



CERTIFIED INFORMATION SYSTEMS AUDITOR®

Guida del candidato all'esame
e alla certificazione CISA® 2012

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA® Exam and Certification)

Esami CISA 2012

Date importanti

Data dell'esame - 9 giugno 2012

Termine per l'iscrizione anticipata: 8 febbraio 2012

Termine per l'iscrizione finale: 4 aprile 2012

Modifiche di iscrizione all'esame: tra il 14 aprile e il 20 aprile, con un supplemento di \$ USA 50; non si accettano modifiche dopo il 20 aprile 2012

Rimborsi: entro il 13 aprile 2012, supplemento amministrativo di \$ USA 100; nessun rimborso sarà concesso dopo tale data

Rinvii: per le domande di rinvio ricevute entro il 20 aprile 2012, è richiesto un supplemento amministrativo di \$ USA 50. Per le domande ricevute dal 21 aprile al 24 maggio 2012, è richiesto un supplemento amministrativo di \$ USA 100. Non si accettano domande di rinvio dopo il 24 maggio 2012.

Data dell'esame - 8 dicembre 2012

Termine per l'iscrizione anticipata: 15 agosto 2012

Termine per l'iscrizione finale: 3 ottobre 2012

Modifiche di iscrizione all'esame: tra il 6 ottobre e il 12 ottobre, con un supplemento di \$ USA 50; non si accettano modifiche dopo il 12 ottobre 2012

Rimborsi: entro il 5 ottobre 2012, con un supplemento amministrativo di \$ USA 100; nessun rimborso sarà concesso dopo tale data

Rinvii: per le domande di rinvio ricevute entro il 12 ottobre 2012, è richiesto un supplemento amministrativo di \$ USA 50. Per le domande ricevute dal 13 ottobre al 21 novembre 2012, è richiesto un supplemento amministrativo di \$ USA 100. Non si accettano domande di rinvio dopo il 21 novembre 2012.

Tutti i termini e le scadenze sono calcolati in base alle ore 17 CT (central time - fuso orario della zona centrale) di Chicago, Illinois, USA.

Guida del candidato all'esame e alla certificazione CISA® 2012
(Candidate's Guide to the CISA® Exam and Certification)
Stampato negli Stati Uniti d'America.

Indice

| | |
|--|---|
| Introduzione..... | 3 |
| Rinnovo del programma CISA ai sensi dell'ISO/IEC 17024:2003 | 3 |
| L'esame CISA | 3 |
| Preparazione all'esame CISA | 4 |
| Svolgimento dell'esame CISA | 4 |
| Punteggio dell'esame CISA | 6 |
| Tipologia di domande dell'esame CISA..... | 6 |
| Domanda di Certificazione CISA | 7 |
| Requisiti per il conseguimento della prima Certificazione CISA..... | 7 |
| Requisiti per il mantenimento della Certificazione CISA | 7 |
| Codice di etica professionale ISACA | 7 |
| Revoca della Certificazione CISA | 7 |
| Compiti e enunciati di conoscenza CISA..... | 8 |

Informazioni su ISACA®

Con 95.000 associati in 160 Paesi, ISACA (www.isaca.org) è leader mondiale nel fornire competenze, certificazioni, community, patrocinio e formazione nei settori dell'assurance e sicurezza dei sistemi informativi (IS), del governo dell'impresa, della gestione dell'IT e dei rischi e della compliance correlati all'IT. Fondata nel 1969, ISACA, associazione indipendente senza fini di lucro, organizza conferenze internazionali, pubblica l'*ISACA® Journal*, e sviluppa standard internazionali relativi all'audit e al controllo dei sistemi informativi (IS), che contribuiscono a garantire i propri componenti sull'affidabilità e a trarre valore dai sistemi informativi. Favorisce inoltre l'acquisizione delle competenze e delle conoscenze IT e le attesta mediante le certificazioni riconosciute a livello internazionale quali: Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) e Certified in Risk and Information Systems Control™ (CRISC™). ISACA aggiorna costantemente COBIT®, che consente ai professionisti dell'IT e ai vertici aziendali di mantenere i propri impegni a livello di governo e gestione dell'IT, in particolar modo nei settori assurance, sicurezza, rischi e controllo, nonché di creare valore per il business.

Limitazione della responsabilità

ISACA e la Commissione di certificazione CISA hanno concepito la guida del candidato all'esame e alla certificazione CISA 2012 (*Candidate's Guide to the CISA® Exam and Certification*) come strumento utile per coloro che aspirano a conseguire la certificazione CISA. ISACA non si pronuncia né fornisce garanzie sulla possibilità che l'utilizzo di questa guida o di altre pubblicazioni dell'Associazione garantiscano ai candidati il superamento dell'esame CISA.

Diritti riservati

Copyright © 2011 ISACA. Sono vietate la riproduzione o la detenzione in qualsiasi forma e per qualsiasi finalità senza una precedente autorizzazione scritta da parte di ISACA. In riferimento alla presente pubblicazione, non vengono concessi altri diritti o autorizzazioni. Tutti i diritti riservati.

ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telefono: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: exam@isaca.org
Sito Web: www.isaca.org

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

Introduzione

Il carattere di eccellenza di un programma di certificazione professionale è dato dal valore e dal riconoscimento conferito a coloro che la conseguono. Dal 1978, il programma Certified Information Systems Auditor (CISA), sponsorizzato da ISACA, è lo standard di realizzazione professionale universalmente accettato tra i professionisti nel settore del controllo, sicurezza e audit dei sistemi informatici (IS).

Le competenze e le prassi tecniche che CISA promuove e valorizza sono gli elementi costitutivi del successo conseguito in questo settore. La certificazione CISA è garanzia di competenza e rappresenta il metro valutativo della professionalità. In un periodo che vede una domanda crescente di professionisti competenti nel settore della sicurezza, controllo e audit di IS, CISA si è imposta come programma di certificazione di gran lunga preferito dai privati e dalle aziende a livello mondiale. La certificazione CISA è sinonimo di impegno meritorio nell'attività svolta nella propria professione e nel servizio fornito ad un'azienda.

Rinnovo del programma CISA ai sensi dell'ISO/IEC 17024:2003

L'American National Standards Institute (ANSI) ha accreditato la certificazione CISA ai sensi delle norme ISO/IEC 17024:2003, Requisiti generali per gli enti che gestiscono sistemi di certificazione delle persone fisiche (General Requirements for Bodies Operating Certification Systems of Persons). ANSI è un'associazione privata senza scopo di lucro che si occupa dell'accREDITAMENTO di aziende che certificano, in qualità di terza parte, sistemi, prodotti e personale.

Lo standard ISO/IEC 17024 definisce le norme a cui tali aziende devono attenersi nel certificare le persone fisiche a fronte di determinati requisiti. L'ANSI definisce ISO/IEC 17024 come "lo standard che, in previsione, rivestirà un ruolo di primaria importanza nella standardizzazione mondiale delle agenzie di certificazione, nell'aumento dell'interscambio tra nazioni, nel miglioramento della sicurezza pubblica e nella tutela dei consumatori".



Programma Accreditato ANSI.
CERTIFICAZIONE
DEL PERSONALE
#0694
ISO/IEC 17024

L'accREDITAMENTO ANSI:

- Promuove le qualifiche e le competenze esclusive sancite dalle certificazioni ISACA
- Tutela la validità stessa delle certificazioni e rende possibile il ricorso alla tutela giuridica
- Rafforza la fiducia del consumatore e del pubblico nelle certificazioni e in chi le detiene
- Facilita l'interscambio e il passaggio tra nazioni e settori diversi

L'accREDITAMENTO ANSI attesta che le procedure ISACA soddisfano i requisiti essenziali ANSI quanto a trasparenza, equilibrio, pubblico consenso e aspetti procedurali. ISACA prevede che per i detentori della certificazione CISA continueranno a presentarsi in tutto il mondo nuove e interessanti opportunità.

L'esame CISA

Sviluppo/Descrizione dell'esame CISA

La Commissione di certificazione CISA sovrintende allo sviluppo dell'esame e garantisce l'attualità del suo contenuto. Le domande contenute nell'esame CISA vengono sviluppate attraverso un processo globale concepito per perfezionare la qualità finale dell'esame. Tale processo comprende una Sottocommissione di ottimizzazione del test (TES - Test Enhancement Subcommittee) che, in collaborazione con gli autori, si occupa della messa a punto e della revisione delle domande prima che esse vengano sottoposte all'attenzione della Commissione di certificazione CISA per un'ulteriore revisione.

La prassi professionale è alla base dell'esame e dell'esperienza richiesta per il conseguimento della certificazione CISA. Questa prassi professionale viene regolarmente aggiornata e consta di cinque aree tematiche (settori). Tali settori, con le relative declaratorie delle attività e delle conoscenze tipiche sono state il risultato di una ricerca dettagliata e delle osservazioni fornite da esperti in materia provenienti da ogni parte del mondo.

Le attività e le conoscenze tipiche riflettono i compiti professionali svolti da coloro che conseguono la certificazione CISA, nonché le conoscenze necessarie allo svolgimento di tali compiti. I candidati all'esame saranno valutati sulla base delle loro conoscenze di prassi professionali associate all'effettivo svolgimento dei relativi compiti.

L'attuale analisi della prassi professionale consiste nei seguenti settori e relative percentuali:

- **Processo di audit dei sistemi informatici (14%)**
- **IT Governance e Management (14%)**
- **Acquisizione, sviluppo e implementazione dei sistemi informatici (19%)**
- **Operazioni, mantenimento e supporto dei servizi informatici (23%)**
- **Protezione delle risorse informatiche (30%)**

Nota: le percentuali associate ai diversi settori indicano l'importanza a essi attribuita o la percentuale di domande presenti nell'esame per ciascun settore. Per una descrizione delle declaratorie delle attività e delle conoscenze tipiche di ciascun settore, consultare le pagine da 8 a 11.

L'esame consiste in 200 domande a scelta multipla e si svolge ogni due anni in giugno e dicembre, in una prova della durata di quattro ore. I candidati possono scegliere la lingua in cui sostenere l'esame fra un'ampia scelta. Per l'elenco delle lingue attualmente disponibili, visitare il sito www.isaca.org/cisaterminology.

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

Preparazione all'esame CISA

Per superare l'esame CISA si consiglia di seguire un piano di studio strutturato. Per assistere i candidati nel definire un buon piano di preparazione, l'ISACA propone diversi sussidi didattici e corsi volti a verificare il livello di preparazione raggiunto da ciascun candidato. Visitare il sito www.isaca.org/cisaguide per prendere visione dei sussidi didattici ISACA che possono rappresentare un valido aiuto nella preparazione dell'esame. Si consiglia di ordinare questo materiale con tempestività, poiché i tempi di consegna possono variare da una a quattro settimane a seconda della zona geografica di destinazione e delle procedure doganali vigenti. Per informazioni aggiornate sulle spedizioni, consultare il sito www.isaca.org/shipping.



ISACA propone inoltre CISA® Online Review Course. Il corso comprende esercizi interattivi, studio di casi, strumenti di ripasso e domande di esercitazione. Consultare www.isaca.org/elearning per ulteriori informazioni e per un'anteprima del corso.

Un elenco di riferimenti bibliografici utili per approfondimenti in vista dell'esame può essere trovato nel *Manuale Tecnico CISA 2012*.

Un elenco di acronimi che i candidati devono conoscere e un ulteriore elenco di acronimi di possibile interesse sono disponibili sul sito www.isaca.org/cisaguide.

Per assistere i candidati nella terminologia tecnica, una lista dei termini tecnici più frequentemente usati in Inglese, mappati con la rispettiva traduzione nelle altre lingue offerte è disponibile sul sito di ISACA su www.isaca.org/cisaguide.

ISACA mantiene un glossario generale e glossari specifici per ciascuna certificazione. Questi glossari sono consultabili sul sito www.isaca.org/glossary.

ISACA e la Commissione di certificazione CISA non si pronunciano né danno garanzie sulla possibilità che queste o altre pubblicazioni o corsi dell'associazione garantiscano ai candidati il superamento dell'esame.

Svolgimento dell'esame CISA

ISACA si serve di un'agenzia esaminatrice professionale accreditata a livello internazionale, che collabora all'elaborazione, allo svolgimento e all'attribuzione dei punteggi dell'esame CISA.

I candidati che desiderano commentare lo svolgimento della prova possono farlo al termine della sessione d'esame, compilando il relativo questionario ("Test Administration Questionnaire"). Il questionario relativo allo svolgimento dell'esame è inserito nella parte posteriore del libretto d'esame e le risposte al questionario devono essere inserite nelle caselle da P a S nella sezione "Codici speciali" (griglia n. 4) nella parte anteriore del foglio risposte.

I candidati che desiderano aggiungere qualsiasi altro commento o domanda sullo svolgimento dell'esame, incluse le informazioni sulla sede dell'esame o sul contenuto dell'esame, devono contattare la sede internazionale di ISACA inviando una notifica per posta o per e-mail (exam@isaca.org). Qualsiasi commento o domanda deve pervenire a ISACA entro due settimane dalla data dell'esame. Per favore includete le seguenti informazioni nei vostri commenti: numero ID dell'esame, luogo del test, giorno dell'esame e ogni altro dettaglio rilevante sul problema specifico. Nel processo di attribuzione finale del punteggio dell'esame verranno conteggiati solo i commenti pervenuti a ISACA nel corso delle prime 2 settimane successive allo svolgimento dell'esame.

Foglio d'ammissione

All'incirca due o tre settimane prima della data dell'esame CISA, ai candidati verrà inviato un foglio cartaceo d'ammissione e una versione elettronica dello stesso ticket da parte di ISACA. I candidati all'esame possono inoltre scaricare una copia del ticket d'ammissione da www.isaca.org > pagina MyISACA del sito. Sui fogli d'ammissione sarà riportata la data, l'ora e il luogo in cui presentarsi per sostenere l'esame, nonché il programma completo del giorno d'esame e l'elenco del materiale che occorre portare con sé il giorno dell'esame CISA. Ad eccezione di cambiamenti delle informazioni sul contatto, ai candidati non è permesso di scrivere sul foglio d'ammissione.

Si tenga presente che: per ricevere una copia del foglio d'ammissione tutte le quote relative all'esame devono essere corrisposte. I fogli d'ammissione sono inviati via posta cartacea e e-mail all'indirizzo postale e di posta elettronica attualmente presente nel file. Saranno ammessi a sostenere l'esame solo i candidati provvisti di un foglio d'ammissione e un documento d'identità valido, e il nome sul foglio d'ammissione e sul documento devono corrispondere. Sia la copia cartacea sia una stampa della versione elettronica del foglio di ammissione sono validi per poter partecipare all'esame. In caso di modifica del proprio recapito o indirizzo di posta elettronica, i candidati devono provvedere ad aggiornare il loro profilo sul sito internet ISACA (www.isaca.org) o contattare exam@isaca.org.

I candidati devono tassativamente prendere nota dell'ora esatta di registrazione e di quella di inizio dell'esame, riportate sul foglio d'ammissione. A NESSUN CANDIDATO SARÀ CONSENTITO L'ACCESSO ALLA SEDE D'ESAME, DOPO CHE L'ESAMINATORE CAPO ABBAIA INIZIATO A LEGGERE LE ISTRUZIONI ORALI, CIRCA 30 MINUTI PRIMA DELL'INIZIO DELL'ESAME. I candidati che si presentino dopo l'inizio della lettura delle istruzioni orali non potranno sostenere l'esame, ma riceveranno il rimborso della quota di iscrizione. Ogni foglio d'ammissione può essere utilizzato esclusivamente nella sede d'esame indicata sul foglio stesso. I documenti d'identità saranno controllati durante lo svolgimento dell'esame.

Disposizioni speciali

Per quanto riguarda le modalità d'esame, ISACA è disponibile a stipulare accordi ragionevoli con i candidati affetti da handicap sensoriali o motori, oppure aventi esigenze particolari di natura religiosa debitamente documentate. I candidati possono chiedere trattamenti o condizioni d'esame particolari (purché ragionevoli), per quanto concerne il formato dell'esame, le presentazioni, la partecipazione, gli alimenti, le bevande o gli orari presso le sedi d'esame. Eventuali richieste di poter consumare cibo o bevande presso le sedi d'esame devono essere accompagnate da una lettera del medico curante. In caso contrario, **non è consentito portare alimenti o bevande presso le sedi degli esami.** Richieste di trattamento o condizioni particolari devono essere inviate ad ISACA International Headquarters per iscritto, corredate dalla documentazione necessaria, entro e non oltre il 4 aprile 2012 per la data d'esame di giugno 2012, e il 3 ottobre 2012 per la data d'esame di dicembre 2012.

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

Puntualità

La registrazione avrà inizio all'ora indicata sul foglio di ammissione presso ciascuna sede d'esame. Tutti i candidati dovranno risultare iscritti e presenti all'interno dell'aula d'esame quando l'esaminatore capo inizierà a leggere le istruzioni orali. **A NESSUN CANDIDATO SARÀ CONSENTITO L'ACCESSO ALLA SEDE D'ESAME DOPO CHE L'ESAMINATORE CAPO ABBA INIZIATO A LEGGERE LE ISTRUZIONI ORALI, CIRCA 30 MINUTI PRIMA DELL'INIZIO DELL'ESAME.**

Ricordarsi di portare il foglio d'ammissione

I candidati possono utilizzare il loro foglio d'ammissione (sia nel formato cartaceo che in quello elettronico) esclusivamente presso la sede d'esame indicata sul foglio stesso. I candidati verranno ammessi in aula d'esame solo se in possesso del foglio d'ammissione e di un documento di identificazione valido. Un documento di identificazione valido deve essere quello originale rilasciato dal governo che riporti la fotografia e il nome del candidato come appare sul foglio d'ammissione. I dati riportati sul documento di identificazione non devono essere scritti a mano. Tutte queste caratteristiche devono essere presenti su un unico documento di identificazione fornito. Esempi di tale documento comprendono, in modo non esaustivo, passaporto, patente di guida, carta d'identificazione militare, carta d'identità statale, carta d'immigrazione (green card) e carta d'identità nazionale. I candidati sprovvisti di un documento d'identificazione valido non potranno sostenere l'esame ma avranno diritto al rimborso degli oneri di iscrizione.

Osservanza delle regole della sede d'esame

- Ai candidati non sarà consentito l'accesso alla sede d'esame dopo l'inizio della lettura delle istruzioni orali.
- I candidati dovranno essere provvisti di diverse matite del tipo HB o n. 2 (morbide) ben temperate e di una gomma da cancellare. Matite e gomme non vengono fornite nella sede d'esame. Verrà compiuto ogni sforzo affinché la temperatura degli ambienti delle varie sedi in cui si svolgono gli esami sia il più possibile confortevole. I candidati possono vestirsi come più lo ritengono opportuno.
- Ai candidati non è consentito portare all'interno della sede d'esame materiale di consultazione, fogli bianchi, blocchi note o dizionari di lingua.
- Ai candidati non è consentito l'uso della calcolatrice in sede d'esame.
- Ai candidati non è consentito portare con sé in sede d'esame alcun tipo di apparecchio di comunicazione (cellulari, PDA, Blackberry®, ecc.). **Se un candidato viene visto durante la sessione di esame con uno di questi articoli, il suo esame verrà invalidato e gli sarà chiesto di lasciare immediatamente la sede d'esame.**
- Non è consentito l'accesso di visitatori all'interno della sede d'esame.
- Non è consentito introdurre nella sede d'esame cibo o bevande. Nessun cibo o bevanda è ammesso nel luogo del test (salvo precedente autorizzazione di ISACA).

Cattiva condotta

I candidati che sono scoperti colpevoli di cattiva condotta – come dare o ricevere assistenza; utilizzare appunti, carta o altri aiuti; cercare di sostenere l'esame per qualcun altro; usare qualunque tipo di dispositivo di comunicazione, incluso telefoni cellulari, durante lo svolgimento dell'esame; oppure portare via il libretto d'esame, il foglio delle risposte o appunti dall'aula del test – sarà squalificato e passabile di azione legale. I candidati che lascino l'area del test senza autorizzazione o accompagnamento di un supervisore non saranno ammessi di nuovo nell'aula del test e saranno squalificati. L'agenzia esaminatrice riporterà tali irregolarità alla Commissione di Certificazione CISA di ISACA.

La normativa completa sugli articoli di proprietà personale è disponibile sul sito www.isaca.org/cisabelongings. Né ISACA né i suoi esecutori degli esami si assumono responsabilità per gli oggetti personali dei candidati.

Prestare attenzione al completamento del foglio risposte

- Prima di dare inizio all'esame, l'esaminatore capo della sede d'esame leggerà a voce alta le istruzioni per l'inserimento sul foglio risposte dei dati identificativi dei candidati. Il numero identificativo del candidato, così come appare sul foglio d'ammissione, e ogni altra informazione richiesta devono essere inserite correttamente per evitare il rischio di ritardi o errori nella comunicazione dei risultati.
- Viene messo a disposizione un sorvegliante che parla la lingua principale utilizzata in ogni sede d'esame. Se un candidato intende sostenere l'esame in una lingua diversa da quella principale utilizzata nella sede d'esame, il sorvegliante potrebbe non essere in grado di esprimersi nella lingua scelta dal candidato. Tuttavia, saranno disponibili istruzioni scritte nella lingua d'esame prescelta.
- Si raccomanda ai candidati di leggere attentamente tutte le istruzioni e di comprenderne il significato prima di cercare di rispondere alle domande. I candidati che saltino la lettura delle istruzioni o che le leggano frettolosamente, potrebbero lasciarsi sfuggire importanti informazioni e perdere punteggio.
- Tutte le risposte devono essere segnate sul foglio risposte all'interno del cerchietto appropriato. I candidati devono prestare attenzione a non marcare più di una risposta per ogni domanda e assicurarsi di rispondere sulla riga giusta del foglio risposte. In caso di correzione di una risposta, si raccomanda al candidato di cancellare completamente la risposta sbagliata prima di marcare una nuova.
- Si deve fornire una risposta a tutte le domande. **Non è prevista sottrazione di punteggio per le risposte sbagliate. La votazione è basata unicamente sul numero di risposte esatte fornite; pertanto si raccomanda di non lasciare alcuna domanda priva di risposta.**
- Una volta completato l'esame, i candidati devono consegnare il foglio risposte e il libretto d'esame.

Gestione del tempo

- L'esame, della durata di quattro ore, consente poco più di un minuto di tempo per ogni risposta. Si consiglia dunque ai candidati di gestire bene il tempo a disposizione per completare l'intero esame. I candidati devono completare in media 50 domande all'ora.
- Si raccomanda ai candidati di segnare immediatamente le proprie risposte sul relativo foglio. **Una volta trascorso il tempo consentito per l'esame, non ne verrà concesso altro per ricopiare o registrare risposte eventualmente segnate dal candidato sul libretto d'esame.**

Condotta corretta

- Per garantire la sicurezza dell'esame e conservare la validità dei punteggi, i candidati sono invitati a firmare il foglio risposte.

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

- La Commissione di certificazione CISA si riserva il diritto di escludere dall'esame qualsiasi candidato responsabile di condotta scorretta o violazione delle regole d'esame, come il dare o ricevere assistenza, l'avvalersi di appunti, di scritti o di altri aiuti, cercare di sostenere l'esame al posto di un altro candidato, portare via materiale d'esame o appunti dalla sede d'esame. L'agenzia esaminatrice fornirà alla Commissione di certificazione CISA rapporti dettagliati su tali irregolarità, per un esame della questione e per l'assunzione di decisioni in merito.

Cause di esclusione o squalificazione

- Accesso non autorizzato alla sede d'esame.
- Il candidato crea turbativa o dà/riceve aiuto.
- Il candidato cerca di portare via materiale d'esame o appunti dalla sede d'esame.
- Il candidato sostiene l'esame al posto di un altro candidato.
- Il candidato introduce nella sede d'esame materiale non autorizzato.
- Possesso da parte del candidato di qualsivoglia apparecchio di comunicazione (es. cellulari, palmari, BlackBerry®) durante lo svolgimento dell'esame.
- Abbandono non autorizzato del luogo del test da parte del candidato.

Se i candidati sono sorpresi con qualsivoglia apparecchio di comunicazione (es. telefono cellulare, palmari, BlackBerry®) durante la somministrazione dell'esame, il loro esame sarà invalidato e gli sarà richiesto di abbandonare immediatamente il luogo del test.

Punteggio dell'esame CISA

L'esame CISA consiste in 200 domande a scelta multipla. I risultati dei candidati vengono espressi con il sistema del punteggio pesato. Il punteggio pesato è la conversione del punteggio lordo realizzato dal candidato in un esame, tradotto in una scala convenzionale. ISACA riporta i punteggi utilizzando una scala convenzionale che va da 200 a 800. Ad esempio, un punteggio pesato di 800 rappresenta un punteggio perfetto corrispondente alla totalità di risposte corrette; un punteggio pesato di 200 è invece il più basso totalizzabile, corrispondente solo a un ristretto numero di risposte corrette. Per superare l'esame, un candidato deve totalizzare un punteggio da 450 in su. Il punteggio di 450 è la rappresentazione coerente di uno standard minimo di conoscenza, secondo la definizione della Commissione di certificazione CISA. I candidati che conseguono il punteggio minimo possono presentare domanda di certificazione soltanto se hanno soddisfatto tutti gli altri requisiti.

L'esame CISA contiene alcune domande che sono incluse esclusivamente a scopo di ricerca e analisi. Tali domande non vengono identificate separatamente e non vengono valutate nel calcolo del punteggio finale.

I risultati vengono spediti per posta ai candidati circa 8 settimane dopo la data dell'esame. Inoltre, con il consenso del candidato ottenuto durante il processo di registrazione, il candidato verrà informato, tramite e-mail, del punteggio conseguito e del superamento o meno dell'esame. La comunicazione tramite e-mail viene inviata soltanto all'indirizzo elettronico che si trova nel profilo del candidato alla data della comunicazione iniziale dei risultati. Per assicurare la riservatezza dei risultati, questi non vengono comunicati per fax o per telefono. Per evitare che la comunicazione tramite e-mail finisca nelle cartelle degli spam, i candidati sono pregati di inserire l'indirizzo *exam@isaca.org* nella lista bianca o lista dei mittenti verificati, o nella propria rubrica.

I candidati riceveranno comunicazione dei risultati, comprendente i punteggi parziali ottenuti per ciascun argomento. I candidati che superano l'esame riceveranno, assieme alla comunicazione dei risultati, dettagli sulle modalità per richiedere la certificazione CISA.

Per coloro che non superano l'esame, conoscere i punteggi parziali può rivelarsi utile a individuare gli argomenti che necessitano di ulteriore approfondimento prima di tornare a sostenere l'esame. I candidati che non superano l'esame tengano presente che il punteggio totale pesato non risulta né dal calcolo della media semplice né dal calcolo della media ponderata dei punteggi parziali.

I candidati che ricevono un risultato negativo hanno facoltà di richiedere un conteggio manuale dei punti dei propri fogli risposte. Tale procedura esclude il rischio che segni casuali, risposte multiple o altri fattori, possano aver interferito con il conteggio elettronico. Tuttavia, i candidati tengano presente che tutti i risultati vengono sottoposti a svariati controlli di qualità prima di essere comunicati; pertanto, è altamente improbabile che nuovi conteggi si traducano in una modifica del risultato. Eventuali richieste di conteggio manuale devono essere presentate per iscritto al reparto di certificazione entro i 90 giorni successivi alla comunicazione dei risultati. Le richieste di conteggio manuale pervenute dopo tale scadenza non verranno prese in esame. Tutte le richieste devono essere corredate dal nome del candidato, dal numero identificativo dell'esame e dal recapito postale. Ogni richiesta deve essere accompagnata dal versamento di un contributo pari a \$ USA 75.

Tipologia di domande dell'esame CISA

Le domande dell'esame CISA sono concepite con l'intento di valutare ed esaminare le conoscenze pratiche, nonché l'applicazione di concetti e standard generali. Tutte le domande sono concepite per avere un'unica risposta ideale.

Ogni domanda CISA si compone di un tema (domanda) e di quattro opzioni (risposte a scelta). Il candidato deve scegliere fra le opzioni la risposta migliore o la più corretta. Il tema può presentarsi sotto forma di domanda o di affermazione incompleta. In alcune domande può essere compresa la presentazione di un caso. Tali domande generalmente prevedono la descrizione di una situazione, rispetto alla quale il candidato è chiamato a rispondere a due o più domande sulla base delle informazioni fornite. Si raccomanda ai candidati di leggere attentamente le domande. In alcune domande dell'esame CISA il candidato è chiamato a scegliere la risposta più appropriata sulla base di qualificatori, come ad esempio **ESTREMAMENTE** probabile o **MIGLIORE**. In ogni caso, il candidato deve leggere attentamente la domanda, escludere le risposte che ritiene scorrette e quindi scegliere la migliore risposta possibile. Esempi di domande proposte nell'esame CISA sono disponibili sul sito www.isaca.org/cisaassessment.

Domanda di Certificazione CISA

Superare l'esame non equivale a ottenere la certificazione CISA. Una volta superato l'esame CISA, il candidato ha cinque anni di tempo dalla data dell'esame

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

per richiedere la certificazione. I candidati che superano l'esame devono completare la loro domanda di certificazione e permettere la verifica della loro esperienza professionale, utilizzando i moduli previsti contenuti nella domanda. **I candidati non ottengono la certificazione, né possono fregiarsi della relativa qualifica CISA, finché la domanda completa non sia stata recepita e approvata.** Tenere presente che le decisioni relative alle domande di certificazione non sono definitive in quanto è previsto un processo di appello per le domande di certificazione respinte. Le richieste di informazioni in merito alle domande di certificazione respinte possono essere inviate a certification@isaca.org. Una volta ottenuta la certificazione, il neo-designato CISA riceverà un certificato e la spilla di certificazione CISA. Al momento della domanda, i soggetti riconoscono inoltre che CISA si riserva il diritto, ma non assume alcun obbligo, di pubblicare o diffondere altrimenti informazioni circa la loro qualifica CISA. La Domanda di Certificazione CISA deve essere accompagnata da un supplemento amministrativo di 50 USD.

Requisiti per il conseguimento della prima Certificazione CISA

La certificazione CISA viene conferita per la prima volta a coloro che abbiano superato l'esame CISA e soddisfino i requisiti di esperienza professionale riportati di seguito.

Per la certificazione, si richiede un minimo di cinque anni di esperienza professionale nel campo dell'audit, del controllo e dell'assurance di sistemi informatici (SI). Forme di sostituzione o deroga a tale periodo di esperienza professionale sono previste nei seguenti termini:

- Un massimo di un anno di esperienza nel campo dei sistemi informatici o di un anno nel campo dell'audit non informatico, possono sostituire un anno di esperienza.
- 60 o 120 ore di crediti universitari semestrali (l'equivalente di una laurea di primo o secondo livello) possono sostituire rispettivamente uno o due anni di esperienza, senza il vecchio limite di 10 anni. Anche in caso di conseguimento di più titoli di laurea, può essere riscattato un massimo di due anni di esperienza.
- Una laurea quadriennale o un master presso una università che si attenga al programma didattico sponsorizzato da ISACA può essere sostitutivo di un anno di esperienza. L'elenco di tali istituti è pubblicato sul sito www.isaca.org/modeluniversities. Coloro che abbiano già sostituito tre anni di esperienza con i propri titoli scolastici non possono ricorrere a questa opzione.
- Un master in sicurezza o in tecnologie informatiche conseguito presso un'università accreditata può essere sostitutivo di un anno di esperienza.

Eccezione: Un biennio di attività come docente universitario a tempo pieno in un ambito attinente (ad es. informatica, contabilità, auditing dei sistemi informatici) può sostituire un anno di esperienza.

L'esperienza professionale deve essere stata acquisita nei 10 anni precedenti la data di domanda di certificazione CISA o entro cinque anni dalla data di superamento iniziale dell'esame. Se una completa domanda di certificazione CISA non viene presentata entro cinque anni dalla data di superamento dell'esame, l'esame dovrà essere nuovamente sostenuto e passato.

È importante sottolineare come molti decidano di sostenere l'esame CISA prima di aver soddisfatto i requisiti di esperienza professionale. Tale prassi è accettabile e incoraggiata, sebbene la certificazione CISA non possa essere conseguita finché non vi sia il pieno soddisfacimento di tutti i requisiti.

Requisiti per il mantenimento della Certificazione CISA

Per poter conservare la certificazione, i detentori di certificazione CISA devono essere in possesso dei seguenti requisiti:

- Conseguire e segnalare un minimo annuo di 20 ore di programma periodico di aggiornamento (CPE, Continuing Professional Education) e conseguire e segnalare un minimo di 120 ore di CPE per un periodo di reporting triennale. Per maggiori informazioni, consultare le norme CPE di CISA all'indirizzo www.isaca.org/cisacpepolicy.
- Recapitare l'intera quota CPE annuale alla sede internazionale di ISACA.
- Rispondere e presentare la necessaria documentazione relativa alle attività CPE a sostegno delle ore indicate, se si viene selezionati per un audit annuale.
- Attenersi al codice etico professionale ISACA.

La mancata osservanza di queste disposizioni ha come conseguenza la revoca della certificazione CISA. Tutti i certificati sono di proprietà di ISACA. Se una persona ottiene l'approvazione alla certificazione, ma successivamente questa viene revocata, la persona è tenuta a distruggere il certificato.

Codice etico professionale ISACA

ISACA ha stabilito questo Codice etico professionale come guida per la condotta professionale e personale dei membri dell'associazione e/o i detentori di certificazione. La mancata osservanza del Codice etico professionale può comportare un'indagine nel comportamento di un membro e/o di un detentore della certificazione e, in ultima analisi, all'adozione di provvedimenti disciplinari. Il codice etico professionale ISACA può essere visionato online su www.isaca.org/ethics.

Revoca della Certificazione CISA

Il Comitato di Certificazione CISA può, a propria discrezione dopo debita e approfondita considerazione, revocare la certificazione CISA di una persona per una o più delle seguenti ragioni:

- Mancata osservanza delle norme CPE di CISA
- Violazione di una o più clausole del codice etico professionale ISACA
- Falsificazione di informazioni importanti o deliberata omissione a fornirle
- Dichiarazione deliberatamente errata di un fatto materiale
- Coinvolgimento diretto o indiretto in azioni disoneste, non autorizzate o indebite in qualsiasi momento in relazione all'esame o al processo di certificazione CISA

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

Descrizione delle aree di prassi professionale Compiti e enunciati di conoscenza CISA

| ARGOMENTO (settore) |
|--|
| 1. Processo di audit dei sistemi informatici — Fornire servizi di IT audit secondo gli standard, le linee guida e le best practice IT, per assistere l'organizzazione nel garantire la protezione ed il controllo dei sistemi informativi. |
| Compiti |
| T1.1 Sviluppare e mettere in atto una strategia di IT audit basata sul rischio per l'organizzazione, in ottemperanza con gli standard It, per garantire che le aree chiave siano comprese. |
| T1.2 Pianificare audit specifici per garantire che i Sistemi Informativi siano protetti controllati e generino valore aggiunto per l'organizzazione. |
| T1.3 Condurre gli audit nel rispetto di Standard di IT Audit per conseguire gli obiettivi di audit pianificati. |
| T1.4 Comunicare i risultati di audit ed effettuare raccomandazioni ai principali interessati per condividere le evidenze e gli effettivi cambiamenti ove necessario. |
| T1.5 Condurre follow up o preparare report di sintesi per garantire che le appropriate azioni siano state prese in considerazione dal Management con tempistiche adeguate. |
| Enunciati di Conoscenza |
| KS1.1 Conoscenza degli standard di IT Audit e Assurance, Linee Guida , Tools, procedure tecniche e codice di etica professionale IS dell'ISACA, compreso altri standard se applicabili. |
| KS1.2 Conoscenza di concetti di Risk Assessment , delle prassi e tecniche di auditing. |
| KS1.3 Conoscenza degli obiettivi di controllo e dei controlli in relazione ai sistemi informativi. |
| KS1.4 Conoscenza delle modalita' di pianificazione degli audit e di tecniche di audit in ambito project management compresi i follow up. |
| KS1.5 Conoscenza dei fondamentali processi di business (per esempio fornitori, paghe , contabilita', ciclo passivo , ciclo attivo) che comprendano una rilevanza in ambito It. |
| KS1.6 Conoscenza della applicabilità delle leggi e regolamenti che impattano sul perimetro di raccolta delle evidenze e conservazione delle stesse e sulla frequenza degli audit. |
| KS1.7 Conoscenza delle tecniche di raccolta delle evidenze (i.e. osservazione, domande, ispezioni interviste , analisi dei dati) |
| KS1.8 Conoscenza di differenti tecniche di campionamento. |
| KS1.9 Conoscenza di tecniche di reportistica e comunicazione (i.e. facilitazione, negoziazione, risoluzione dei conflitti e tipi di strutture di report di audit). |
| KS1.10 Conoscenza delle metodologie di audit e garanzia (quality assurance). |
| 2. IT Governance e Management — Fornire assurance che la leadership necessaria, le strutture organizzative e i processi siano in esercizio contribuendo al raggiungimento degli obiettivi e supportando la strategia dell'impresa. |
| Compiti |
| T2.1 Valutare l'efficacia della struttura dell'IT Governance al fine di determinare se le decisioni, gli orientamenti e le prestazioni dei Sistemi Informativi sono in grado di supportare le strategie e gli obiettivi aziendali. |
| T2.2 Valutare la struttura organizzativa IT e la gestione delle risorse umane al fine di determinare se esse supportino adeguatamente le strategie e gli obiettivi aziendali. |
| T2.3 Valutare la strategia e gli orientamenti IT e il loro processo di sviluppo, approvazione, implementazione e manutenzione al fine di assicurare il loro allineamento con le strategie e gli obiettivi aziendali. |
| T2.4 Valutare le policy, gli standard e le procedure aziendali in ambito IT ed i relativi processi di sviluppo, approvazione, implementazione e manutenzione al fine di determinare se supportino adeguatamente la strategia IT e se siano conformi con i requisiti di legge e di regolamento applicabili. |
| T2.5 Valutare l'adeguatezza del sistema di gestione della qualità al fine di determinare se esso supporti le strategie e gli obiettivi aziendali in maniera efficiente ed efficace. |
| T2.6 Valutare l'IT management e il monitoraggio dei controlli (i.e. monitoraggio continuo, quality assurance [QA]) in conformità con le policy, standard e le procedure aziendali. |
| T2.7 Valutare le attività di investimento, utilizzo ed allocazione delle risorse IT per assicurare l'allineamento con le strategie e gli obiettivi aziendali. |
| T2.8 Valutare le strategie e le policy per la definizione dei contratti IT e le attività di gestione di tali contratti al fine di determinare se supportino adeguatamente le strategie e gli obiettivi aziendali. |
| T2.9 Valutare le attività di risk management al fine di determinare se i rischi aziendali di natura tecnologica siano propriamente gestiti. |
| T2.10 Valutare le attività di monitoraggio e assurance al fine di determinare se il Consiglio d'Amministrazione e il management ricevano sufficienti e tempestive informazioni relative alle prestazioni dei Sistemi Informativi. |
| T2.11 Valutare il business continuity plan al fine di determinare se l'azienda è in grado di garantire la continuità delle operazioni di business essenziali durante il periodo di interruzione dei Sistemi Informativi. |

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

| ARGOMENTO (settore) |
|--|
| Enunciati di Conoscenza |
| KS2.1 Conoscenza della governance, management, sicurezza e framework di controllo in ambito IT, nonché relativi standard, linee guida e pratiche. |
| KS2.2 Conoscenza degli obiettivi delle strategie, policy, standard e procedure aziendali in ambito IT e degli elementi essenziali di ciascuno di essi. |
| KS2.3 Conoscenza della struttura organizzativa, ruoli e responsabilità relativi ai Sistemi Informativi. |
| KS2.4 Conoscenza dei processi di sviluppo, implementazione e manutenzione delle strategie, delle policy, degli standard e delle procedure IT. |
| KS2.5 Conoscenza dell'orientamento tecnologico dell'azienda, dell'architettura IT e delle loro implicazioni sulla definizione della direzione strategica di lungo termine. |
| KS2.6 Conoscenza delle leggi, dei regolamenti e degli standard rilevanti nel mercato di riferimento e applicabili all'azienda. |
| KS2.7 Conoscenza dei sistemi di gestione della qualità. |
| KS2.8 Conoscenza dell'utilizzo di modelli di maturità. |
| KS2.9 Conoscenza dei modelli di miglioramento dei processi. |
| KS2.10 Conoscenza delle attività di investimento e allocazione delle risorse IT, incluse le pratiche e i criteri di prioritizzazione (i.e. portfolio management, value management, project management). |
| KS2.11 Conoscenza delle pratiche di selezione dei fornitori IT, di gestione dei contratti e delle relazioni, nonché dei processi di monitoraggio delle prestazioni, incluse le relazioni con outsource terzi. |
| KS2.12 Conoscenza dell'enterprise risk management. |
| KS2.13 Conoscenza dell'analisi d'impatto sul business (BIA) nell'ambito del business continuity planning (BCP). |
| KS2.14 Conoscenza delle pratiche di gestione delle risorse umane adibite ai servizi dei Sistemi Informativi nell'ambito del business continuity plan dell'azienda. |
| KS2.15 Conoscenza della gestione delle risorse umane (personale) IT |
| KS2.16 Conoscenza degli standard e delle procedure per lo sviluppo e la manutenzione del business continuity plan (BCP) e delle metodologie di test |
| 3. Acquisizione, sviluppo e implementazione dei sistemi informatici — Fornire assurance che le prassi di gestione per l'acquisizione, sviluppo, il test e l'implementazione di sistemi informativi siano allineati alle strategie e agli obiettivi dell'Organizzazione. |
| Compiti |
| T3.1 Valutare il business case per le proposte di investimento in acquisizione, sviluppo, manutenzione e conseguente dismissione di un sistema informativo per determinare se soddisfa gli obiettivi di business dell'organizzazione. |
| T3.2 Valutare le pratiche e i controlli di gestione del progetto per determinare se i requisiti di business siano conseguiti in modo economico ed efficace, salvaguardando l'organizzazione dai rischi. |
| T3.3 Eseguire riesami per assicurare che un progetto si sviluppi in accordo ai piani di progetto, sia corredato di adeguata documentazione e che il reporting sullo stato del progetto sia accurato. |
| T3.4 Valutare i meccanismi di controllo proposti per i sistemi e le infrastrutture durante le fasi dei requisiti, acquisizione, sviluppo e collaudo per la conformità con le policy, gli standards, le procedure e altri requisiti esterni dell'organizzazione. |
| T3.5 Valutare la semplicità del sistema informativo per l'implementazione e la migrazione in ambiente di produzione per determinare se gli insiemi di documenti di progetto, i controlli e i requisiti dell'organizzazione siano soddisfatti. |
| T3.6 Eseguire riesami di post-implementazione dei sistemi per determinare che i documenti di progetto, i controlli e i requisiti dell'organizzazione siano soddisfatti. |
| Enunciati di Conoscenza |
| KS3.1 Conoscenza delle prassi o pratiche di realizzazione di benefici (ad esempio, studi di fattibilità, business case, costo totale di proprietà o possesso [TCO]. ROI). |
| KS3.2 Conoscenza dei meccanismi di governo o gestione dei progetti (ad esempio, comitati guida, commissioni di controllo e vigilanza dei progetti e l'ufficio di gestione dei progetti). |
| KS3.3 Conoscenza di strutture e metodologie di controllo di gestione dei progetti. |
| KS3.4 Conoscenza delle prassi o pratiche di gestione dei rischi applicabili ai progetti. |
| KS3.5 Conoscenza di architetture IT relative ai dati, applicativi e tecnologie (ad esempio, applicativi distribuiti, applicativi basati sul web, servizi basati sul web, applicativi a n livelli). |
| KS3.6 Conoscenza di prassi su come si gestiscono le acquisizioni (ad esempio, la valutazione dei fornitori, la gestione dei fornitori, le garanzie di disponibilità 'escrow'). |
| KS3.7 Conoscenza di analisi dei requisiti e pratiche di gestione (ad esempio, verifica dei requisiti, tracciabilità, analisi di scostamento, gestione delle vulnerabilità, requisiti di sicurezza). |
| KS3.8 Conoscenza di criteri di successo di progetti e rischi. |
| KS3.9 Conoscenza di obiettivi e tecniche di controllo che assicurano la completezza, accuratezza, validità e l'autorizzazione di transazioni e dati. |

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

| ARGOMENTO (settore) |
|--|
| 3. Acquisizione, Sviluppo e Implementazione dei Sistemi Informativi (continua) |
| KS3.10 Conoscenze delle metodologie e strumenti per lo sviluppo di sistemi includendo i punti di forza e debolezza (per esempio, pratiche di sviluppo semplificato 'agile', prototipazione, sviluppo rapido di applicativi [RAD], tecniche di disegno orientate agli oggetti). |
| KS3.11 Conoscenza di pratiche e metodologie per il collaudo 'testing' relative allo sviluppo di sistemi informativi. |
| KS3.12 Conoscenza di gestione di configurazioni e delle versioni relativi allo sviluppo di sistemi informativi. |
| KS3.13 Conoscenza di sistemi di migrazione, di pratiche di sviluppo infrastrutture, strumenti, procedure e tecniche di conversione dati. |
| KS3.14 Conoscenza pratiche e metodi delle revisioni di post-implementazione degli obiettivi (ad esempio, chiusura di progetti, implementazione di controlli, ottenimento di benefici, misura delle prestazioni). |
| 4. Operazioni, mantenimento e supporto dei servizi informatici — Fornire assurance che i processi di esercizio dei sistemi informativi, manutenzione e supporto siano allineati alle strategie e agli obiettivi dell'Organizzazione. |
| Compiti |
| T4.1 Condurre revisioni periodiche dei sistemi informativi per verificare l'attinenza di quanto impostato con gli obiettivi dell'organizzazione. |
| T4.2 Valutare le prassi di Service Level Management per verificare se i livelli di servizio forniti dai service provider interni ed esterni sono definiti e gestiti. |
| T4.3 Valutare le prassi di gestione delle terze parti per verificare se i livelli di controllo attesi dall'organizzazione sono seguiti dal provider. |
| T4.4 Valutare le operazioni e le procedure dell'utente finale per verificare se i processi schedulati e non schedulati sono gestiti in modo completo. |
| T4.5 Valutare i processi di manutenzione dei sistemi informativi per verificare se sono controllati in modo efficace e se continuano a supportare gli obiettivi dell'organizzazione. |
| T4.6 Valutare le pratiche di amministrazione dei dati per verificare l'integrità e l'ottimizzazione delle basi dati. |
| T4.7 Valutare l'utilizzo di strumenti e tecniche di monitoraggio dell'adeguatezza della capacità elaborativa e delle prestazioni dei servizi IT per verificare se gli stessi corrispondono agli obiettivi dell'organizzazione. |
| T4.8 Valutare le prassi di gestione degli incidenti e dei problemi per verificare se gli incidenti, i problemi o gli errori siano registrati, analizzati e risolti tempestivamente. |
| T4.9 Valutare le prassi di gestione delle modifiche della configurazione e le prassi di rilascio per verificare se le modifiche schedulate e non schedulate apportate all'ambiente di produzione dell'organizzazione siano adeguatamente controllate e documentate. |
| T4.10 Valutare l'adeguatezza delle forniture di backup e restore per verificare la disponibilità delle informazioni richieste per ripristinare i processi. |
| T4.11 Valutare il piano di disaster recovery per verificare se consente il ripristino dei processi IT nell'eventualità di un disastro. |
| Enunciati di Conoscenza |
| KS4.1 Conoscenza delle prassi di gestione dei livelli di servizio e delle componenti comprese negli accordi sui livelli di servizio; |
| KS4.2 Conoscenza delle tecniche per monitorare la conformità delle terze parti con i controlli interni all'organizzazione; |
| KS4.3 Conoscenza delle attività e delle procedure dell'utente finale per gestire i processi schedulati e non schedulati; |
| KS4.4 Conoscenza dei concetti tecnologici correlati alle componenti hardware, di rete, di software di sistema e dei sistemi di gestione della base dati; |
| KS4.5 Conoscenza delle tecniche di controllo che assicurano l'integrità delle interfacce di sistema; |
| KS4.6 Conoscenza delle licenze software e delle prassi di gestione degli inventari software; |
| KS4.7 Conoscenza delle tecniche e degli strumenti di resilienza dei sistemi (ad es. hardware fault-tolerant, eliminazione dei punti di guasto singolo, clustering); |
| KS4.8 Conoscenza delle tecniche di pianificazione e monitoraggio delle capacità elaborative; |
| KS4.9 Conoscenza delle prassi di gestione degli incidenti/problemi (ovvero help desk, procedure di escalation e controllo) |
| KS4.10 Conoscenza dei processi, strumenti e tecniche di monitoraggio delle prestazioni dei sistemi (ad es. analizzatori di rete, report di utilizzo dei sistemi, bilanciamento dei carichi); |
| KS4.11 Conoscenza delle prassi di gestione degli incidenti e dei problemi (ad es. help desk, procedure per aumentare la classe di rilevanza -escalation-dell'errore, tracciamento); |
| KS4.12 Conoscenza dei processi di gestione delle modifiche pianificate e di quelle d'emergenza apportate ai sistemi di produzione e/o alle infrastrutture ivi incluse le prassi di gestione delle modifiche, della configurazione, del rilascio e delle correzioni; |
| KS4.13 Conoscenza dei processi e delle prassi di salvataggio, immagazzinamento, conservazione e ripristino dei dati; |
| KS4.14 Conoscenza delle questioni riguardanti i regolamenti, le leggi, le norme contrattuali, l'ambito assicurativo per quanto correlato al disaster recovery; |
| KS4.15 Conoscenza dell'analisi d'impatto sul business (BIA) correlata al Disaster Recovery Planning; |
| KS4.16 Conoscenza sullo sviluppo e la manutenzione dei piani di disaster recovery; |
| KS4.17 Conoscenza delle tipologie di siti alternativi di centri di elaborazione e di metodi usati per monitorare gli accordi contrattuali (cioè siti "caldi", "tiepidi", "freddi"); |

Guida del candidato all'esame e alla certificazione CISA® (Candidate's Guide to the CISA Exam and Certification)

| |
|--|
| ARGOMENTO (settore) |
| 4. Supporto, Manutenzione e Esercizio dei Sistemi Informativi (continua) |
| KS4.18 Conoscenze dei processi usati per attivare i piani di disaster recovery; |
| KS4.19. Conoscenze degli approcci e metodi di test del disaster recovery. |
| 5. Protezione delle risorse informatiche — Fornire assurance che l'architettura di sicurezza (policy, standard, procedure e controlli) garantisca la riservatezza, integrità e disponibilità delle risorse informative. |
| Dichiarazioni sulla pratica |
| T5.1 Valutare le politiche di sicurezza delle informazioni, standard e procedure in termini di completezza e allineamento con le pratiche generalmente accettate. |
| T5.2 Valutare la progettazione, realizzazione e monitoraggio dei sistemi e dei controlli di sicurezza logica per verificare l'integrità, la riservatezza e la disponibilità delle informazioni. |
| T5.3 Valutare la progettazione, realizzazione e monitoraggio dei processi di classificazione dei dati e delle procedure per l'allineamento con le politiche dell'organizzazione, norme, procedure e ai requisiti di esterni. |
| T5.4 Valutare la progettazione, realizzazione e il controllo degli accessi fisici e i controlli ambientali per determinare se le risorse informative sono adeguatamente salvaguardate. |
| T5.5 Valutare i processi e le procedure utilizzate per l'archiviazione, il recupero, il trasporto e la cessione di asset inerenti le informazioni (ad esempio, i supporti di backup, lo storage offsite, la copia / stampa di dati e supporti formato elettronico) per determinare se le risorse informative sono adeguatamente salvaguardate. |
| Enunciati di Conoscenza |
| KS5.1 Conoscenza delle tecniche per la progettazione, realizzazione e monitoraggio dei controlli di sicurezza, compresi i programmi di sensibilizzazione alla sicurezza |
| KS5.2 Conoscenza dei processi relativi al monitoraggio e alle risposte agli incidenti di sicurezza (ad esempio, procedure di escalation, team di risposta alle emergenze negli incident) |
| KS5.3 Conoscenza dei controlli di accesso logico per l'identificazione l'autenticazione e l'autorizzazione in ambito ristretto degli utenti alle funzioni e ai dati |
| KS5.4 Conoscenza dei controlli di sicurezza relativi a hardware, software di sistema (ad esempio, applicazioni, sistemi operativi), e sistemi di gestione di database |
| KS5.5 Conoscenza dei rischi e dei controlli connessi con la virtualizzazione dei sistemi |
| KS5.6 Conoscenza delle configurazione, gestione e manutenzione dei controlli di sicurezza di rete |
| KS5.7 Conoscenza dei dispositivi di sicurezza di rete e Internet, dei protocolli e di tecniche inerenti |
| KS5.8 Conoscenza dei metodi e delle tecniche di attacco alle informazioni |
| KS5.9 Conoscenza di strumenti di rilevamento e tecniche di controllo (ad esempio, il malware, il rilevamento di virus, spyware) |
| KS5.10 Conoscenza delle tecniche di test di sicurezza (ad esempio, test di intrusione, la scansione delle vulnerabilità) |
| KS5.11 Conoscenza dei rischi e dei controlli associati alla perdita dei dati |
| KS5.12 Conoscenza delle tecniche di crittografia correlate |
| KS5.13 Conoscenza della infrastruttura a chiave pubblica (PKI) e delle componenti tecniche di firma digitale. |
| KS5.14 Conoscenza dei rischi e dei controlli connessi con il peer-to-peer, instant messaging, e le tecnologie web-based (ad esempio, social network, forum, blog) |
| KS5.15 Conoscenza dei controlli e dei rischi associati all'utilizzo di dispositivi mobili e wireless |
| KS5.16 Conoscenza della sicurezza delle comunicazioni vocali (ad esempio, PBX, VoIP) |
| KS5.17 Conoscenza delle tecniche di conservazione delle prove e dei processi seguiti nelle indagini forensi (ad esempio, IT, processi, catena logica della custodia) |
| KS5.18 Conoscenza delle norme di classificazione dei dati e delle procedure a supporto |
| KS5.19 Conoscenza dei controlli sugli accessi fisici per l'identificazione l'autenticazione e l'autorizzazione in modalità ristretta degli utenti agli impianti. |
| KS5.20 Conoscenza dei dispositivi di protezione ambientale e delle pratiche di supporto |
| KS5.21 Conoscenza dei processi e delle procedure utilizzate per archiviare, recuperare, trasportare e cedere asset inerenti informazioni riservate. |



Prepara l'esame CISA 2012

Materiale per la preparazione all'esame CISA 2012 e per lo sviluppo professionale

I candidati che affrontano con successo l'esame Certified Information Systems Auditor® (CISA®) hanno un piano di studi organizzato. Per supportare i candidati nello sviluppo di un piano di studi vincente ISACA® offre ai candidati materiale di studio e corsi di preparazione. Questi includono:

Materiale di studio

- *Manuale Tecnico CISA® 2012*
- *Manuale di esercitazione CISA® 2011: Domande, risposte e spiegazioni*
- *Manuale di esercitazione CISA®: Domande, risposte e spiegazioni - Supplemento 2011*
- *Manuale di esercitazione CISA®: Domande, risposte e spiegazioni - Supplemento 2012*
- CISA® Practice Question Database v12

Per ordinarlo: www.isaca.org/cisabooks.

Corsi di preparazione

- Corsi di preparazione organizzati dai capitoli locali (www.isaca.org/cisareview)
- CISA® Online Review Course (www.isaca.org/elearning)

