ISACA CISM Exam Summary:

Exam Name	ISACA Certified Information Security Manager (CISM)
Exam Code	CISM
Exam Price ISACA Member	$575 (USD)
Exam Price ISACA Nonmember	$760 (USD)
Duration	240 mins
Number of Questions	150
Passing Score	450/800
Books / Training	CISM requirements, CISM Review Manual
Schedule Exam	Exam Registration
Sample Questions	ISACA CISM Sample Questions
Practice Exam	**ISACA CISM Certification Practice Exam**

ISACA CISM Exam Syllabus Topics:

Topic	Details	Weights
Information Security Governance	- Establish and/or maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives. **- Task Statements** • Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program. • Establish and/or maintain an information security governance framework to guide activities that support the information security strategy. • Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program. • Establish and maintain information security policies to guide the development of standards, procedures and	24%

Topic	Details	Weights
	guidelines in alignment with enterprise goals and objectives. • Develop business cases to support investments in information security. • Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy. • Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy. • Define, communicate, and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end-users, privileged or high-risk users) and lines of authority. • Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy. **- Knowledge Statements** • Knowledge of techniques used to develop an information security strategy (e.g., SWOT [strengths, weaknesses, opportunities, threats] analysis, gap analysis, threat research) • Knowledge of the relationship of information security to business	

Topic	Details	Weights
	goals, objectives, functions, processes and practices. • Knowledge of available information security governance frameworks. • Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development. • Knowledge of the fundamental concepts of governance and how they relate to information security. • Knowledge of methods to assess, plan, design and implement an information security governance framework. • Knowledge of methods to integrate information security governance into corporate governance. • Knowledge of contributing factors and parameters (e.g., organizational structure and culture, tone at the top, regulations) for information security policy development • Knowledge of content in, and techniques to develop, business cases. • Knowledge of strategic budgetary planning and reporting methods. • Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy.	

Topic	Details	Weights
	• Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact). • Knowledge of methods and considerations for communicating with senior leadership and other stakeholders (e.g., organizational culture, channels of communication, highlighting essential aspects of information security). • Knowledge of roles and responsibilities of the information security manager. • Knowledge of organizational structures, lines of authority and escalation points. • Knowledge of information security responsibilities of staff across the organization (e.g., data owners, end-users, privileged or high-risk users) • Knowledge of processes to monitor performance of information security responsibilities. • Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization. • Knowledge of methods to select, implement and interpret key information security metrics (e.g., key performance indicators [KPIs] or key risk indicators [KRIs]).	
Information Risk Management	- Manage information risk to an acceptable level based on risk appetite	30%

Topic	Details	Weights
	in order to meet organizational goals and objectives. **- Task Statements** • Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value. • Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels. • Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information. • Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite. • Determine whether information security controls are appropriate and effectively manage risk to an acceptable level. • Facilitate the integration of information risk management into business and IT processes (e.g., systems development, procurement, project management) to enable a consistent and comprehensive information risk management program across the organization. • Monitor for internal and external factors (e.g., key risk indicators [KRIs], threat	

Topic	Details	Weights
	landscape, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately. • Report noncompliance and other changes in information risk to facilitate the risk management decision-making process. • Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives. **- Knowledge Statements** • Knowledge of methods to establish an information asset classification model consistent with business objectives. • Knowledge of considerations for assigning ownership of information assets and risk. • Knowledge of methods to identify and evaluate the impact of internal or external events on information assets and the business. • Knowledge of methods used to monitor internal or external risk factors. • Knowledge of information asset valuation methodologies. • Knowledge of legal, regulatory, organizational and other requirements related to information security. • Knowledge of reputable, reliable and timely sources of information regarding emerging information security threats and vulnerabilities.	

Topic	Details	Weights
	• Knowledge of events that may require risk reassessments and changes to information security program elements. • Knowledge of information threats, vulnerabilities and exposures and their evolving nature. • Knowledge of risk assessment and analysis methodologies. • Knowledge of methods used to prioritize risk scenarios and risk treatment/response options. • Knowledge of risk reporting requirements (e.g., frequency, audience, content). • Knowledge of risk treatment/response options (avoid, mitigate, accept or transfer) and methods to apply them. • Knowledge of control baselines and standards and their relationships to risk assessments. • Knowledge of information security controls and the methods to analyze their effectiveness. • Knowledge of gap analysis techniques as related to information security. • Knowledge of techniques for integrating information security risk management into business and IT processes. • Knowledge of compliance reporting requirements and processes. • Knowledge of cost/benefit analysis to assess risk treatment options.	
Information Security Program Development and Management	- Develop and maintain an information security program that identifies, manages and protects the organization’s assets while aligning to	27%

Topic	Details	Weights
	information security strategy and business goals, thereby supporting an effective security posture. **- Task Statements** • Establish and/or maintain the information security program in alignment with the information security strategy. • Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business. • Identify, acquire and manage requirements for internal and external resources to execute the information security program. • Establish and maintain information security processes and resources (including people and technologies) to execute the information security program in alignment with the organization's business goals. • Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies. • Establish, promote and maintain a program for information security awareness and training to foster an effective security culture. • Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, system	

Topic	Details	Weights
	development, business continuity, disaster recovery) to maintain the organization's security strategy. • Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) and monitor adherence to established requirements in order to maintain the organization's security strategy. • Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program. • Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance. **- Knowledge Statements** • Knowledge of methods to align information security program requirements with those of other business functions • Knowledge of methods to identify, acquire, manage and define requirements for internal and external resources • Knowledge of current and emerging information security technologies and underlying concepts • Knowledge of methods to design and implement information security controls	

Topic	Details	Weights
	• Knowledge of information security processes and resources (including people and technologies) in alignment with the organization's business goals and methods to apply them • Knowledge of methods to develop information security standards, procedures and guidelines • Knowledge of internationally recognized regulations, standards, frameworks and best practices related to information security program development and management • Knowledge of methods to implement and communicate information security policies, standards, procedures and guidelines • Knowledge of training, certifications and skill set development for information security personnel • Knowledge of methods to establish and maintain effective information security awareness and training programs • Knowledge of methods to integrate information security requirements into organizational processes (e.g., access management, change management, audit processes) • Knowledge of methods to incorporate information security requirements into contracts, agreements and third-party management processes • Knowledge of methods to monitor and review contracts and agreements with third parties and associated change processes as required	

Topic	Details	Weights
	• Knowledge of methods to design, implement and report operational information security metrics • Knowledge of methods for testing the effectiveness and efficiency of information security controls • Knowledge of techniques to communicate information security program status to key stakeholders	
Information Security Incident Management	- Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact. **- Task Statements** • Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents. • Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents. • Develop and implement processes to ensure the timely identification of information security incidents that could impact the business. • Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements. • Establish and maintain incident notification and escalation	

Topic	Details	Weights
	processes to ensure that the appropriate stakeholders are involved in incident response management. • Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner. • Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities. • Establish and maintain communication plans and processes to manage communication with internal and external entities. • Conduct post-incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions. • Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan. **- Knowledge Statements** • Knowledge of incident management concepts and practices. • Knowledge of the components of an incident response plan. • Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan.	

Topic	Details	Weights
	• Knowledge of incident classification/categorization methods. • Knowledge of incident containment methods to minimize adverse operational impact. • Knowledge of notification and escalation processes. • Knowledge of the roles and responsibilities in identifying and managing information security incidents. • Knowledge of the types and sources of training, tools and equipment required to adequately equip incident response teams. • Knowledge of forensic requirements and capabilities for collecting, preserving and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody). • Knowledge of internal and external incident reporting requirements and procedures. • Knowledge of post-incident review practices and investigative methods to identify root causes and determine corrective actions. • Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents. • Knowledge of technologies and processes to detect, log, analyze and document information security events. • Knowledge of internal and external resources available to investigate information security incidents.	

Topic	Details	Weights
	• Knowledge of methods to identify and quantify the potential impact of changes made to the operating environment during the incident response process. • Knowledge of techniques to test the incident response plan. • Knowledge of applicable regulatory, legal and organization requirements. • Knowledge of key indicators/metrics to evaluate the effectiveness of the incident response plan.	