Hewlett Packard Enterprise

HPE Digital Learner CISA + CISM Content Pack

HPE Content Pack number	CP035
Content Pack length	22 Hours
Content Pack category	Category 2
Learn more	**View now**

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

This training prepares students for the CISM and CISA examination and certification process. CISM and CISA are both offered by ISACA.

CISM (Certified Information Security Manager) is management-focused, promotes international security practices, and recognizes the individual who manages, designs, oversees and assesses an enterprise's information security.

CISA (Certified Information Systems Auditor) is a globally recognized certification for IS audit control, assurance, and security professionals. It showcases your audit experience, skills and knowledge, and demonstrates your capability to assess vulnerabilities, report on compliance and institute controls within the enterprise.

Audience

This course is for security professionals with a specific focus on cybersecurity, specifically management and auditing. HPE believes these two complement each other from a management perspective.

Pre-Requisites

Both certifications have a range of pre-requisites that require compliance in terms of work experience. Details can be found at the following websites:

- CISM – Complete the CISM Application for Certification: www.isaca.org/cismapp
- CISA – Complete the CISA Application for Certification: www.isaca.org/cisaapp

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Objectives

The objective of CISM training is for learners to fully understand and be able to articulate the four domains. This course also assists in the preparation of candidates for the optional CISM examination using job practice domains, tasks and knowledge statements. Domains are as follows:

- Information Security Governance (24%)
- Information Risk Management (30%)
- Information Security Program Development and Management (27%)
- Information Security Incident Management (19%)

The objective of CISA training is for learners to fully understand and be able to articulate the following five domains. This course also assists in the preparation of candidates for the optional CISA examination using job practice domains, tasks and knowledge statements. Domains are as follows:

- The Process of Auditing Information Systems (21%)
- Governance and Management of IT (16%)
- Information Systems Acquisition, Development and Implementation (18%)
- Information Systems Operations, Maintenance and Service Management (20%)
- Protection of Information Assets (25%)

Examination

- The CISM examination consists of 200 multiple choice questions to be answered within four hours.
- The CISA examination consists of 200 multiple choice questions to be answered within four hours.
- On completion of the exam, the raw score is converted into a point scale of 200 – 800. To pass the exam, candidates must receive a scaled score of 450, representing a minimum consistent standard of knowledge determined by ISACA.

Detailed Content Pack outline

CISA: The Process of Auditing Information Systems - Part 1

- Recognize the task and knowledge statements of domain 1
- Describe characteristics of the IS audit function
- Identify best practices in IS audit resource management
- Identify best practices for planning audits
- Identify the effects of laws and regulations on IS audit planning
- Recognize the ISACA Code of Professional Ethics
- Identify the IS audit and assurance general standards
- Identify the IS audit and assurance performance standards
- Identify the IS audit and assurance reporting standards
- Identify the IS audit and assurance general guidelines
- Identify the IS audit and assurance performance guidelines
- Identify the IS audit and assurance reporting guidelines
- Distinguish between the different categories of IS audit and assurance tools and techniques
- Identify best practices when applying ISACA guidelines, standards, and tools and techniques in relation to each other, and external guidelines such as regulatory requirements
- Recognize characteristics of the ITAF reference model
- Identify the steps of the risk management process
- Distinguish between preventive, detective and corrective controls
- Identify different types of IS control objectives
- Describe how the COBIT 5 framework is used as part of IS control
- Identify general controls used for information systems
- Identify IS control procedures
- Identify best practices when planning and managing IS audits

CISA: The Process of Auditing Information Systems - Part 2

- Describe the objectives of an IS audit
- Distinguish between different types of audits
- Identify characteristics of an audit methodology
- Identify best practices in a risk-based audit approach
- Recognize risk influences and best practices when auditing risk for materiality
- Identify risk assessment and risk treatment best practices
- Describe characteristics of audit programs
- Identify best practices for fraud detection when performing IS audits
- Distinguish between compliance and substantive testing when conducting IS audits
- Distinguish between different computer-assisted audit techniques and tools
- Identify best practices for evaluating the control environment
- Describe characteristics and best practices for using exit interviews and audit reports to present IS audit findings
- Identify characteristics and best practices of audit documentation
- Identify best practices for evaluating and using evidence when conducting IS audits
- Identify best practices when interviewing and observing personnel in performance of their duties
- Identify best practices for sampling as part of an IS audit
- Identify best practices when outsourcing IS assurance and security services for IS audit activities
- Identify best practices for IS audit follow-up activities
- Recognize the characteristics and objectives of CSA
- Identify the benefits and disadvantages of CSA
- Describe the auditor's role in a CSA program
- Identify characteristics of the CSA approach and its technology drivers
- Identify best practices for integrating auditing activities in an organization
- Identify best practices for continuous auditing activities in an organization
- Identify best practices for managing risk, communicating results, and CSA during IS audit activities

CISA: Governance and Management of IT - Part 1

- Recognize the task and knowledge statements of domain 2
- Identify characteristics of corporate governance
- Identify GEIT characteristics and best practices
- Recognize the purpose and responsibilities of IT governing committees
- Describe the purpose and characteristics of an IT balanced scorecard
- Identify IS governance best practices
- Describe the purpose and best practices of EA
- Recognize the role of IS strategic planning in IS audit activities
- Identify characteristics and role of procedures in the IS audit framework
- Identify characteristics of risk management and the steps for developing a risk management program
- Identify role and responsibilities of an IT steering committee
- Distinguish between different maturity process improvement models
- Recognize the financial and nonfinancial value of IT
- Identify characteristics of IT portfolio management
- Identify characteristics and role of policies in the IS audit framework
- Distinguish between the steps of the risk management process; distinguish between qualitative, semi-quantitative and quantitative analysis methods
- Identify characteristics of organizational human resource management practices
- Distinguish between different sourcing options for delivering and performing IT functions
- Identify characteristics of organizational change management practices
- Identify characteristics of financial management practices
- Identify characteristics of information security management practices
- Identify characteristics and best practices of performance optimization
- Identify best practices for IT governance, IT risk management, and general IT management in an organization

CISA: Governance and Management of IT - Part 2

- Distinguish between the different IT roles and responsibilities
- Identify characteristics and best practices of segregation of duties within IT
- Identify characteristics and best practices of segregation of duties controls
- Identify the documents that are reviewed as part of auditing IT governance structure and implementation
- Identify best practices when reviewing contractual commitments as part of auditing IT governance structure and implementation
- Identify characteristics and best practices of IT business continuity planning
- Identify best practices for auditing disaster and other disruptive events procedures
- Identify characteristics and best practices in business continuity planning process and policy activities
- Distinguish between the different classifications of incident and best practices for incident management
- Identify characteristics and best practices of business impact analysis
- Identify the factors and issues for consideration when developing business continuity plans
- Identify the components and best practices of a business continuity plan
- Identify best practices for testing business continuity plans
- Identify the audit procedures to follow when reviewing business continuity plans
- Identify best practices when evaluating prior test results and interviewing key personnel
- Identify best practices when evaluating offsite storage and offsite facility security
- Identify best practices for reviewing alternative processing contracts and insurance coverage
- Identify best practices when auditing the IT organizational structure, implementation practices, and business continuity plans of an organization

CISA: Information Systems Acquisition, Development, and Implementation

- Recognize the task and knowledge statements of domain 3
- Identify the objectives, characteristics, and techniques of benefits realization through portfolio/program management and business case development and approval
- Identify characteristics of the project management structure
- Identify characteristics of project initiation and planning
- Identify characteristics of project execution, control and closure
- Identify characteristics of the SDLC approach and phases, integrated resource management systems, and risk associated with software development
- Identify characteristics of the SDLC approach and phases, integrated resource management systems, and risk associated with software development
- Identify characteristics, key risk areas, and typical controls of virtual and cloud environments
- Distinguish between e-commerce, Electronic Data Interchange, email, point-of-sale, electronic banking, electronic finance, payment, and integrated manufacturing business application system characteristics
- Distinguish between electronic funds transfer, ATM, interactive voice response, purchase accounting, image processing, industrial control, AI and expert, business intelligence, decision support, customer relationship management, and supply chain management business application systems characteristics
- Distinguish between structured analysis, design and development techniques, Agile, prototyping-evolutionary, rapid application, and object-oriented system development methods
- Distinguish between component-based, web-based application, software reengineering, and reverse engineering development methods
- Identify characteristics of physical architecture analysis, infrastructure implementation planning, and critical success factors in infrastructure development activities
- Identify best practices for hardware acquisition, system software acquisition, and system software implementation activities
- Identify characteristics and best practices for the change management process and change management documentation
- Identify characteristics and best practices for testing and auditing change programs, emergency changes, and configuration management
- Identify characteristics and best practices for code generators, computer-aided software engineering, and fourth-generation languages
- Distinguish between BPR methods and techniques, ISO 9126, CMMI, and ISO/IEC 330XX series process improvement practices
- Identify characteristics of input/origination controls
- Identify characteristics of processing procedures and controls
- Identify characteristics of output controls and business process control assurance best practices
- Identify best practices for auditing application controls
- Identify best practices for auditing systems development, acquisition, and maintenance
- Identify best practices when auditing IS acquisitions, development, and implementation activities within an organization

CISA: Information Systems Operations, Maintenance, and Service Management

- Recognize key concepts of domain 4
- Identify characteristics and best practices of IS operations management
- Identify characteristics of IT service management frameworks and best practices
- Identify best practices for IS operations
- Identify problem management and support/help desk best practices
- Identify characteristics and best practices of change management, release management, and quality assurance in IS operations
- Identify characteristics and best practices for IT asset management
- Distinguish between computer hardware components
- Identify characteristics and best practices for hardware maintenance and hardware monitoring
- Identify characteristics and best practices for capacity planning and monitoring activities
- Identify operating systems features and options
- Identify characteristics of access control software and data communications software
- Identify characteristics and best practices for data management
- Identify characteristics and best practices of a DBMS
- Identify characteristics of utility programs, source code management, end-user computing, and utility programs in IS architecture and software
- Identify characteristics of enterprise network architectures, types of networks, and network services, standards, and protocols
- Identify characteristics of OSI architecture and best practices for applying the OSI model in network architectures
- Identify best practices for auditing and reviewing enterprise architecture, hardware, operating system, database, and network infrastructure
- Identify best practices for auditing and reviewing IS operations, scheduling, and problem management reporting
- Identify best practices for disaster recovery point and time objectives, recovery strategies, and recovery alternatives
- Identify best practices for developing a disaster recovery plan, and organizing and assigning responsibilities within an organization
- Identify backup and restoration options and best practices
- Distinguish between disaster recovery testing methods and identify best practices for testing disaster recovery plans and activities in an organization
- Identify best practices for invoking disaster recovery plans within an organization
- Identify best practices when auditing IS operations, maintenance, and service management activities within an organization

CISA: Protection of Information Assets - Part 1

- Recognize key concepts in domain 5
- Identify characteristics and key elements of information security management and information security management systems
- Distinguish between the different information security roles and responsibilities
- Identify characteristics and best practices of classifying information assets
- Identify fraud risk factors in information security management
- Identify characteristics of information security control design
- Identify characteristics and best practices of system access permission activities
- Recognize characteristics of mandatory and discretionary access controls
- Identify privacy principles and the IS auditor's role
- Identify the critical success factors of information security management and awareness, training and education best practices
- Identify best practices for information security activities involving external parties
- Identify best practices for human resources activities with third parties
- Identify characteristics of computer crime issues and exposures, and best practices for avoiding negative impacts
- Identify best practices for security incident handling and response activities
- Identify logical access exposures
- Identify best practices for enterprise IT environment familiarization
- Identify best practices when auditing paths of logical access
- Identify logical access control software
- Identify best practices for identification and authentication activities
- Identify features of SSO
- Identify best practices for storing, retrieving, transporting, and disposing confidential information
- Identify best practices for information security management and logical access

CISA: Protection of Information Assets - Part 2

- Identify characteristics of LAN security including virtualization
- Identify characteristics of client-server security
- Identify best practices for wireless security
- Distinguish between common internet threats
- Distinguish between different firewall technologies
- Compare IDS and IPS
- Identify cryptography and cryptanalysis
- Identify common cryptosystems
- Classify common cryptosystems
- Identify characteristics of malware and best practices for mitigating risk from them
- Identify characteristics and security issues of VoIP
- Recognize characteristics of PBX
- Identify best practices for auditing information security management frameworks
- Identify best practices for auditing logical access
- Distinguish between different security testing techniques when auditing information security management frameworks
- Identify investigation techniques and best practices when auditing information security management frameworks
- Identify characteristics and best practices for auditing remote access, auditing internet points of presence, and performing network penetration tests
- Identify characteristics and best practices for performing full network assessment reviews, for auditing network change development and authorization, and for auditing unauthorized changes activities
- Identify environmental issues and exposures
- Distinguish between different controls for environmental exposures
- Identify best practices for auditing environmental controls
- Identify physical access issues and exposures, and controls for mitigating threats
- Identify best practices for auditing physical access
- Identify mobile computing information security best practices
- Identify peer-to-peer computing information security best practices
- Identify instant messaging information security best practices
- Identify social media information security best practices
- Identify cloud computing information security best practices
- Identify characteristics and best practices for data leak prevention
- Identify challenges and considerations for data leak prevention techniques and practices
- Identify end-user security risks and controls
- Identify best practices for auditing information security management frameworks and mobile, social, and cloud asset protection

CISM: Information Security Governance Part 1

- Identify InfoSec strategy techniques
- Compare InfoSec relationships to key factors
- Describe InfoSec governance frameworks
- Recognize concepts of governance
- Recall standards, frameworks and best practices
- Define governance planning, design and implementation
- Work with integrating into corporate governance
- Specify the contributing factors for InfoSec development
- Recognize developing business cases
- Describe strategic budgetary planning and reporting
- Describe InfoSec governance

CISM: Information Security Governance Part 2

- Recognize the impact of internal and external influences
- Obtain commitment from senior leadership and stakeholders by using key information
- Specify the methods and considerations of senior leadership and stakeholder communication
- Define the responsibilities of the InfoSec manager
- Describe the types of organizational structures, lines of authority, and escalation points
- Recognize information security responsibilities of staff across the organization
- Recognize processes to monitor performance of InfoSec responsibilities
- Describe reporting and communication channels
- Work with key information security metrics
- Define InfoSec governance

CISM: Information Risk Management Part 1

- Recognize information asset classification
- Assign ownership of assets and risk
- Evaluate impacts of events on information assets
- Monitor internal and external risk factors
- Recognize information asset valuation methods
- Specify legal, regulatory and organizational requirements
- Recognize information security threat sources
- Identify events needing risk reassessment
- Define information threats, vulnerabilities and exposures
- Describe what is involved with information risk management

CISM: Information Risk Management Part 2

- Identify risk assessment and analysis methodologies
- Prioritize risk scenarios and treatment
- Specify risk reporting requirements
- Apply risk treatment and response methodologies
- Compare control baselines and standards
- Analyze information security controls and methods
- Describe information security gap analysis techniques
- Define risk management for business and IT processes
- Specify compliance reporting requirements and processes
- Perform cost benefit analysis for risk assessment
- Describe information risk management

CISM: Information Security Program Development and Management Part 1 • Align security programs with business functions • Acquire and manage resource requirements • Recognize current and emerging security technologies	• Design and implement security controls • Apply information security controls and resources • Define security standards, procedures and guidelines	• Describe regulations, standards, frameworks and practices • Implement information security standards • Describe program development and control
CISM: Information Security Program Development and Management Part 2 • Describe skills training for information security personnel • Develop security awareness and training programs	• Integrate mandates into organizational processes • Define contracts, agreements and third-parties • Review third-party contracts and agreements • Implement operational security metrics	• Test the effectiveness of security controls • Communicate program status to key stakeholders • Describe program development and management
CISM: Information Security Incident Management Part 1 • Describe incident management concepts • Define components of an incident response plan (IRP) • Map the BCP and DRP to the IRP	• Specify methods for incident classification and categorization • Define incident containment methods • Describe notification and escalation processes	• Define roles and responsibilities in security Incidents • Know IRT training, tools and equipment • Classify forensic requirements for handling evidence • Describe security incident management
CISM: Information Security Incident Management Part 2 • Describe incident reporting requirements and procedures • Define post-incident review practices and investigations • Quantify damages, costs and business impacts	• Detect, log, analyze and document events • Classify resources for investigation of incidents • Identify impact of changes to the environment • Know techniques to test the incident response plan	• Specify regulatory, legal and organization requirements • Define KPIs and metrics to evaluate the response plan • Define InfoSec security management

Learn more at

www.hpe.com/ww/digitallearner

www.hpe.com/ww/digitallearner-contentpack

Follow us:

CP035, May 2019

Hewlett Packard Enterprise