



# CERTIFIED INFORMATION SYSTEMS AUDITOR<sup>®</sup>

2012 Kandidatengids voor  
CISA<sup>®</sup>-examen en -certificering

# Kandidatengids voor CISA®-examen en -certificering

## CISA-examens 2012— Belangrijke datuminformatie

### Examendatum—9 juni 2012

Deadline vroege inschrijving: 8 februari 2012

Deadline laatste inschrijving: 4 april 2012

Wijzigingen in exameninschrijvingen: Tussen 14 april en 20 april bedragen de kosten \$50; na 20 april 2012 worden geen wijzigingen meer geaccepteerd

Terugbetaling: Tot 13 april 2012 worden verwerkingskosten van \$100 in rekening gebracht; na die datum vindt geen terugbetaling meer plaats

Opschorting: Voor verzoeken om opschorting die worden ontvangen op of vóór 20 april 2012, worden verwerkingskosten van \$50 in rekening gebracht. Voor verzoeken die worden ontvangen vanaf 21 april tot en met 24 mei 2012, worden verwerkingskosten van \$100 in rekening gebracht. Na 24 mei 2012 zijn geen opschortingen meer toegestaan.

### Examendatum—8 december 2012

Deadline vroege inschrijving: 15 augustus 2012

Deadline laatste inschrijving: 3 oktober 2012

Wijzigingen in exameninschrijvingen: Tussen 6 oktober en 12 oktober, tegen de kosten van \$50; na 12 oktober 2012 worden geen wijzigingen meer geaccepteerd

Terugbetaling: Tot 5 oktober 2012 worden verwerkingskosten van \$100 in rekening gebracht; na die datum vindt geen terugbetaling meer plaats

Opschorting: Voor verzoeken om opschorting die worden ontvangen op of vóór 12 oktober 2012, worden verwerkingskosten van \$50 in rekening gebracht. Voor verzoeken die worden ontvangen vanaf 13 oktober tot en met 21 november 2012, worden verwerkingskosten van \$100 in rekening gebracht. Na 21 november 2012 zijn geen opschortingen meer toegestaan.

Alle deadlines zijn gebaseerd op Chicago, Illinois, VS, 5 p.m. CT (Central Time).

2012 Kandidatengids voor CISA®-examen en -certificering  
Gedrukt in de Verenigde Staten.

## Inhoudsopgave

Overzicht.....	3
Registratie van CISA-programma vernieuwd onder ISO/IEC 17024:2003 .....	3
Het CISA-examen.....	3
Vorbereiden op het CISA-examen.....	3
Organisatie van het CISA-examen.....	4
Het CISA-examen beoordelen .....	6
Typen vragen in het CISA-examen .....	6
CISA-certificering aanvragen.....	6
Vereisten voor een eerste CISA-certificering .....	7
Vereisten voor het behouden van de CISA-certificering .....	7
Professionele gedragscode van ISACA.....	7
Intrekken van CISA-certificering .....	7
Taak- en kennisverklaringen van CISA .....	8

### Omtrent ISACA®

Met 95.000 leden in 160 landen is ISACA ([www.isaca.org](http://www.isaca.org)) wereldwijd een leider op het gebied van kennis, certificeringen, gemeenschap, bevordering en opleiding betreffende assurance en beveiliging van informatiesystemen (IS), Enterprise Governance en beheer van IT en met IT verbonden risico's en naleving. ISACA is in 1969 opgericht als onafhankelijke organisatie zonder winstoogmerk en organiseert internationale conferenties, publiceert het *ISACA® Journal* en ontwikkelt internationale audit- en controlestandaarden voor informatiesystemen dankzij welke haar leden deze systemen kunnen vertrouwen en er toegevoegde waarde uit kunnen halen. ISACA promoot en certificeert tevens IT-vaardigheden en kennis met behulp van de wereldwijd gerespecteerde CISA®-erkenning (Certified Information Systems Auditor®), CISM®-erkenning (Certified Information Security Manager®), CGEIT®-erkenning (Certified in the Governance of Enterprise IT®) en CRISC™-erkenning (Certified in Risk and Information Systems Control™). ISACA werkt doorlopend COBIT® bij, waarmee IT-professionals en leiders binnen grote ondernemingen kunnen voldoen aan hun verantwoordelijkheden met betrekking tot IT-governance en -beheer, in het bijzonder op het gebied van assurance, beveiliging, risico's en controle, en waarde kunnen leveren aan hun onderneming.

### Disclaimer

ISACA en het CISA Certification Committee (certificeringscommissie) hebben de *2012 Kandidatengids voor CISA-examen en -certificering* opgesteld als een leidraad voor de mensen die streven naar de CISA-certificering. ISACA geeft geen garantie dat kandidaten door deze of andere uitgaven of cursussen van de vereniging te gebruiken zullen slagen voor het CISA-examen.

### Voorbehoud van rechten

Copyright © 2011 ISACA. Reproductie of opslag in enige vorm voor enig doel is niet toegestaan zonder voorafgaande schriftelijke toestemming van ISACA. Er wordt geen enkel ander recht of toestemming verleend met betrekking tot dit werk. Alle rechten voorbehouden.

### ISACA

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008, Verenigde Staten  
Telefoon: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [exam@isaca.org](mailto:exam@isaca.org)  
Website: [www.isaca.org](http://www.isaca.org)

# Kandidatengids voor CISA®-examen en -certificering

## Overzicht

De toetssteen voor een professioneel certificeringsprogramma is de waarde en erkenning die aan de persoon worden toegekend die deze certificering haalt. Sinds 1978 is het door ISACA ondersteunde CISA-programma (Certified Information Systems Auditor) wereldwijd de geaccepteerde prestatienorm voor IT-specialisten op het gebied van audit, controle en beveiliging.

De technische vaardigheden, kennis en werkwijzen die CISA aanbeveelt en evalueert, vormen de basis voor succes in de praktijk. Het hebben van de CISA-erkenning toont vakkundigheid en is normstellend voor het vakgebied. Met een groeiende vraag naar professionals die beschikken over IT-vaardigheden op het gebied van audit, controle en beveiliging, wordt CISA over de hele wereld gewaardeerd door personen en organisaties. CISA-certificering staat voor streven naar perfectie bij het bedienen van een organisatie en de beroepsuitoefening.

## Registratie van CISA-programma vernieuwd onder ISO/IEC 17024:2003

Het American National Standards Institute (ANSI) heeft de CISA-certificering geregistreerd onder ISO/IEC 17024:2003, algemene vereisten voor instellingen die certificeringssystemen voor personen hanteren. ANSI, een particuliere organisatie zonder winstoogmerk, registreert andere organisaties om als certificeerders van derden, systemen en personeel te fungeren.

ISO/IEC 17024 specificeert de vereisten waaraan moet worden voldaan door organisaties die personen volgens specifieke eisen certificeren. ANSI beschrijft ISO/IEC 17024 als “zal naar verwachting een prominente rol spelen in het bevorderen van wereldwijde standaardisatie van de certificeringsgemeenschap, in het verbeteren van de uitwisselbaarheid tussen landen en in het vergroten van de openbare veiligheid en het beschermen van consumenten”.

Registratie van ANSI:

- Bevordert de unieke kwalificaties en expertise waarin de certificeringen van ISACA voorzien
- Beschermde de integriteit van de certificeringen op een juridische grondslag
- Versterkt het vertrouwen van de consument en de maatschappij in de certificeringen en de mensen die zijn gecertificeerd
- Bevordert mobiliteit over grenzen of bedrijfstakken

Registratie door ANSI houdt in dat de procedures van ISACA voldoen aan de essentiële ANSI-vereisten voor openheid, evenwichtigheid, en consensus over normen en voorschriften. Door deze registratie anticipeert ISACA op het gegeven dat zich belangrijke kansen voor CISA's blijven voordoen in de hele wereld.

## Het CISA-examen

### Ontwikkeling/beschrijving van het CISA-examen

De CISA-certificeringscommissie houdt toezicht op de ontwikkeling van het examen en zorgt ervoor dat de inhoud actueel blijft. Vragen voor het CISA-examen worden ontwikkeld via een uitgebreid proces dat is ontworpen om de uiteindelijke kwaliteit van het examen te verbeteren. Zo werkt een commissie ter verbetering van toetsen (Test Enhancement Subcommittee) samen met schrijvers van artikelen om vragen te ontwikkelen en evalueren voordat deze ter controle bij de CISA-certificeringscommissie worden ingediend.

Een praktijkgebied dient als de basis voor het examen en de ervaringsvereisten om de CISA-certificering te halen. Dit praktijkgebied wordt regelmatig bijgewerkt en bestaat uit vijf inhoudsgebieden (domeinen). De domeinen en de bijbehorende taak- en kennisverklaringen zijn het resultaat van uitgebreid onderzoek en de feedback van deskundigen in deze onderwerpen uit de hele wereld.

De taak- en functieomschrijving beschrijft de door CISA's uitgevoerde taken en de kennis die nodig is om deze taken uit te voeren. Examenkandidaten worden getest op basis van hun praktische kennis gekoppeld aan het uitvoeren van deze taken.

De bijgewerkte praktijkanalyse bevat de volgende domeinen en percentages:

- **Het auditproces voor informatiesystemen (14%)**
- **IT-governance en -management (14%)**
- **Acquisitie, ontwikkeling en implementatie van informatiesystemen (19%)**
- **Operaties, onderhoud en ondersteuning van informatiesystemen (23%)**
- **Bescherming van informatiemiddelen (30%)**

**Opmerking:** De bij de domeinen weergegeven percentages geven het belang aan van de vragen die in het examen voor elk domein zullen worden gesteld. Raadpleeg pagina 8 tot en met 11 voor een beschrijving van de taak- en kennisverklaringen van elk domein.

Het examen bestaat uit 200 meerkeuzevragen en wordt twee keer per jaar, in juni en december, afgenomen. Het examen duurt vier uur. Kandidaten kunnen ervoor kiezen het examen in een van de aangeboden talen af te leggen. Ga naar [www.isaca.org/cisaterminology](http://www.isaca.org/cisaterminology) voor een actuele lijst met talen.

## Vorbereiden op het CISA -examen

Via een georganiseerd studieplan kan men voor het CISA-examen slagen. Om mensen te helpen met de ontwikkeling van een succesvol studieplan biedt ISACA verscheidene studiehulpmiddelen en evaluatiecursussen aan examenkandidaten aan. Zie [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide) om de ISACA -studiehulpmiddelen te bekijken die u bij de voorbereiding van het examen kunnen helpen. Bestel deze op tijd aangezien de levertijd één tot vier weken in beslag neemt, afhankelijk van geografische locatie en inklaringspraktijken van de douane. Zie [www.isaca.org/shipping](http://www.isaca.org/shipping) voor actuele informatie over verzendingen.



Geregistreerd ANSI-programma  
PERONEELSCERTIFICERING  
#0694  
ISO/IEC 17024

# Kandidatengids voor CISA®-examen en -certificering



ISACA biedt ook een CISA® Online Review Course (online evaluatiecursus) aan. De cursus bevat interactieve oefeningen, casestudies, evaluatiehulpmiddelen en praktijkvragen. Ga naar [www.isaca.org/elearning](http://www.isaca.org/elearning) voor meer informatie en om een cursusvoorbeeld te bekijken.

Een uitgebreide lijst van referenties aanbevolen voor het studeren vindt u in de *CISA Review Manual 2012*.

Op [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide) staat een lijst met acroniemen die kandidaten moeten kennen en een aanvullende lijst met acroniemen die kandidaten wellicht willen bekijken.

Als hulpmiddel bij technische terminologie is er voor de kandidaten een lijst met de meest voorkomende technische termen in het Engels met bijbehorende vertaling in andere talen beschikbaar op de ISACA-website op [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide).

ISACA onderhoudt een verklarende woordenlijst met termen, evenals woordenlijsten die specifiek voor elke certificering gelden. Deze woordenlijsten zijn beschikbaar op [www.isaca.org/glossary](http://www.isaca.org/glossary).

*ISACA of de CISA-certificeringscommissie geeft geen garantie dat kandidaten door deze of andere uitgaven of cursussen van de vereniging te gebruiken, zullen slagen.*

## Organisatie van het CISA-examen

ISACA maakt gebruik van een internationaal erkend professioneel examenbureau dat helpt bij het samenstellen, de organisatie en de beoordeling van het CISA-examen.

Kandidaten die opmerkingen willen maken over de voorwaarden van de toetsadministratie, kunnen dat na het voltooien van het examen doen door de "Vragenlijst toetsadministratie" in te vullen. De Vragenlijst toetsadministratie staat achterop het examenformulier. Uw antwoorden moeten in vakken P tot en met S van het deel Speciale codes (raster nr. 4) voorop uw antwoordvel worden ingevuld.

Kandidaten die aanvullende opmerkingen willen maken over de examenadministratie, met inbegrip van de omstandigheden op de examenlocatie of de inhoud van het examen, kunnen per brief of e-mail ([exam@isaca.org](mailto:exam@isaca.org)) contact opnemen met het internationale hoofdkantoor van ISACA. Deze opmerkingen moeten binnen 2 weken na de examendatum door ISACA zijn ontvangen. Gelieve aan uw opmerkingen de volgende informatie toe te voegen: het ID-nummer van het examen, de examensite, de examendatum en eventuele relevante details over uw specifieke kwestie. Bij de uiteindelijke beoordeling van het examen wordt alleen rekening gehouden met de opmerkingen die in de eerste twee weken na het examen door ISACA zijn ontvangen.

### Toelatingsbewijs

Ongeveer twee tot drie weken vóór de CISA-examendatum stuurt ISACA kandidaten een fysiek toelatingsbewijs of een e-ticket toe. Examenkandidaten kunnen ook een exemplaar van het toelatingsbewijs downloaden op de pagina [www.isaca.org](http://www.isaca.org) > MyISACA van de website. Op het toelatingsbewijs staan de datum, de inschrijftijd en de locatie van het examen, evenals het programma voor die dag en een lijst met materialen die kandidaten moeten meebrengen voor het afleggen van het CISA-examen. Behalve bij wijzigingen in hun contactinformatie, is het kandidaten niet toegestaan op het toelatingsbewijs te schrijven.

**Let op:** Om een toegangsbewijs te ontvangen, moeten alle kosten zijn betaald. Toelatingsbewijzen worden per post of via e-mail verzonden naar het actuele post- of e-mailadres dat werd opgegeven. Alleen kandidaten met een toelatingsbewijs en een geldig, door een overheidsdienst uitgegeven identiteitsbewijs wordt toegestaan het examen af te leggen. De naam op het toelatingsbewijs moet identiek zijn aan de naam op het officiële identiteitsbewijs. Het papieren toelatingsbewijs of de afdruk van het e-ticket zijn geldig om tot het examen te worden toegelaten. Kandidaten van wie het post- en/of e-mailadres verandert, moeten hun profiel op de ISACA-website ([www.isaca.org](http://www.isaca.org)) wijzigen of contact opnemen met [exam@isaca.org](mailto:exam@isaca.org).

**Kandidaten moeten goede notie nemen van de specifieke inschrijvings- en examentijd op hun toelatingsbewijs. ZODRA DE HOOFDEXAMINATOR DE MONDELINGE INSTRUCTIES BEGINT VOOR TE LEZEN, ONGEVEER DERTIG MINUTEN VOORDAT HET EXAMEN BEGINT, WORDT GEEN ENKELE KANDIDAAT MEER TOEGELATEN TOT DE EXAMENRUIMTE.** Kandidaten die arriveren nadat de mondelinge instructies zijn begonnen, worden niet tot het examen toegelaten en verbeuren hun inschrijfgeld. Een toelatingsbewijs kan alleen worden gebruikt in het aangewezen examencentrum dat op het toelatingsbewijs is aangegeven. Identiteitsbewijzen zullen tijdens het examen worden gecontroleerd.

### Speciale voorzieningen

ISACA zal op verzoek redelijke aanpassingen in de examenprocedures aanbrengen voor kandidaten met aantoonbare handicaps of religieuze behoeften. Deze kandidaten kunnen verzoeken om redelijke wijzigingen in overweging te nemen voor wat betreft de examenopzet, de presentaties, eten en drinken op de plaats waar het examen wordt afgenomen of de planning. Verzoeken om eten en drinken op de plaats waar het examen wordt afgenomen moeten worden vergezeld van een doktersattest. Anders **wordt er geen eten en drinken op de plaats van het examen toegestaan**. Verzoeken om dergelijke wijzigingen in overweging te nemen moeten uiterlijk op 4 april 2012 voor het examen van juni 2012 en op 3 oktober 2012 voor het examen van december 2012 schriftelijk en vergezeld van de juiste documenten bij het internationale hoofdkantoor van ISACA worden ingediend.

### Op tijd zijn

Registratie begint op de aangegeven tijd op het toelatingsbewijs in elk centrum. Alle kandidaten moeten zijn geregistreerd en in de examenruimte aanwezig zijn wanneer de hoofdexaminator begint met het voorlezen van de mondelinge instructies. **ZODRA DE HOOFDEXAMINATOR DE MONDELINGE INSTRUCTIES BEGINT VOOR TE LEZEN, ONGEVEER DERTIG MINUTEN VOORDAT HET EXAMEN BEGINT, WORDT GEEN ENKELE KANDIDAAT MEER TOEGELATEN TOT DE EXAMENRUIMTE.**

# Kandidatengids voor CISA®-examen en -certificering

## Het toelatingsbewijs niet vergeten mee te brengen

Kandidaten kunnen hun toelatingsbewijs (een e-ticket of een papieren toelatingsbewijs) alleen in de toegewezen examenruimte gebruiken. Kandidaten worden alleen in de examenruimte toegelaten indien zij een geldig toelatingsbewijs hebben en een geldig identiteitsbewijs (id). Een geldig identiteitsbewijs moet een recent door de overheid uitgegeven identiteitsbewijs zijn waarop de naam van de kandidaat staat vermeld, zoals deze ook op het toelatingsbewijs staat, en de foto van de kandidaat. De informatie op het id mag niet met de hand geschreven zijn. De naam en de foto moeten op hetzelfde identiteitsbewijs staan. Voorbeelden hiervan zijn onder andere een paspoort, een rijbewijs, militaire identificatie, of een identiteitskaart. Een kandidaat die geen geldig identiteitsbewijs kan overleggen, wordt niet tot het examen toegelaten en verspeelt zijn/haar inschrijfgeld.

## De regels van het examencentrum in acht nemen

- Kandidaten worden niet tot de examenruimte toegelaten nadat de mondelinge instructies zijn begonnen.
- Kandidaten moeten meerdere geslepen potloden van nr. 2 of HB (zacht) en een goede gum meebrengen. Potloden en gummen zijn niet in de examenruimte verkrijgbaar. Het examen wordt op verschillende locaties afgenomen en er wordt getracht op elke examenlocatie voor een goede klimaatbeheersing te zorgen. Kandidaten mogen dragen waar ze zich prettig bij voelen.
- Kandidaten mogen geen naslagmateriaal, blanco papier, notitieblokken of woordenboeken meebrengen naar de examenruimte.
- Kandidaten mogen geen rekenmachine gebruiken of meebrengen naar de examenruimte.
- Kandidaten mogen geen enkel communicatieapparaat (dat wil zeggen: mobiele telefoon, PDA, Blackberry® enzovoort) meebrengen naar de examenruimte.  
**Als examenkandidaten tijdens het examen met een dergelijk apparaat worden gezien, zal hun examen ongeldig worden verklaard en zullen zij worden verzocht de examensite onmiddellijk te verlaten.**
- In de examenruimte zijn geen bezoekers toegestaan.
- Etenswaars en dranken zijn niet toegelaten in de examenruimte (zonder voorafgaande toestemming van ISACA).

## Ongeoorloofd gedrag

Kandidaten die worden betrapt op enigerlei vorm van ongeoorloofd gedrag—zoals het geven of krijgen van hulp; het gebruik van notities, papiertjes of andere hulpmiddelen; het proberen het examen voor iemand anders af te leggen; het gebruik van enigerlei vorm van communicatieapparatuur, inclusief mobiele telefoons, tijdens het examen; of het meenemen van het examenboekje, antwoordblad of notities uit de examenruimte—zullen worden gediskwalificeerd en kunnen gerechtelijk worden vervolgd. Kandidaten die de examenruimte zonder de toestemming van of niet in het gezelschap van een toezichthouder verlaten, zullen niet naar de examenruimte mogen terugkeren en worden gediskwalificeerd. Het examenbureau zal de CISA-certificeringscommissie van ISACA van zulke onregelmatigheden op de hoogte brengen.

Het beleid ten aanzien van persoonlijke bezittingen vindt u op [www.isaca.org/cisabelongings](http://www.isaca.org/cisabelongings). Noch ISACA noch diens examenorganisator kunnen verantwoordelijk worden gehouden voor de persoonlijke bezittingen van kandidaten.

## Het antwoordblad zorgvuldig invullen

- Voordat een kandidaat met het examen begint, leest de hoofdexaminator van de examenruimte de instructies voor het invoeren van de identificatiegegevens op het antwoordblad hardop voor. Het identificatienummer van een kandidaat zoals het op het toelatingsbewijs en alle andere aangevraagde informatie wordt weergegeven, moet correct worden ingevoerd. Als dat niet gebeurt, kunnen scores worden vertraagd of onjuist worden weergegeven.
- Er is een toezichthouder aanwezig die de voertaal van de kandidaten van de examenruimte spreekt. Als een kandidaat het examen in een andere taal dan het Nederlands voertaal wil afleggen, is het mogelijk dat de toezichthouder de gekozen taal niet spreekt. Schriftelijke instructies zijn echter wel in de taal van het examen beschikbaar.
- Een kandidaat wordt geïnstrueerd om zorgvuldig alle instructies door te lezen voordat hij of zij de vragen probeert te beantwoorden. Kandidaten die de aanwijzingen overslaan of te snel lezen, kunnen belangrijke informatie missen en mogelijk punten verliezen.
- Alle antwoorden worden in de desbetreffende cirkel op het antwoordblad gemarkeerd. Kandidaten moeten opletten dat ze niet meer dan één antwoord per vraag invullen en controleren dat ze een vraag in de juiste antwoordenrij beantwoorden. Als een kandidaat een antwoord wil veranderen, moet hij of zij het verkeerde antwoord helemaal uitgummen alvorens het nieuwe antwoord in te vullen.
- Alle vragen moeten worden beantwoord. **Er worden geen strafpunten gegeven voor onjuiste antwoorden. Cijfers worden uitsluitend gebaseerd op het aantal juist beantwoorde vragen. Laat dus geen vragen open.**
- Na afloop moeten kandidaten hun antwoordblad en examenboekje inleveren.

## Tijd goed indelen

- Het examen duurt vier uur. Per vraag heeft een kandidaat iets meer dan één minuut de tijd. Kandidaten wordt aangeraden snel te werken zodat ze het hele examen af krijgen. Kandidaten moeten gemiddeld vijftig vragen per uur invullen.
- Kandidaten worden verzocht hun antwoorden onmiddellijk op het antwoordblad aan te kruisen. **Na het verstrijken van de examentijd is er geen extra tijd toegestaan om antwoorden over of op te schrijven, mocht een kandidaat antwoorden in het examenboekje hebben aangegeven.**

## Gewenst gedrag

- Om de integriteit van het examen te waarborgen en de geldigheid van de scores te bevestigen, wordt kandidaten gevraagd het antwoordblad te ondertekenen.
- De CISA-certificeringscommissie behoudt zich het recht voor een kandidaat te diskwalificeren die wordt betrapt op enigerlei vorm van ongeoorloofd gedrag of inbreuk op het examenreglement, zoals het geven of krijgen van hulp; het gebruik van notities, papiertjes of andere hulpmiddelen; het proberen het examen voor iemand anders af te leggen; of het meenemen van examenmaterialen of notities uit de examenruimte. Het examenbureau zal de CISA-certificeringscommissie gegevens verschaffen betreffende dergelijke onregelmatigheden. De commissie zal dan één en ander evalueren en een beslissing nemen.

# Kandidatengids voor CISA®-examen en -certificering

## Redenen voor uitsluiting of diskwalificatie

De toezichthouder kan een kandidaat om één van de volgende redenen weigeren:

- Onbevoegde toelating tot het examen centrum.
- Kandidaat toont verstoring gedrag of geeft of krijgt hulp.
- Kandidaat probeert examenmaterialen of notities uit de examenruimte mee te nemen.
- Kandidaat doet zich voor als een andere kandidaat
- Kandidaat brengt niet-toegestane artikelen binnen de examenruimte.
- Kandidaat heeft tijdens het examen een communicatieapparaat (bv. mobiele telefoon, PDA, BlackBerry®) bij zich
- Kandidaat verlaat de testruimte zonder toestemming.

**Als kandidaten tijdens het examen worden gezien met een communicatieapparaat (bv. mobiele telefoon, PDA, BlackBerry®), zal hun examen ongeldig worden verklaard en zullen zij worden verzocht de examensite onmiddellijk te verlaten.**

## Het CISA-examen beoordelen

Het CISA-examen bestaat uit 200 meerkeuzevragen. De scores van kandidaten worden als een schaalscore doorgegeven. Een schaalscore is een conversie van de ruwe score van een kandidaat op een examen naar een standaardschaal. ISACA gebruikt en rapporteert scores op een standaardschaal van 200 tot 800. De schaalscore van 800 vertegenwoordigt bijvoorbeeld een perfecte score waarbij alle vragen juist zijn beantwoord. Een schaalscore van 200 is de laagst mogelijk score en geeft aan dat slechts een klein aantal vragen juist is beantwoord. Een kandidaat moet een score van 450 of hoger hebben om de slagen voor het examen. Een score van 450 vertegenwoordigt een minimaal consistente standaard van kennis zoals dit door de CISA-certificeringscommissie is vastgesteld. Een kandidaat met een hogere score dan 450 kan vervolgens certificering aanvragen indien aan alle andere vereisten is voldaan.

Het CISA-examen bevat enkele vragen die alleen zijn opgenomen voor onderzoeks- en analysedoeleinden. Deze vragen worden niet apart aangegeven en worden niet gebruikt om uw definitieve score te berekenen.

**Ongeveer acht weken na de examendatum worden de officiële examenuitslagen per post aan de kandidaten verstuurd.** Bovendien wordt, als de kandidaat hiervoor tijdens de inschrijving toestemming heeft gegeven, aan de kandidaat een e-mailbericht gestuurd waarin wordt aangegeven of de kandidaat is geslaagd of gezakt en waarin zijn/haar score wordt vermeld. Dit e-mailbericht wordt alleen verstuurd naar het adres dat staat vermeld in het profiel van de kandidaat op het moment dat de uitslagen voor het eerst worden vrijgegeven. Om ervoor te zorgen dat scores vertrouwelijk blijven, worden examenuitslagen niet per telefoon of fax doorgegeven. Om te voorkomen dat e-mailberichten in spammappen terechtkomen, moeten kandidaten *exam@isaca.org* toevoegen aan hun adresboek, 'whitelist' of lijst met veilige afzenders.

Kandidaten krijgen een uitslag die een subscore voor elk domein bevat. Kandidaten die zijn geslaagd, krijgen samen met de uitslag informatie over het aanvragen van CISA-certificering.

De subscores kunnen handig zijn om te bepalen aan welke gebieden de gezakte kandidaat meer aandacht moet besteden voordat hij of zij het examen opnieuw aflegt. Gezakte kandidaten moeten er rekening mee houden dat de totale schaalscore niet kan worden vastgesteld door een enkelvoudig of gewogen gemiddelde van de subscores te berekenen.

Kandidaten die een te lage score hebben gehaald voor het examen, kunnen een verzoek indienen om hun antwoordbladen handmatig te laten nakijken. Met deze procedure wordt gecontroleerd dat de score die door een computer is vastgesteld, niet is verstoord door strepen, meerdere antwoorden of andere invloeden. Kandidaten dienen er echter vanuit te gaan dat alle scores zijn onderworpen aan verschillende kwaliteitscontroles voordat deze worden gerapporteerd, waardoor een nieuwe beoordeling zeer waarschijnlijk niet in een andere score zal resulteren. Aanvragen van handmatig vastgestelde scores moeten binnen negentig dagen nadat de examenresultaten zijn doorgegeven, schriftelijk worden ingediend bij de certificeringsafdeling. Aanvragen van een handmatig vastgestelde score na de einddatum worden niet verwerkt. Alle aanvragen moeten de naam, examenidentificatienummer en postadres bevatten. Elke aanvraag kost \$75.

## Typen vragen in het CISA -examen

CISA-examenvragen worden ontwikkeld met de bedoeling praktische kennis en de toepassing van algemene concepten en standaarden te meten en testen. Alle vragen zijn ontworpen met één beste antwoord.

Elke CISA-vraag heeft een stam (vraag) en vier opties (antwoordmogelijkheden). De kandidaat wordt gevraagd het juiste of beste antwoord te kiezen uit de opties. De stam kan in de vorm van een vraag of een onvolledige bewering zijn. In sommige gevallen kan ook een scenario worden toegevoegd. Deze vragen bevatten normaal gesproken een beschrijving van een situatie en vereisen dat de kandidaat twee of meer vragen op basis van de verschaft informatie beantwoordt. De kandidaat wordt gewaarschuwd om elke vraag zorgvuldig te lezen. Een CISA-examenvraag kan van de kandidaat vereisen het juiste antwoord te kiezen op basis van een kwalificatie, zoals **MEEST** waarschijnlijk of **BESTE**. In elk geval moet de kandidaat de vraag zorgvuldig lezen, onjuiste antwoorden wegstrepen en vervolgens de best mogelijke keuze maken. Voorbeelden van CISA-examenvragen zijn beschikbaar op [www.isaca.org/cisaassessment](http://www.isaca.org/cisaassessment).

## CISA-certificering aanvragen

Als een kandidaat is geslaagd voor een examen, houdt dat niet in dat hij of zij CISA-gecertificeerd is. Zodra een kandidaat voor het CISA-examen is geslaagd, heeft hij of zij vijf jaar vanaf de examendatum om de certificering aan te vragen. Kandidaten die zijn geslaagd, moeten de aanvraag voor certificering en hun werkervaring invullen op de daarvoor bestemde formulieren die bij de aanvraag worden meegeleverd. **Kandidaten zijn pas gecertificeerd en kunnen de CISA-erkenning pas gebruiken, als de volledige aanvraag is ontvangen en goedgekeurd.** Beslissingen met betrekking tot aanvragen zijn niet definitief: kandidaten kunnen in beroep gaan wanneer hun aanvraag voor certificering is afgewezen. Vragen met betrekking tot geweigerde certificeringen kunnen worden gestuurd naar [certification@isaca.org](mailto:certification@isaca.org). Na certificering ontvangt de nieuwe CISA een certificaat en een CISA-certificeringsspeldje. Op het moment van de aanvraag moeten personen tevens bevestigen dat ISACA zich het recht voorbehoudt, maar hiertoe niet is verplicht, hun CISA-status te publiceren of anderszins openbaar te maken. Voor uw aanvraag voor CISA-certificering wordt \$50 aan verwerkingskosten in rekening gebracht.

# Kandidatengids voor CISA®-examen en -certificering

---

## Vereisten voor een eerste CISA-certificering

Certificering wordt in eerste instantie verleend aan personen die het CISA-examen met succes hebben afgelegd en voldoen aan de volgende werkervaringsvereisten.

Voor certificering is minimaal vijf jaar professionele IT-werkervaring vereist op het gebied van audit, controle, assurance of beveiliging. Vervanging en vrijstelling van dergelijke ervaring kan als volgt worden verkregen:

- Maximaal één jaar ervaring op het gebied van informatiesystemen OF één jaar audit-ervaring buiten IT kan als vervanging dienen voor één jaar ervaring.
- Zestig tot 120 behaalde studiepunten van een universiteitssemester (gelijk aan een graad van twee of vier jaar), niet beperkt door de 10 jaar-restrictie, kan als vervanging dienen voor één of twee jaar ervaring. Ook als meerdere graden zijn behaald, kan maximaal twee jaar worden geclaimd.
- Een graad als doctorandus (Master's degree) van een universiteit die toeziet op de naleving van het door het ISACA gesteunde Model Curriculum kan als vervanging dienen voor één jaar werkervaring. Ga naar [www.isaca.org/modeluniversities](http://www.isaca.org/modeluniversities) voor een lijst van deze scholen. Deze optie kan niet worden gebruikt als vervanging van drie jaar ervaring en opleidingsvrijstelling al zijn geclaimd.
- Een mastergraad in beveiliging- of informatietechnologie van een geregistreerde universiteit kan als vervanging dienen voor één jaar ervaring.

Uitzondering: twee jaar als voltijds universiteitsdocent in een verwant veld (bijvoorbeeld computerwetenschap, boekhouden of auditing van informatiesystemen) kan als vervanging dienen voor één jaar werkervaring.

Ervaring moet worden opgedaan binnen een periode van tien jaar voorafgaand aan de inschrijfdatum voor CISA-certificering of binnen vijf jaar na de datum waarop men voor het eerst voor het examen is geslaagd. Als een volledige aanvraag voor CISA-certificering niet binnen vijf jaar vanaf de datum van slagen voor het examen wordt ingediend, moet het examen worden overgedaan en moet men opnieuw slagen.

Veel mensen leggen het CISA-examen af voordat ze aan de ervaringsvereisten hebben voldaan. Deze gang van zaken is acceptabel en wordt aangemoedigd, maar de CISA-erkenning pas wordt verleend als aan alle vereisten is voldaan.

## Vereisten voor het behouden van de CISA-certificering

CISA's moeten voldoen aan de volgende vereisten om de certificering te behouden:

- Jaarlijks minimaal 20 CPE-uren halen en rapporteren en voor een driejaarlijkse rapportageperiode minimaal 120 CPE-uren halen en rapporteren. Voor meer informatie raadpleegt u het CPE-beleid van CISA op [www.isaca.org/cisacpepolicy](http://www.isaca.org/cisacpepolicy).
- Jaarlijkse de volledige CPE-onderhoudskosten voldoen aan het internationale hoofdkantoor van ISACA.
- Vereiste documentatieverzoeken over CPE-activiteiten beantwoorden en indienen ter ondersteuning van de gerapporteerde uren indien deze zijn geselecteerd voor een jaarlijkse controle.
- De professionele gedragscode van ISACA naleven.

**Wanneer niet aan deze algemene vereisten wordt voldaan, wordt de CISA-erkenning van een persoon ingetrokken. Alle certificaten zijn eigendom van ISACA. Als een persoon goedgekeurd is voor certificering en deze vervolgens is ingetrokken, dient de persoon het certificaat te vernietigen.**

## ISACA Code of Professional Ethics (Professionele gedragscode van ISACA)

Wanneer deze Professionele gedragscode niet wordt nageleefd, kan dat resulteren in een onderzoek naar het gedrag en uiteindelijk in disciplinaire maatregelen van een lid en/of houder van een certificering. ISACA heeft een Code of Professional Ethics (Professionele gedragscode) als richtlijn ingevoerd voor het professionele en persoonlijke gedrag van leden van de vereniging en/of de houders van certificeringen. De ISACA Code of Professional Ethics kan online worden geraadpleegd op [www.isaca.org/ethics](http://www.isaca.org/ethics).

## Intrekken van CISA-certificering

De CISA-certificeringscommissie kan op eigen initiatief na een zorgvuldige en grondige afweging de CISA-certificering van een persoon intrekken om een van de volgende redenen:

- Niet naleven van het CPE-beleid van CISA
- Schending van een bepaling van de ISACA-gedragscode voor professionals
- Informatie vervalsen of met opzet achterhouden
- Een valse verklaring afgeven over een materieel feit
- Anderen betrekken of helpen in oneerlijk, onbevoegd of ongepast gedrag op enig moment in verband met het CISA-examen of het certificeringsproces

# Kandidatengids voor CISA®-examen en -certificering

## Beschrijving van de CISA-praktijkgebieden

### Taak- en kennisverklaringen van CISA

<b>INHOUDSGEBIED (DOMEIN)</b>
<b>Domein 1: Het auditproces voor informatiesystemen</b> —Voorzien in auditservices met IT-auditstandaarden om de organisatie te helpen bij het beschermen en beheren van informatiesystemen.
<b>Domein 1: Taken</b>
T1.1 Een op risico's gebaseerde IT-auditstrategie ontwikkelen en implementeren in overeenstemming met IT-auditnormen en zo garanderen dat de sleutelgebieden aan bod komen.
T1.2 Specifieke audits plannen om te bepalen of IT-informatiesystemen worden beveiligd en beheerd en of deze van waarde zijn voor de organisatie.
T1.3 Audits houden in overeenstemming met IT-auditnormen om geplande auditdoelstellingen te bereiken.
T1.4 Auditresultaten rapporteren en aanbevelingen doen aan belanghebbenden om resultaten te communiceren en indien nodig aanpassingen uit te voeren.
T1.5 Follow-ups houden of statusrapporten opmaken om ervoor te zorgen dat de gepaste acties tijdig door het management worden ondernomen.
<b>Domein 1: Kennisgebieden</b>
KS1.1 Kennis van ISACA IT Audit and Assurance Standards, Guidelines en Tools and Techniques; Code of Professional Ethics en andere van toepassing zijnde normen
KS1.2 Kennis van concepten, programma's en technieken voor risicobepaling in een auditcontext
KS1.3 Kennis van controledoelstellingen en controles die zijn gerelateerd aan informatiesystemen
KS1.4 Kennis van methoden voor auditplanning en -management, met inbegrip van follow-up
KS1.5 Kennis van fundamentele businessprocessen (bv. aankoop, loonlijst, crediteuren, debiteuren), met inbegrip van relevante IT
KS1.6 Kennis van toepasselijke wetten en regels die van invloed zijn op de draagwijdte, bewijsgeving en -bewaring, en frequentie van audits.
KS1.7 Kennis van bewijsgevingstechnieken (bv. observatie, navraag, inspectie, interview, gegevensanalyse) die worden gebruikt om auditbewijs te verzamelen, beschermen en bewaren
KS1.8 Kennis van verschillende samplingmethodologieën
KS1.9 Kennis van rapportage- en communicatiemethoden (bv. ondersteuning bieden, onderhandelen, conflicten oplossen en auditverslagstructuur)
KS1.10 Kennis van systemen en frameworks voor de kwaliteitswaarborg van audits
<b>Domein 2: IT-governance en -management</b> —Garanderen dat het nodige leiderschap en de nodige organisatiestructuren en -processen aanwezig zijn om doelstellingen te realiseren en de strategie van de organisatie te ondersteunen.
<b>Domein 2: Taken</b>
T2.1 De doeltreffendheid van de IT-governancestructuur evalueren om te bepalen of beslissingen, richting en prestaties van IT de strategieën en doelstellingen van de organisatie ondersteunen.
T2.2 De IT-organisatiestructuur en HR-management (personeelsmanagement) evalueren om ervoor te zorgen dat deze de strategieën en doelstellingen van de organisatie ondersteunen.
T2.3 Evalueren of de IT-strategie, met inbegrip van de IT-richting, en de processen voor de strategieontwikkeling, -goedkeuring, -implementatie en -handhaving in overeenstemming zijn met de strategieën en doelstellingen van de organisatie.
T2.4 De beleidsregels, normen en procedures van de organisatie op het gebied van IT en de processen van de ontwikkeling, goedkeuring, implementatie, handhaving en controle ervan evalueren om te bepalen of deze de IT-strategie ondersteunen en voldoen aan de regelgevende en wettelijke voorschriften.
T2.5 De adequaatheid van het kwaliteitsmanagementsysteem evalueren om te bepalen of het de strategieën en doelstellingen van de organisatie op een kosteneffectieve manier ondersteunt.
T2.6 Evalueren of het IT-management en de opvolging van controles (bv. continue controle, kwaliteitswaarborg [QA]) in overeenstemming zijn met het beleid, de normen en de procedures van de organisatie.
T2.7 Evalueren of investering, gebruik en toewijzing van IT-resources, met inbegrip van criteria voor prioriteitsverlening, in overeenstemming zijn met de strategieën en doelstellingen van de organisatie.
T2.8 Strategieën en doelstellingen op het gebied van IT-contracten en contractmanagementpraktijken evalueren om te bepalen of deze de strategieën en doelstellingen van de organisatie ondersteunen.
T2.9 Risicomanagementpraktijken evalueren om te bepalen of de IT-gerelateerde risico's van de organisatie op juiste wijze worden beheerd.
T2.10 Controle- en assurancepraktijken evalueren om te bepalen of de directie en het management op tijd en voldoende informatie krijgen over IT-prestaties.
T2.11 Het bedrijfscontinuïteitsplan van de organisatie evalueren om te bepalen of de organisatie essentiële bedrijfsactiviteiten kan voortzetten gedurende de periode van een IT-verstoring.

# Kandidatengids voor CISA® -examen en -certificering

<b>INHOUDSGEBIED (DOMEIN)</b>	
<b>Domein 2: Kennisgebieden</b>	
KS2.1	Kennis van IT-governance, -management, -beveiliging en -controleframeworks en gerelateerde normen, richtlijnen en werkwijzen
KS2.2	Kennis van het doel van de strategie, het beleid, de normen en de procedures op IT-gebied voor een organisatie en de essentiële elementen ervan
KS2.3	Kennis van de organisatiestructuur, rollen en verantwoordelijkheden op het gebied van IT
KS2.4	Kennis van de processen voor de ontwikkeling, implementatie en handhaving van de strategie, het beleid, de normen en de procedures op IT-gebied.
KS2.5	Kennis van de technologische richting en IT-architectuur van de organisatie en de implicaties ervan voor het bepalen van strategische richtingen op lange termijn
KS2.6	Kennis van relevante wetten, regels en industriële normen die van invloed zijn op de organisatie
KS2.7	Kennis van kwaliteitsmanagementsystemen
KS2.8	Kennis van het gebruik van maturiteitsmodellen
KS2.9	Kennis van procesoptimalisatietechnieken
KS2.10	Kennis van investering en toewijzing van IT-resources, met inbegrip van criteria voor prioriteitsverlening (bv. portfoliomanagement, waardemanagement, projectmanagement)
KS2.11	Kennis van IT-leveranciersselectie, contractmanagement, relatiemanagement en prestatiecontroleprocessen, met inbegrip van outsourcingrelaties met derden
KS2.12	Kennis van ondernemingsrisicomanagement
KS2.13	Kennis van werkwijzen voor de controle en rapportage van IT-prestaties (bv. balanced scorecards en KPI's (Key Performance Indicators))
KS2.14	Kennis van HR-managementpraktijken (personeelsmanagement) op IT-gebied die worden gebruikt om het businesscontinuïteitsplan te activeren
KS2.15	Kennis van de businessimpactanalyse (BIA) betreffende de businesscontinuïteitsplanning (BCP)
KS2.16	Kennis van de normen en procedures voor het ontwikkelen en handhaven van het businesscontinuïteitsplan (BCP) en testmethoden.
<b>Domein 3: Acquisitie, ontwikkeling en implementatie van informatiesystemen</b> —Garanderen dat het beleid voor acquisitie, ontwikkeling, testen en implementatie van informatiesystemen aan de strategieën en doelstellingen van de organisatie voldoet.	
<b>Domein 3: Taken</b>	
T3.1	De business case voor voorgestelde investeringen in acquisitie, ontwikkeling, handhaving en de daaropvolgende afdanking van informatiesystemen evalueren om te bepalen of deze voldoet aan de businessdoelstellingen.
T3.2	Werkwijzen en controles van het projectmanagement evalueren om te bepalen of op een kosteneffectieve manier aan de businessvereisten wordt voldaan terwijl de risico's voor de organisatie worden beheerst.
T3.3	Controles uitvoeren om te bepalen of een project vorderingen maakt in overeenstemming met projectplannen, dat een project adequaat wordt gedocumenteerd en dat de statusrapportage ervan accuraat is.
T3.4	Evalueren of controles voor informatiesystemen tijdens de fasen van vereisten, acquisitie, ontwikkeling en tests in overeenstemming zijn met het beleid, de normen en de procedures van de organisatie en relevante externe vereisten.
T3.5	Evalueren in hoeverre informatiesystemen gereed zijn voor implementatie en migratie naar productie om te bepalen of leverbare items van projecten en controles zijn gerealiseerd en of aan de vereisten van de organisatie is voldaan.
T3.6	Controle uitvoeren na de implementatie van systemen om te bepalen of leverbare items en controles zijn gerealiseerd en of aan de vereisten van de organisatie is voldaan.
<b>Domein 3: Kennisgebieden</b>	
KS3.1	Kennis van winstrealisatiepraktijken (bv. haalbaarheidsstudies, business cases, totale eigendomskosten [TCO] en ROI)
KS3.2	Kennis van mechanismen van projectbestuur (bv. stuurgroep, toezichtcommissie voor projecten en bureau voor projectmanagement)
KS3.3	Kennis van controleframeworks, werkwijzen en programma's voor projectmanagement
KS3.4	Kennis van risicomanagementpraktijken toegepast op projecten
KS3.5	Kennis van IT-architectuur gerelateerd aan gegevens, toepassingen en technologie (bv. gedistribueerde toepassingen, webtoepassingen, webservices en n-tier toepassingen)
KS3.6	Kennis van acquisitiepraktijken (bv. evaluatie van leveranciers, leveranciersmanagement en escrow)
KS3.7	Kennis van analyse en -managementpraktijken voor vereisten (bv. verificatie, foutopsporing, gap-analyse, kwetsbaarheidsmanagement en beveiligingsvoorschriften van vereisten)
KS3.8	Kennis van succescriteria en risico's van projecten
KS3.9	Kennis van controledoelstellingen en -methoden om te zorgen voor volledigheid, nauwkeurigheid, geldigheid en autorisatie van transacties en gegevens
KS3.10	Kennis van methodologieën en programma's voor systeemontwikkeling, met inbegrip van de sterke en zwakke punten ervan (bv. 'agile' ontwikkelingspraktijken, prototypen, snelle toepassingsontwikkeling [RAD] en objectgeoriënteerde ontwerpstechnieken)

# Kandidatengids voor CISA®-examen en -certificering

<b>INHOUDSGEBIED (DOMEIN)</b>
KS3.11 Kennis van testmethodologieën en -werkwijzen gerelateerd aan de ontwikkeling van informatiesystemen
KS3.12 Kennis van configuratie- en releasemanagement gerelateerd aan de ontwikkeling van informatiesystemen
KS3.13 Kennis van systeemmigratie- en infrastructuurontwikkelingspraktijken en programma's, technieken en procedures voor gegevensconversie
KS3.14 Kennis van doelstellingen en werkwijzen van controle na implementatie (bv. projectafsluiting, controle-implementatie, opbrengstrealisatie en prestatiemeting)
<b>Domein 4: Operaties, onderhoud en ondersteuning van informatiesystemen</b> —Garanderen dat de processen voor operaties, onderhoud en ondersteuning van informatiesystemen aan de strategieën en doelstellingen van de organisatie voldoen.
<b>Domein 4: Taken</b>
T4.1 Periodieke controles van informatiesystemen houden om te bepalen of deze nog steeds aan de doelstellingen van de organisatie voldoen.
T4.2 Managementpraktijken op serviceniveau evalueren om te bepalen of het niveau van interne en externe dienstverleners is gedefinieerd en beheerd.
T4.3 Managementpraktijken van derden evalueren om te bepalen of de controle niveaus die door de organisatie worden verwacht door de provider worden gehaald.
T4.4 Operaties en eindgebruikerprocedures evalueren om te bepalen of geplande en ongeplande processen volledig worden beheerd.
T4.5 Het handhavingproces van informatiesystemen evalueren om te bepalen of deze op een doeltreffende wijze worden gecontroleerd en nog steeds de doelstellingen van de organisatie ondersteunen.
T4.6 Gegevensbeheerpraktijken evalueren om de integriteit en optimalisatie van databases te bepalen.
T4.7 Het gebruik van controleprogramma's en -methoden voor capaciteit en prestaties evalueren om te bepalen of IT-diensten voldoen aan de doelstellingen van de organisatie.
T4.8 Probleem- en incidentmanagementpraktijken evalueren om te bepalen of incidenten, problemen of fouten op tijd worden geregistreerd, geanalyseerd en opgelost.
T4.9 Wijzigings-, configuratie- en releasemanagementpraktijken evalueren om te bepalen of geplande en ongeplande wijzigingen die worden aangebracht in de productieomgeving van de organisatie adequaat worden beheerd en gedocumenteerd.
T4.10 De adequaatheid van back-up- en herstelvoorzieningen evalueren om de beschikbaarheid van informatie die nodig is om de verwerking te hervatten, te bepalen.
T4.11 Het calamiteitenherstelplan van de organisatie evalueren om te bepalen of het herstel van IT-verwerkingsmogelijkheden mogelijk zijn in het geval van een calamiteit.
<b>Domein 4: Kennisgebieden</b>
KS4.1 Kennis van managementpraktijken op serviceniveau en de componenten van een overeenkomst op serviceniveau
KS4.2 Kennis van technieken om de inachtneming van derden van de interne controles van de organisatie te controleren
KS4.3 Kennis van operaties en eindgebruikerprocedures voor het beheer van geplande en ongeplande processen
KS4.4 Kennis van de technologieconcepten gerelateerd aan hardware- en netwerkcomponenten, systeemsoftware en systemen voor databasemanagement
KS4.5 Kennis van controletechnieken die de integriteit van systeeminterfaces waarborgen
KS4.6 Kennis van softwarelicentie- en licentiebeheerpraktijken
KS4.7 Kennis van programma's en methoden voor de betrouwbaarheid van systemen (bv. fouttolerantiehardware, elimineren van 'single point-of-failure' en clusteren)
KS4.8 Kennis van databasebeheerpraktijken
KS4.9 Kennis van capaciteitsplanning en gerelateerde controleprogramma's en -technieken
KS4.10 Kennis van controleprocessen, -programma's en -methoden voor systeemprestaties (bv. netwerkanalyseprogramma's, systeemgebruiksrapporten en werkdrukverdeling)
KS4.11 Kennis van probleem- en incidentmanagementpraktijken (bv. helpdesk, escalatieprocedures en probleemopvolging)
KS4.12 Kennis van processen voor het beheren van geplande en ongeplande wijzigingen in de productiesystemen en/of infrastructuur met inbegrip van wijzigings-, configuratie-, release- en patchmanagementpraktijken
KS4.13 Kennis van werkwijzen voor back-up, opslag, onderhoud, bewaren en herstel van gegevens
KS4.14 Kennis van geldende wet- en regelgeving, contractuele kwesties en verzekeringsaangelegenheden betreffende calamiteitenherstel
KS4.15 Kennis van de businessimpactanalyse (BIA) betreffende de planning voor calamiteitenherstel
KS4.16 Kennis van de ontwikkeling en handhaving van calamiteitenherstelplannen
KS4.17 Kennis van typen alternatieve verwerkingssites en methoden waarmee de contractuele overeenkomsten worden bewaakt (bv. hot sites, warm sites en cold sites)
KS4.18 Kennis van processen gebruikt om de calamiteitenherstelplannen in te roepen
KS4.19 Kennis van testmethoden voor calamiteitenherstel

# Kandidatengids voor CISA®-examen en -certificering

## INHOUDSGEBIED (DOMEIN)

**Domein 5: Bescherming van informatiemiddelen**—Garanderen dat beveiligingsbeleid, -normen, -procedures en -beheer van de organisatie de vertrouwelijkheid, integriteit en beschikbaarheid van informatiemiddelen verzekeren.

### *Domein 5: Taken*

T5.1 Evalueren of beleid, normen en procedures voor informatiebeveiliging volledig en in overeenstemming zijn met algemeen gangbare werkwijzen.

T5.2 Het ontwerp, de implementatie en de controle evalueren van systeem- en logische beveiligingscontroles om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te verifiëren.

### *Domein 5: Taken (vervolg)*

T5.3 Evalueren of het ontwerp, de implementatie en de controle van de processen en procedures voor gegevensclassificatie in overeenstemming zijn met het beleid, de normen en de procedures van de organisatie en relevante externe vereisten.

T5.4 Het ontwerp, de implementatie en de controle evalueren van fysieke toegangs- en omgevingscontroles om te bepalen of informatiemiddelen adequaat worden beschermd.

T5.5 De processen en procedures waarmee informatiemiddelen worden opgeslagen, opgevraagd, getransporteerd en vernietigd (bv. back-upmedia, offsite-opslag, afgedrukte gegevens en softcopy media) evalueren om te bepalen of informatiemiddelen adequaat worden beschermd.

### *Domein 5: Kennisgebieden*

KS5.1 Kennis van de technieken voor het ontwerp, de implementatie en de controle van beveiligingscontroles, met inbegrip van beveiligingsbewustzijnsprogramma's

KS5.2 Kennis van processen die zijn gerelateerd aan controle van en reactie op beveiligingsincidenten (bv. escalatieprocedures en afhandelingsteam van noodincidenten)

KS5.3 Kennis van logische toegangscontroles voor de identificatie, verificatie en beperking van gebruikers tot geautoriseerde functies en gegevens

KS5.4 Kennis van de beveiligingscontroles voor hardware, systeemsoftware (bv. toepassingen en besturingssystemen) en databasemanagementsystemen

KS5.5 Kennis van risico's en controles die worden geassocieerd met de virtualisatie van systemen

KS5.6 Kennis van de configuratie, implementatie, besturing en handhaving van netwerkbeveiligingscontroles

KS5.7 Kennis van netwerk- en internetbeveiligingsapparaten, -protocols en -technieken

KS5.8 Kennis van aanvalsmethoden en -technieken op informatiesystemen

KS5.9 Kennis van opsporingsprogramma's en controletechnieken (bv. malware, virusdetectie, spyware)

KS5.10 Kennis van technieken voor beveiligingstests (bv. tests op binnendringing en kwetsbaarheidsscanning)

KS5.11 Kennis van risico's en controles die worden geassocieerd met gegevenslekken

KS5.12 Kennis van technieken voor encryptie

KS5.13 Kennis van KPI-componenten (Public Key Infrastructure) en technieken voor digitale handtekening

KS5.14 Kennis van risico's en controles die worden geassocieerd met peer-to-peer computing, instant messaging en webgebaseerde technologieën (bv. sociale netwerken, message boards en blogs)

KS5.15 Kennis van controles en risico's die worden geassocieerd met het gebruik van draagbare en draadloze apparaten

KS5.16 Kennis van beveiliging via spraakcommunicatie (bv. PBX en VoIP)

KS5.17 Kennis van technieken en processen voor bewijsbewaring die in forensische onderzoeken worden gevolgd (bv. IT, proces, chain of custody)

KS5.18 Kennis van normen en ondersteunende procedures voor gegevensclassificatie

KS5.19 Kennis van fysieke toegangscontroles voor de identificatie, verificatie en beperking van gebruikers tot geautoriseerde faciliteiten

KS5.20 Kennis van apparaten en ondersteuningsmethoden voor milieubescherming

KS5.21 Kennis van de processen en procedures waarmee vertrouwelijke informatiemiddelen worden opgeslagen, opgevraagd, getransporteerd en vernietigd



# Vorbereiding op de CISA- examens van 2012

## 2012 CISA-evaluatiebronnen voor examenvorbereiding en persoonlijke ontwikkeling

---

Succesvolle kandidaten voor het CISA®-examen (Certified Information Systems Auditor®) hebben een goed georganiseerd studieplan. Om mensen te helpen met de ontwikkeling van een succesvol studieplan biedt ISACA® verscheidene studiehulpmiddelen en evaluatiecursussen aan examenkandidaten aan. Deze bestaan uit:

### Studiehulpmiddelen

- *CISA® Review Manual 2012*
- *CISA® Review Questions, Answers & Explanations Manual 2011*
- *CISA® Review Questions, Answers & Explanations Manual 2011 Supplement*
- *CISA® Review Questions, Answers & Explanations Manual 2012 Supplement*
- CISA® Practice Question Database v12

Om te bestellen bezoekt u [www.isaca.org/cisabooks](http://www.isaca.org/cisabooks).

### Evaluatiecursussen

- Chapter-gesponsorde evaluatiecursussen ([www.isaca.org/cisareview](http://www.isaca.org/cisareview))
- CISA® Online Review Course ([www.isaca.org/elearning](http://www.isaca.org/elearning))