describe the function of ISO/IEC 27001:2013 in the information security management framework
- Recognize the components of the information security management framework
- Create an information security program road map
- Recognize what the information security architecture involves
- Recognize the questions an information security manager should ask when building an IS architecture
- Develop an information security management framework

CISM: Information Security Program Development and Management (Part 3)

Duration: 1.5 Hour

- Identify responsibilities of an information security manager related to administering an information security program
- Identify good practices related to security personnel and positive security culture
- Identify areas that should be part of a security awareness program
- Identify areas that an information security manager must be aware of and raise awareness of amongst security personnel
- Identify responsibilities of information security manager related to documentation
- Identify project management processes that are performed by information security managers
- Recognize key activities of the PDCA methodology
- Identify key points regarding the evaluation of an information security program
- Recognize key points related to information security management
- Recognize key project management responsibilities of an information security manager
- Recognize key points about evaluating an information security program

CISM: Information Security Program Development and Management (Part 4)

Duration: 2 Hour

- Match information organizational roles to their corresponding responsibilities
- Determine the responsibilities of individuals within an organization related to standard security program components
- Sequence the steps of a security review, given a scenario
- Identify key points regarding audits that an information security manager should remember during program implementation
- Identify preventive measures that minimize security risk
- Identify the responsibilities of an information security manager with relation to compliance monitoring and enforcement
- Recognize the results of commonly used risk analysis methods
- Recognize the responsibilities of an information security manager related to monitoring and compliance
- Identify activities that allow an information security manager to integrate a security program within an organization
- Recognize strategies for managing risk of outsourcing when using third-party service providers
- Recognize examples of cloud computing models
- Recognize the responsibilities of an information security manager related to process integration and outsourcing

CISM: Information Security Program Development and Management (Part 5)

Duration: 2 Hour

- Distinguish between two types of information security controls
- Recognize principles of effective security control
- Recognize examples of physical, environmental, and technical controls
- Distinguish between examples of controls and countermeasures
- Identify factors to consider when recommending improvements to information security controls
- Describe types of controls and how they are used in information security management
- Explain the use of controls and countermeasures to manage risk
- Categorize examples of information security metrics
- Determine whether a given metric would be effective
- Recognize examples of measures used to assess the effectiveness of an information security program
- Recognize examples of monitoring activities
- Recognize the relationship between information security metrics, measurement, and monitoring
- Recognize effective approaches to measuring and monitoring an information security program

CISM: Information Security Incident Management (Part 1)

Duration: 2.5 Hour

- Identify the tasks within the incident management and response job practice area
- Recognize incident management planning considerations
- Order the steps in the incident management process
- Recognize the elements of an incident management plan
- Match causes of challenges in developing an incident management plan with corresponding solutions
- Recognize key points related to incident management planning
- Matching key incident management roles and their corresponding responsibilities
- Identify the roles that make up an incident response team
- Recognize examples of personal skills required by members of an incident response team
- Recognize examples of technical knowledge required by members of an incident response team
- Recognize the activities that are performed during a business impact analysis
- Conduct a business impact analysis using incident management resources

CISM: Information Security Incident Management (Part 2)

Duration: 2 Hour

- Determine the appropriate method for identifying the current state of response capability for a given company
- Identify the factors that determine incident response capability
- Match phases of an incident response plan with their corresponding descriptions
- Match members of response and recovery teams with their corresponding responsibilities
- Recognize examples of individuals who may require notification in case of a serious security incident
- Recognize the types of insurance coverage that an organization may have
- Label descriptions of different types of recovery sites
- Determine the appropriate type of recovery site given examples of requirements
- Recognize methods for recovering communication and computing systems
- Distinguish between the characteristics of an incident response plan and a recovery plan
- Recognize the method being used to test incident response and recovery plans
- Recognize examples of metrics used for testing incident response and recovery plans
- Identify important aspects of executing incident response and recovery plans
- Recognize key concepts related to testing and incident management

- Recognize strategies for overcoming common challenges to information security management