ControlSolutions International

CISA Certified Information Systems Auditor®
An ISACA® Certification

ISACA®

Trust in, and value from, information systems

ISACA®
Trust in, and value from, information systems

ControlSolutions International

Agenda

- Introductie
- Wat is (een) CISA?
- Waarom zou je CISA worden?
- Hoe word je CISA?
- Hoe blijf je CISA?

ControlSolutions International

Introductie

- Zari Haji Rasoul RE CISA
- IT-Auditor
- Partner bij ControlSolutions International

- Achtergrond
  - PWC (senior IT-Auditor en Consultant)
  - Ziggo (Senior IT-Audit / IT Risk Manager)
  - Freelance IT-auditor en consultant

Wat is (een) CISA

- Certified Information Systems Auditor
- Wereldwijd (h)erkend en geaccepteerd
- Staat voor:
  - Onafhankelijkheid
  - Onpartijdigheid
  - Deskundigheid
- IT Audit, Control & Security
- De eisen voor CISA worden gezien als zeer hoog
- Grote beroepsgroep (85.000+ certificaten)

Wat is (een) CISA

Definition of auditing

Systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an economic entity or event for the purpose of forming an opinion about and reporting on the degree to which the assertion conforms to an identified set of standards.

Definition of IS auditing

Any audit that encompasses review and evaluation (wholly or partly) of automated information processing systems, related non-automated processes and the interfaces between them.

Wat is (een) CISA

Verschil in perspectief tussen uitvoering en auditing

Uitvoering:

- gericht op (technische of vakinhoudelijke) kennis
- Wie, wat, hoe waarom, wanneer, etc.

Auditing:

- gericht op beheersing van risico's
- Hoe weet je zeker dat…. (guilty until proven innocent)

ControlSolutions International

Wat is (een) CISA

CISA betekent:

- Ervaring
- Erkenning:
- Betere loopbaanperspectieven en hogere verdiensten
- As evidenced by:

15 Top-Paying Certifications for 2017 (*Global Knowledge)*

1. **Certified in Risk and Information Systems Control (CRISC) - $131,298**
2. **Certified Information Security Manager (CISM) - $128,156**
3. **Certified Information Systems Auditor (CISA) - $125,091**
4. **Certified Information Systems Security Professional (CISSP) - $121,729**
5. **Project Management Professional (PMP®) - $119,349**

……

15. **Microsoft Certified Solutions Associate (MCSA) - $93,718**

Hoe word je CISA?

- Word lid van ISACA (www.isaca.org)
- Schaf studiematerialen aan en volg een cursus
- Slaag voor het examen
- Vraag de titel aan

ControlSolutions International

Lidmaatschap ISACA

Kosten:

- Basic membership dues: 135 USD
- Netherlands Chapter dues: 50 USD
- Transaction fee 30 USD (online 10 USD)

---

215 USD

Lidmaatschap ISACA

Baten:

- ISACA eLibrary—more than 425 third-party titles
- Free CPE—ISACA certified members can earn over 60 FREE CPEs per year.
- CISA, CISM, CGEIT and CRISC certification—Member discounts for exam study aids, registration and maintenance
- Conferences and Training—Member discounts on more than 25 ISACA events annually
- Webcasts and e-Symposia—Members obtain up to **3 free CPE hours monthly!**
- Local (Chapter-level) Education—Access to affordable CPE programs and information exchange through regular chapter meetings and events
- Bookstore —Member discounts on ISACA publications and research
- Downloads—Members-only research discounts or preferred access to COBIT 4.1, Risk IT: Based on COBIT, Val IT and many other publications from ITGI
- Knowledge Center—Exclusive access to one convenient online location where members can access professional knowledge. Network, learn and exchange ideas globally with peers through communities, shared interest groups, discussions and document sharing. Get a holistic view into all ISACA resources.
- Standards—Easy access to ISACA's IS Auditing Standards, Guidelines and Procedures

ControlSolutions International

Schaf studiematerialen aan en volg een cursus

➢ The Candidate's Guide to the CISA Exam	Gratis
➢ CISA Review Manual 2017	135/105 USD
➢ CISA Practice Question Database (download or CD)	225/185 USD
➢ CISA Review Questions, Answers & Explanations| Manual 2017	156/120 USD
➢ CISA Review Questions, Answers & Explanations Manual 2017 Supplement	65/45 USD

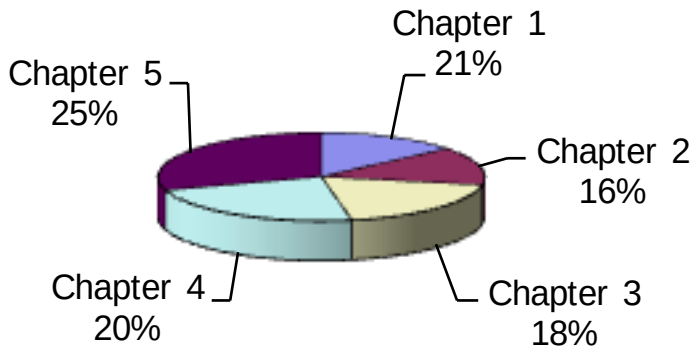
Volg een cursus!

The process of Auditing Information Systems

Ensure that the CISA candidate…

Has the knowledge necessary to provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems

The content area in this chapter will represent approximately 21% of the CISA examination (approximately 31 questions).

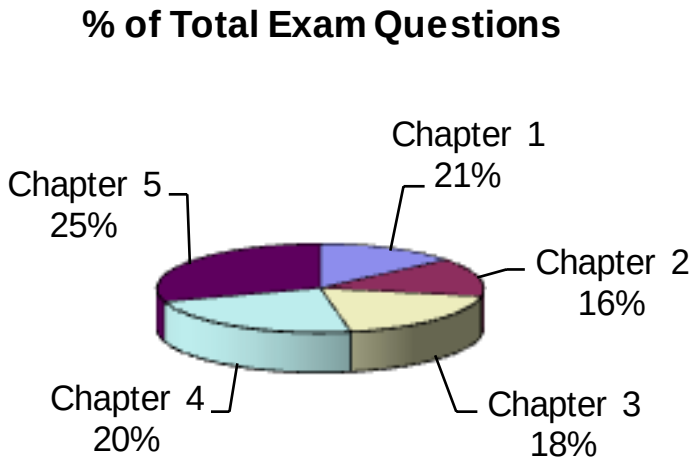


Governance and Management of IT

Ensure that the CISA candidate…

Understands and can provide assurance that the necessary leadership and organizational structures and processes are in place to achieve the objectives and to support the enterprise's strategy.

The content area in this chapter will represent approximately 16% of the CISA examination (approximately 24 questions).

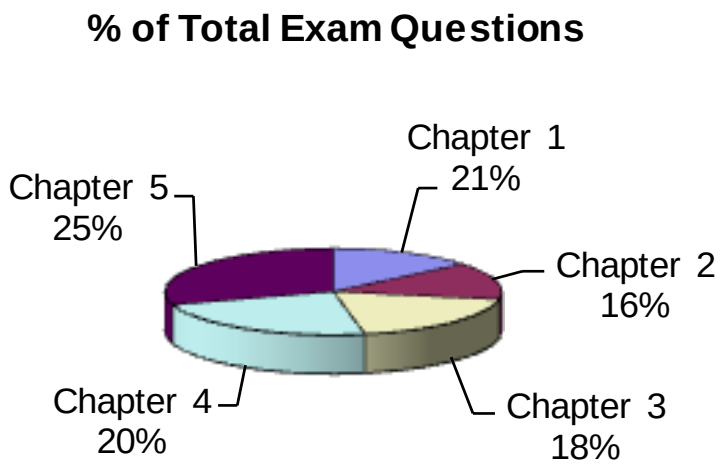


Information Systems Acquisition, Development and Implementation

Ensure that the CISA candidate…

Understands and can provide assurance that the practices for the acquisition, development, testing and implementation of information systems meet the enterprise's strategies and objectives.

The content area in this chapter will represent approximately 18% of the CISA examination (approximately 27 questions).

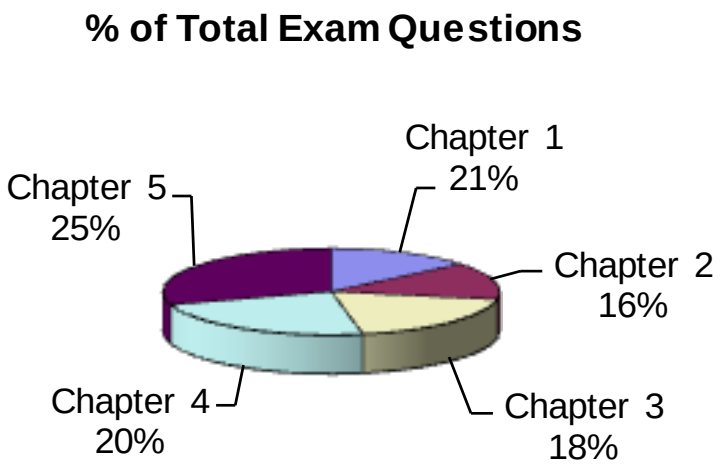


Information Systems Operations, Maintenance and Service Management

Ensure that the CISA candidate…

Understands and can provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives.

The content area in this chapter will represent approximately 20% of the CISA examination (approximately 30 questions).

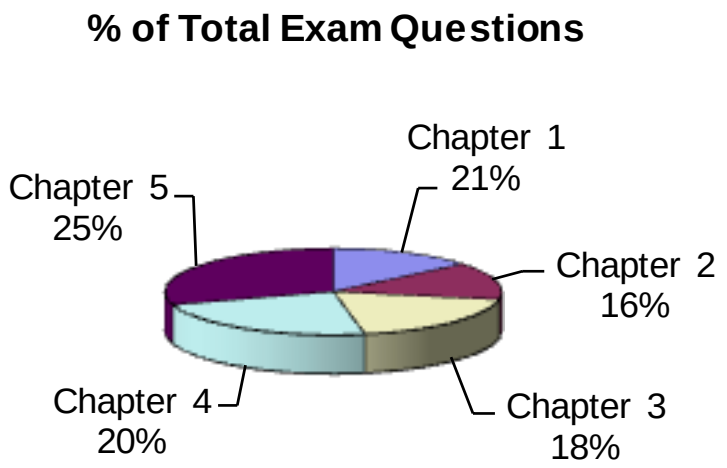


Protection of Information Assets

Ensure that the CISA candidate…

Understands and can provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

The content area in this chapter will represent approximately 25% of the CISA examination (approximately 38 questions).



Slaag voor het examen (1)

- 'ISACA Exam Candidate Information Guide' bevat nuttige registratie-informatie, studiehulpgegevens en informatie over hoe een ISACA-lidmaatschap je geld kan besparen.
- The guide is beschikbaar in het Engels en aantal andere talen (helaas niet meer in het Nederlands).

Examen registratie fee

- ISACA-leden USD 575
- Geen ISACA-leden USD 760
- Wijzigingen zonder extra kosten mogelijk uiterlijk 48 uur voor het examen
- Uitstellen van examen naar een andere periode mogelijk tegen betaling van USD 200.

Slaag voor het examen (2)

Examenperiodes 2017

- 1 mei t/m 30 juni 2017
- 1 augustus t/m 30 september 2017
- 1 november t/m 31 december 2017

Examen

- 150 meerkeuzevragen
- 4 uur
- Keuze uit meerdere locaties (zie www.isaca.org/examlocations)

ISACA Exam Candidate Information Guide bevat veel info

Vraag de titel aan

A minimum of 5 years of professional information systems auditing, control or security work experience is required for certification. Substitutions and waivers of such experience, to a maximum of 3 years, may be obtained as follows:

- A maximum of 1 year of information systems experience OR 1 year of non-IS auditing experience can be substituted for 1 year of experience.
- 60 to 120 completed university semester credit hours (the equivalent of an 2-year or 4-year degree) not limited by the 10-year preceding restriction, can be substituted for 1 or 2 years, respectively, of experience.
- A bachelor's or master's degree from a university that enforces the ISACA-sponsored Model Curricula can be substituted for 1 year of experience. A master's degree in information security or information technology from an accredited university can be substituted for 1 year of experience.

Houd de titel (1)

- Leden van ISACA en/of houders van CISA-certificaten gaan akkoord met ‘Code of Professional Ethics’ met betrekking tot persoonlijk en professioneel gedrag.

- De beroepscode ‘Code of Professional Ethics’ biedt richtlijnen voor het professionele en persoonlijke gedrag van leden van ISACA en/of houders van CISA en CISM-certificaten.

Code of Ethics

Leden en houders van ISACA-certificaten zullen:

1. De implementatie en naleving ondersteunen van de toepasselijke standaarden en procedures voor de effectieve beheersing en het beheer van informatiesystemen en technologie, met inbegrip van: audit, controle, veiligheid en risicobeheer.

2. Hun taken objectief, toegewijd en professioneel uitvoeren in lijn met de professionele standaarden.

3. Op een wettige wijze de belangen dienen van de belanghebbenden en tegelijk hoge standaarden qua gedrag en houding hanteren en zich niet inlaten met zaken die hun beroep of de Vereniging in diskrediet brengen.

4. De privacy en vertrouwelijkheid handhaven van gegevens die zijn verkregen tijdens de uitvoering van hun werkzaamheden, tenzij openbaarmaking door een juridische autoriteit wordt vereist. Dergelijke informatie zal niet voor persoonlijk gewin worden aangewend of worden doorgegeven aan niet relevante partijen.

5. Vakkennis en vaardigheden onderhouden in hun respectievelijke gebieden en ermee instemmen alleen die activiteiten te ondernemen die ze naar verwachting redelijkerwijs kunnen uitvoeren op basis van de nodige competenties, kennis en vaardigheden.

6. De relevante partijen op de hoogte brengen van de resultaten van het uitgevoerde werk, met inbegrip van de bekendmaking van alle significante feiten die hen bekend zijn en die, indien niet bekend gemaakt, de rapportering van de resultaten zouden kunnen vertekenen.

7. De professionele opleiding van belanghebbenden ondersteunen om hun begrip van de beheersing en het beheer van informatiesystemen en technologie te verbeteren, met inbegrip van: audit, controle, veiligheid en risicobeheer.

Houd de titel (2)

De doelstellingen voor de permanente educatie (CPE) zijn:

- De competentie van een CISA behouden door het updaten van bestaande kennis en vaardigheden op het gebied van audits, control of informatiebeveiliging,
- Een middel bieden om onderscheid te maken tussen gekwalificeerde CISA's en degenen die niet hebben voldaan aan de eisen voor voortzetting van hun certificering,
- Een mechanisme bieden voor het toezicht op de information systems audits, controle en security ‘onderhoud van competenties van auditors’,
- Het topmanagement ondersteunen bij het ontwikkelen van audit, controle- en security-functies door criteria te geven voor de selectie en ontwikkeling van personeel,
- Onderhoudskosten en een minimum van 20 CPE punten zijn jaarlijks vereist. Daarnaast is een minimum van 120 CPE punten vereist gedurende een vaste periode van 3 jaar.

Houd de titel (3)

Professionals met CISA-certificaten stemmen ermee in zich te houden aan de standaarden van ISACA voor ‘Information Systems Auditing’.

ControlSolutions International

Standaards

General	Performance	Reporting
1001 Audit Charter	1201 Engagement Planning	1401 Reporting
1002 Organizational Independence	1202 Risk Assessment in Planning	1402 Follow-up Activities
1003 Professional Independence	1203 Performance and Supervision	
1004 Reasonable Expectation	1204 Materiality	
1005 Due Professional Care	1205 Evidence	
1006 Proficiency	1206 Using the Work of Other Experts	
1007 Assertions	1207 Irregularity and Illegal Acts	
1008 Criteria		

ControlSolutions International

Oefenvragen

ControlSolutions International

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be **PRIMARILY** responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor

B. Database administrator

C. Project manager

D. Data owner

ControlSolutions International

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be **PRIMARILY** responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor

B. Database administrator

C. Project manager

D. Data owner

During a compliance audit of a small bank, the IS auditor notes that both the IT and accounting functions are being performed by the same user of the financial system. Which of the following reviews conducted by the user's supervisor would represent the **BEST** compensating control?

A. Audit trails that show the date and time of the transaction.

B. A daily report with the total numbers and dollar amounts of each transaction.

C. User account administration.

D. Computer log files that show individual transactions.

During a compliance audit of a small bank, the IS auditor notes that both the IT and accounting functions are being performed by the same user of the financial system. Which of the following reviews conducted by the user's supervisor would represent the **BEST** compensating control?

A. Audit trails that show the date and time of the transaction.

B. A daily report with the total numbers and dollar amounts of each transaction.

C. User account administration.

D. Computer log files that show individual transactions.

An IS auditor discovers that the chief information officer (CIO) of an organization is using a wireless broadband modem utilizing global system for mobile communications (GSM) technology. This modem is being used to connect the CIO's laptop to the corporate virtual private network (VPN) when the CIO travels outside of the office. The IS auditor should:

A. do nothing because the inherent security features of GSM technology are appropriate.

B. recommend that the CIO stop using the laptop computer until encryption is enabled.

C. ensure that media access control (MAC) address filtering is enabled on the network so unauthorized wireless users cannot connect.

D. suggest that two-factor authentication be used over the wireless link to prevent unauthorized communications.

ControlSolutions International

An IS auditor discovers that the chief information officer (CIO) of an organization is using a wireless broadband modem utilizing global system for mobile communications (GSM) technology. This modem is being used to connect the CIO's laptop to the corporate virtual private network (VPN) when the CIO travels outside of the office. The IS auditor should:

A. do nothing because the inherent security features of GSM technology are appropriate.

B. recommend that the CIO stop using the laptop computer until encryption is enabled.

C. ensure that media access control (MAC) address filtering is enabled on the network so unauthorized wireless users cannot connect.

D. suggest that two-factor authentication be used over the wireless link to prevent unauthorized communications.

An IS auditor discovers that some hard drives disposed of by an enterprise were not sanitized in a manner that would reasonably ensure the data could not be recovered. In addition, the enterprise does not have a written policy on data disposal. The IS auditor should **FIRST**:

A. draft an audit finding, and discuss it with the auditor in charge.

B. determine the sensitivity of the information on the hard drives.

C. discuss with the IT manager the best practice in data disposal.

D. develop an appropriate data disposal policy for the enterprise.

An IS auditor discovers that some hard drives disposed of by an enterprise were not sanitized in a manner that would reasonably ensure the data could not be recovered. In addition, the enterprise does not have a written policy on data disposal. The IS auditor should **FIRST**:

A. draft an audit finding, and discuss it with the auditor in charge.

B. determine the sensitivity of the information on the hard drives.

C. discuss with the IT manager the best practice in data disposal.

D. develop an appropriate data disposal policy for the enterprise.

Which of the following is the **MOST** important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

A. meets or exceeds industry security standards.

B. agrees to be subject to external security reviews.

C. has a good market reputation for service and experience.

D. complies with security policies of the organization.

ControlSolutions International

Which of the following is the **MOST** important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

A. meets or exceeds industry security standards.

B. agrees to be subject to external security reviews.

C. has a good market reputation for service and experience.

D. complies with security policies of the organization.

After reviewing its business processes, a large organization is deploying a new web application based on a Voice-over IP (VoIP) technology. Which of the following is the **MOST** appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

A. Fine-grained access control

B. Role-based access control (RBAC)

C. Access control lists

D. Network/service access control

After reviewing its business processes, a large organization is deploying a new web application based on a Voice-over IP (VoIP) technology. Which of the following is the **MOST** appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

A. Fine-grained access control

B. Role-based access control (RBAC)

C. Access control lists

D. Network/service access control

ControlSolutions International

An IS auditor is testing employee access to a large financial system. The IS auditor selected a sample from the current employee list provided by the auditee. Which of the following evidence is the MOST reliable to support the testing?

A. A spreadsheet provided by the system administrator
B. Human resources (HR) documents signed by employees' managers
C. A list of accounts with access levels generated by the system
D. Observations performed onsite in the presence of a system administrator

An IS auditor is testing employee access to a large financial system. The IS auditor selected a sample from the current employee list provided by the auditee. Which of the following evidence is the MOST reliable to support the testing?

A. A spreadsheet provided by the system administrator
B. Human resources (HR) documents signed by employees' managers
C. A list of accounts with access levels generated by the system
D. Observations performed onsite in the presence of a system administrator

ControlSolutions International

An IT steering committee should review information systems **PRIMARILY** to assess:

A. Whether IT processes support business requirements
B. Whether proposed system functionality is adequate
C. The stability of existing software
D. The complexity of installed technology

ControlSolutions International

An IT steering committee should review information systems **PRIMARILY** to assess:

A. Whether IT processes support business requirements
B. Whether proposed system functionality is adequate
C. The stability of existing software
D. The complexity of installed technology

ControlSolutions International

Which of the following goals would you expect to find in an organization's strategic plan?

A. Test a new accounting package
B. Perform an evaluation of information technology needs
C. Implement a new project planning system within the next 12 months
D. Become the supplier of choice for the product offered

Which of the following goals would you expect to find in an organization's strategic plan?

A. Test a new accounting package
B. Perform an evaluation of information technology needs
C. Implement a new project planning system within the next 12 months
D. Become the supplier of choice for the product offered

ControlSolutions International

When implementing an application software package, which of the following presents the GREATEST risk?

A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. Incorrectly set parameters
D. Programming errors

ControlSolutions International

When implementing an application software package, which of the following presents the GREATEST risk?

A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. Incorrectly set parameters
D. Programming errors

ControlSolutions International

An organization has implemented an online customer helpdesk application using a Software as a Service (SaaS) operating model. An IS auditor is asked to recommend the best control to monitor the service level agreement (SLA) with the SaaS vendor as it relates to availability. What is the **BEST** recommendation that the IS auditor can provide?

A. Ask the SaaS vendor to provide a weekly report on application uptime
B. Implement an online polling tool to monitor the application and record outages
C. Log all application outages reported by users and aggregate the outage time weekly
D. Contract an independent third party to provide weekly reports on application uptime

ControlSolutions International

An organization has implemented an online customer helpdesk application using a Software as a Service (SaaS) operating model. An IS auditor is asked to recommend the best control to monitor the service level agreement (SLA) with the SaaS vendor as it relates to availability. What is the **BEST** recommendation that the IS auditor can provide?

A. Ask the SaaS vendor to provide a weekly report on application uptime
B. Implement an online polling tool to monitor the application and record outages
C. Log all application outages reported by users and aggregate the outage time weekly
D. Contract an independent third party to provide weekly reports on application uptime

ControlSolutions International

When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

A. Passwords are not shared
B. Transmission of unencrypted passwords
C. Redundant logon IDs are deleted
D. The allocation of logon IDs is controlled

ControlSolutions International

When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

A. Passwords are not shared
B. Transmission of unencrypted passwords
C. Redundant logon IDs are deleted
D. The allocation of logon IDs is controlled