

CISA®, Certified Information Systems Auditor® + Oefen vragen (QAE)

Cursusduur: 4 Dagen Cursuscode: CISAU

Beschrijving:

CISA® — Certified Information Systems Auditor is the globally recognized gold standard for IS audit, control, and assurance, in demand and valued by leading global brands. It's often a mandatory qualification for employment as an IT auditor. CISA professionals offer the credibility to leverage standards, manage vulnerabilities, ensure compliance, offer solutions, institute controls and deliver value to organizations.

This 4-day CISA training course is the preparation for your CISA certification. During this course, you will learn about the IT audit process.

Continuing Professional Education (CPE) : 31

Doelgroep:

Designed for mid-career IS audit, control and assurance professionals looking to leverage career growth including: IT Audit Directors/Managers/Consultants IT Auditors Compliance/Risk/Privacy Directors IT Directors/Managers/Consultants

Doelstelling:

- Reduce risk: CISAs provide assurance that the organization's IT and business systems are effectively monitored, managed and protected.
- Create a common language: CISAs serve as trusted business advisors by assuring that the necessary leadership and organizational structures and processes are in place to achieve business objectives and support the enterprise's strategy.
- Drive business successes: Regulators and clients look for a CISA designation and many businesses and government agencies require it.
- Be prepared: Research has shown that businesses lose up to 5% of their annual revenue to fraud and irregularities. This reality is prompting leadership to hire CISAs to implement preventive controls and provide assurance on information security and risk management.

Vereiste kennis en vaardigheden:

There are no specific entry requirements to participate in this CISA training.

Examens en certificering

- Please note: The exam voucher is not included in the course price.
- 4 hours (240 minutes),
- 150 multiple choice questions
- In addition to passing the examination, there are additional requirements for obtaining the certificate. These can be found at: <https://www.isaca.org/credentialing/cisa/get-cisa-certified>

Vervolg cursussen:

CISSP Certification Preparation

Cursusinhoud:

Domain 1—INFORMATION SYSTEMS AUDITING PROCESS - (21%)

Providing audit services in accordance with standards to assist organizations in protecting and controlling information systems. Domain 1 affirms your credibility to offer conclusions on the state of an organization's IS/IT security, risk and control solutions.

A. Planning

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management

B. IT Management

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management

- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

B. Execution

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT

- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

Domain 3—Information Systems Acquisition, Development and Implementation - (12%) ?

A. Information Systems Acquisition and Development

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies

- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

B. Business Resilience

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces

- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

Domain 2—Governance and Management of IT - (17%)

Domain 2 confirms to stakeholders your abilities to identify critical issues and recommend enterprise-specific practices to support and safeguard the governance of information and related technologies.

A. IT Governance

- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

??B. Information Systems Implementation

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication

- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

Domain 5—Protection of Information Assets - (27%)

Cybersecurity now touches virtually every information systems role, and understanding its principles, best practices and pitfalls is a major focus within Domain 5.

?A. Information Asset Security and Control

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

- Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

Domain 4—INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE - (23%)

Domains 3 and 4 offer proof not only of your competency in IT controls, but also your understanding of how IT relates to business.

A. Information Systems Operations

B. Security Event Management

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)??
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental

Controls

- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein