HPE Digital Learner CISA + CISM Content Pack

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
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 ISAF reference model

**CISA: The Process of Auditing Information Systems - Part 2**
- Describe the objectives of an IS audit
- Distinguish between objectives of different types of audits
- Describe 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
- Identify best practices when using ISACA guidelines, standards, and tools and techniques in relation to each other, and external guidelines such as regulatory requirements
- Recognize characteristics of the ISAF reference model

**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 the 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
- 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 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/originatation 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 for IS operations
- 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
- 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
- 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
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify characteristics of LAN security including virtualization</td>
<td>• Recall standards, frameworks and best practices</td>
<td>• Define the responsibilities of the InfoSec manager</td>
<td>• Monitor internal and external risk factors</td>
<td></td>
</tr>
<tr>
<td>• Identify characteristics of client-server security</td>
<td>• Define governance planning, design and implementation</td>
<td>• Describe types of organizational structures, lines of authority, and escalation points</td>
<td>• Recognize information asset classification</td>
<td></td>
</tr>
<tr>
<td>• Identify best practices for wireless security</td>
<td>• Work with integrating into corporate governance</td>
<td>• Recognize information security responsibilities of staff across the organization</td>
<td>• Assign ownership of assets and risk</td>
<td></td>
</tr>
<tr>
<td>• Distinguish between common internet threats</td>
<td>• Specify the contributing factors for InfoSec development</td>
<td>• Recognize processes to monitor performance of InfoSec responsibilities</td>
<td>• Evaluate impacts of events on information assets</td>
<td></td>
</tr>
<tr>
<td>• Distinguish between different firewall technologies</td>
<td></td>
<td>• Describe reporting and communication channels</td>
<td>• Identify information asset classification and analysis methodologies</td>
<td></td>
</tr>
<tr>
<td>• Compare IDS and IPS</td>
<td></td>
<td>• Work with key information security metrics</td>
<td>• Prioritize risk scenarios and treatment</td>
<td></td>
</tr>
<tr>
<td>• Identify cryptography and cryptanalysis</td>
<td>• Recognize developing business cases</td>
<td>• Define information threats, vulnerabilities and exposures</td>
<td>• Specify risk reporting requirements</td>
<td></td>
</tr>
<tr>
<td>• Identify common cryptosystems</td>
<td>• Describe strategic budgetary planning and reporting</td>
<td>• Describe what is involved with information risk management</td>
<td>• Apply risk treatment and response methodologies</td>
<td></td>
</tr>
<tr>
<td>• Classify common cryptosystems</td>
<td>• Describe InfoSec governance</td>
<td></td>
<td>• Compare control baselines and standards</td>
<td></td>
</tr>
<tr>
<td>• Identify characteristics of malware and best practices for mitigating risk from them</td>
<td></td>
<td></td>
<td>• Analyze information security controls and methods</td>
<td></td>
</tr>
<tr>
<td>• Identify characteristics and security issues of VoIP</td>
<td></td>
<td></td>
<td>• Describe information security gap analysis techniques</td>
<td></td>
</tr>
<tr>
<td>• Recognize characteristics of PBX</td>
<td></td>
<td></td>
<td>• Define risk management for business and IT processes</td>
<td></td>
</tr>
<tr>
<td>• Identify best practices for auditing information security management frameworks</td>
<td></td>
<td></td>
<td>• Specify compliance reporting requirements and processes</td>
<td></td>
</tr>
<tr>
<td>• Identify best practices for auditing logical access</td>
<td></td>
<td></td>
<td>• Perform cost benefit analysis for risk assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Describe information risk management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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

### CISM: Information Security Program Development and Management Part 2
- Integrate mandates into organizational processes
- Define contracts, agreements and third-parties
- Review third-party contracts and agreements
- Implement operational security metrics

### 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

### 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

### CISM: Information Security Program Development and Management
- 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 Incident Management
- Specify methods for incident classification and categorization
- Define incident containment methods
- Describe notification and escalation processes
- Implement operational security metrics

Learn more at [www.hpe.com/ww/digitallearner](http://www.hpe.com/ww/digitallearner)  

Interested in purchase of this Content Pack as a stand-alone WBT? Contact Us for information on purchasing this Content Pack for individual use.