



CERTIFIED INFORMATION SYSTEMS AUDITOR®

Handbuch für Kandidaten für das CISA®-Examen
und die CISA®-Zertifizierung 2012

CISA-Examen 2012 – Wichtige Termine

Examenstermin: 9. Juni 2012

Frühanmeldung:	8. Februar 2012
Anmeldeschluss:	4. April 2012
Änderung der Anmeldung zum Examen:	14. bis 20. April 50 USD Bearbeitungsgebühr. Nach dem 20. April 2012 sind keine Änderungen mehr möglich.
Rückerstattung:	Bis 13. April 2012 100 USD Bearbeitungsgebühr. Nach diesem Datum ist keine Rückerstattung mehr möglich.
Verschiebung:	Für Anträge auf Verschiebung, die bis zum 20. April 2012 eingehen, wird eine Bearbeitungsgebühr von 50 USD erhoben. Für Anträge auf Verschiebung, die zwischen 21. April und 24. Mai 2012 eingehen, wird eine Bearbeitungsgebühr von 100 USD erhoben. Nach dem 24. Mai 2012 werden keine Verschiebungsanträge mehr angenommen.

Examenstermin: 8. Dezember 2012

Frühanmeldung:	15. August 2012
Anmeldeschluss:	3. Oktober 2012
Änderung der Anmeldung zum Examen:	6. bis 12. Oktober 50 USD Bearbeitungsgebühr. Nach dem 12. Oktober 2012 sind keine Änderungen mehr möglich.
Rückerstattung:	Bis 5. Oktober 2012 100 USD Bearbeitungsgebühr. Nach diesem Datum ist keine Rückerstattung mehr möglich.
Verschiebung:	Für Anträge auf Verschiebung, die bis zum 12. Oktober 2012 eingehen, wird eine Bearbeitungsgebühr von 50 USD erhoben. Für Anträge auf Verschiebung, die zwischen 13. Oktober und 21. November 2012 eingehen, wird eine Bearbeitungsgebühr von 100 USD erhoben. Nach dem 21. November 2012 werden keine Verschiebungsanträge mehr angenommen.

Alle Termine orientieren sich an Chicago, Bundesstaat Illinois, USA, 17.00 Uhr Zentralzeit (MEZ - 7 Std.).

Handbuch für Kandidaten für das CISA®-Examen und die CISA®-Zertifizierung 2012
Printed in the USA.

Inhalt

Übersicht.....	3
CISA-Programm gemäß ISO/IEC 17024:2003 erneut akkreditiert	3
Das CISA-Examen	3
Vorbereitung auf das CISA-Examen	3
Ablauf des CISA-Examens	4
Bewertung des CISA-Examens	6
Arten der Fragen im CISA-Examen.....	6
Bewerbung für die CISA-Zertifizierung	6
Voraussetzungen für die CISA-Erstzertifizierung	7
Voraussetzungen zur Aufrechterhaltung der CISA-Zertifizierung	7
ISACA-Berufsehrenkodex.....	7
Entzug der CISA-Zertifizierung	7
Tätigkeitsfelder und Fachkenntnisse eines CISA	8

Über ISACA®

ISACA (www.isaca.org) ist mit mehr als 95 000 Mitgliedern in über 160 Ländern ein führender internationaler Anbieter für Wissensvermittlung, Zertifizierung, Förderung und Bildung in den Bereichen Prüfung und Sicherheit von Informationssystemen (IS), IT-Governance und -Management sowie IT-bezogenen Risiken und Einhaltung von Richtlinien (Compliance). Der 1969 gegründete Interessenverband veranstaltet internationale Konferenzen, ist Herausgeber des *ISACA® Journal* und entwickelt internationale Standards zur Prüfung und Steuerung von Informationssystemen, mit deren Hilfe Mitglieder dafür sorgen können, dass Informationssysteme vertrauenswürdig und profitabel werden. Darüber hinaus fördert und prüft ISACA IT-Kenntnisse und -Fähigkeiten und verleiht die folgenden international anerkannten Berufstitel: Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) und Certified in Risk and Information Systems Control™ (CRISC™). ISACA aktualisiert fortlaufend das Framework COBIT®, das IT-Fachleute und Manager dabei unterstützt, ihre Verantwortung in den Bereichen IT-Governance und Management zu erfüllen und den Wert des Unternehmens zu steigern. Dies gilt insbesondere für die Bereiche Gewährleistung, Sicherheit, Risiko und Kontrolle.

Haftungsausschluss

Das von ISACA und dem CISA-Zertifizierungsausschuss herausgegebene *Handbuch 2012 für Kandidaten für das CISA®-Examen und die CISA®-Zertifizierung* möchte Interessenten den Weg zur CISA-Zertifizierung erleichtern. ISACA übernimmt keinerlei Gewährleistungen, dass die Anwendung dieses Handbuchs oder jeglicher anderer Publikationen den Kandidaten das Bestehen des CISA-Examens garantiert.

Rechtsvorbehalt

Copyright © 2011 ISACA. Die Vervielfältigung oder Speicherung in jeglicher Form und zu jeglichen Zweck ist nur nach der schriftlichen Genehmigung durch ISACA zulässig. Es werden keine weiteren Rechte oder Berechtigungen hinsichtlich dieses Werks gewährt. Alle Rechte vorbehalten.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008, USA
Telefon: +1.847.253.1545
Fax: +1.847.253.1443
E-Mail: exam@isaca.org
Website: www.isaca.org

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung

Übersicht

Der Maßstab für die Güte eines Zertifikationsprogramms für Fachleute ist der Wert und die Anerkennung, die das Zertifikat dem Erwerber verleiht. Das von ISACA getragene CISA-Programm (Certified Information Systems Auditor) ist seit 1978 der weltweit unter Informationssystem-Prüfungs-, -Steuerungs-, -Gewährleistungs- und -Sicherheitsexperten anerkannte Leistungsstandard.

Die von CISA geförderten und beurteilten technischen Kenntnisse und Arbeitstechniken sind die Bausteine zu beruflichem Erfolg. Ein CISA-Zertifikat belegt Ihre Kompetenz und ist eine objektive Qualifikation, die Sie gegenüber anderen auszeichnet. Aufgrund des steigenden Bedarfs an Experten zur Prüfung, Steuerung und Sicherheit von Informationssystemen ist CISA zu einem der wichtigsten Zertifikationsprogrammen für Einzelpersonen und Organisationen weltweit avanciert. Mit einem CISA-Zertifikat zeigen Sie Ihr Engagement, im Dienste der Organisation und des Berufsstandes hervorragende Leistungen zu erbringen.

CISA-Programm gemäß ISO/IEC 17024:2003 erneut akkreditiert

Das American National Standards Institute (ANSI) hat die CISA-Zertifizierung gemäß ISO/IEC 17024:2003 (Konformitätsbewertung - Allgemeine Anforderungen an Stellen, die Personen zertifizieren) erneut akkreditiert. ANSI, eine private gemeinnützige Organisation, akkreditiert andere Organisationen, um als externe Prüfer für Produkte, Systeme und Personal zu fungieren.

ISO/IEC 17024 gibt die Auflagen vor, die von Organisationen beim Zertifizieren von Personen im Hinblick auf spezifische Bestimmungen einzuhalten sind. ANSI erwartet, dass die ISO/IEC 17024 eine wichtige Rolle bei der Einrichtung einer globalen Standardisierung in der Zertifizierungsbranche, der gesteigerten Mobilität zwischen Ländern, der Verstärkung der öffentlichen Sicherheit und dem Verbraucherschutz spielen wird.

Die ANSI-Akkreditierung:

- Fördert die von den ISACA-Zertifikationen gebotene herausragende Qualifikation und Expertise
- Schützt die Integrität der Zertifikationen und bietet rechtliche Verteidigung
- Steigert das Vertrauen der Verbraucher und der breiten Öffentlichkeit in die Zertifikationen und deren Inhaber
- Fördert die grenzen- und branchenübergreifende Mobilität

Die Akkreditierung durch ANSI bedeutet, dass die ISACA-Verfahren die grundlegenden ANSI-Vorschriften bezüglich Offenheit, Ausgewogenheit, Konsens und ordnungsgemäße Verfahren erfüllen. ISACA geht davon aus, dass sich dank dieser Akkreditierung weiterhin bedeutende Möglichkeiten für CISAs und CISMs auf der ganzen Welt bieten werden.



ANSI-akkreditiertes Programm
ANGESTELLTENZERTIFIKATION
#0694
ISO/IEC 17024

Das CISA-Examen

Entwicklung/Beschreibung des CISA-Examens

Der CISA-Zertifizierungsausschuss betreut die Entwicklung des Examens und sichert die Aktualität des Inhalts. Die im CISA-Examen gestellten Fragen werden in einem aufwändigen Verfahren entwickelt, die den hohen Anspruch des Examens gewährleisten. Dazu gehört u. a. ein spezieller Unterausschuss, der die Fragen in Zusammenarbeit mit Fachautoren entwickelt und überprüft, bevor sie dem CISA-Zertifizierungsausschuss zur Prüfung vorgelegt werden.

Berufspraxis ist die Grundlage für das Examen und die erforderliche Erfahrung zur Erlangung des CISA-Zertifikats. Diese Berufspraxis wird regelmäßig aktualisiert und umfasst fünf Inhaltsbereiche (Fachgebiete). Die Fachgebiete und die Tätigkeitsfelder sowie Fachkenntnisse sind Ergebnis umfangreicher Recherche und Feedback von Fachexperten aus aller Welt.

Die Tätigkeitsfelder und Fachkenntnisse orientieren sich an den beruflichen Aufgaben eines CISA und dem dafür erforderlichen Fachwissen. Die Examenskandidaten werden auf der Grundlage ihrer praktischen Kenntnisse hinsichtlich der Durchführung dieser Aufgaben geprüft.

Die aktualisierte Berufspraxisanalyse umfasst folgende Fachgebiete und die prozentuale Gewichtung der Sachgebiete innerhalb des Examens:

- **Prüfung von Informationssystemen (14%)**
- **IT-Governance und IT-Management (14%)**
- **Anschaffung, Entwicklung und Implementierung von Informationssystemen (19%)**
- **Betrieb, Pflege/Instandhaltung und Unterstützung von Informationssystemen (23%)**
- **Schutz von Informationswerten (30%)**

Hinweis: Die Prozentangaben bei den Berufspraxisbereichen geben die schwerpunktmäßige Bedeutung bzw. den Prozentsatz der Fragen an, die bei dem Examen gestellt werden. Eine Beschreibung der Tätigkeitsfelder und Fachkenntnisse für die einzelnen Bereiche finden Sie auf den Seiten 8 bis 11.

Das Examen umfasst 200 Multiple-Choice-Fragen, dauert etwa vier Stunden und wird zweimal pro Jahr (Juni und Dezember) abgehalten. Die Kandidaten können die Prüfung in verschiedenen Sprachen ablegen. Die derzeit angebotenen Sprachen sind unter www.isaca.org/cisaterminology aufgeführt.

Vorbereitungen auf das CISA-Examen

Grundlage für die erfolgreiche Bewältigung des CISA-Examens ist ein organisierter Studienplan. Um Interessenten bei der Ausarbeitung eines erfolgreichen Studienplanes zu unterstützen, stellt ISACA den Examenskandidaten Studienhilfen und Auffrischkurse zur Verfügung. Unter www.isaca.org/cisaguide finden Sie von ISACA bereitgestelltes Material, das Sie bei der Examensvorbereitung unterstützen kann. Wir empfehlen Ihnen, frühzeitig zu bestellen, da die Auslieferung je nach Wohnort und Zollabfertigung zwischen einer und vier Wochen dauern kann. Aktuelle Versandinformationen finden Sie unter www.isaca.org/shipping.

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung



ISACA bietet auch einen CISA®-Online-Vorbereitungskurs. Der Kurs umfasst interaktive Übungen, Fallstudien, Hilfsmittel zur Überprüfung und praxisbezogene Fragen. Für weiterführende Informationen und eine Vorschau des Kurses besuchen Sie bitte www.isaca.org/elearning.

Ein umfassendes Verzeichnis des zur Examensvorbereitung empfohlenen Referenzmaterials können Sie dem *CISA Handbuch 2012* entnehmen.

Ein Verzeichnis der Akronyme, die den Kandidaten geläufig sein sollten, und ein weiteres Akronymverzeichnis, das für die Kandidaten von Interesse sein könnte, finden Sie unter www.isaca.org/cisaguide.

Als weitere Hilfe zur technischen Terminologie finden Sie ein Verzeichnis der wichtigsten technischen Begriffe auf Englisch mit Übersetzungen in andere Sprachen auf der ISACA-Website unter www.isaca.org/cisaguide.

ISACA pflegt neben einem Terminologieglossar auch spezielle Glossare für die einzelnen Zertifikationen. Diese Glossare finden Sie unter www.isaca.org/glossary.

Die ISACA bzw. der Zertifizierungsausschuss übernehmen keinerlei Zusicherungen und Gewährleistungen, dass die genannten bzw. andere vom Verband angebotene Veröffentlichungen oder Kurse den Examenskandidaten das Bestehen des Examens garantieren.

Ablauf des CISA-Examens

ISACA setzt eine international anerkannte professionelle Prüfungsagentur zur Organisation, Abwicklung und Bewertung des CISA-Examens ein.

Kandidaten, die eine Rückmeldung zum Prüfungsablauf geben möchten, können im Anschluss an die Prüfung den Fragebogen zum Prüfungsablauf ausfüllen. Dieser Fragebogen befindet sich auf der Rückseite des Prüfungshefts. Tragen Sie Ihre Antworten in die Felder P bis S im Abschnitt „Spezialcodes“ (Raster 4) auf der Vorderseite des Antwortbogens ein.

Kandidaten, die zusätzliche Anmerkungen oder Bedenken zum Prüfungsablauf, zu den Gegebenheiten am Prüfungsort oder zum Prüfungsinhalt selbst äußern möchten, können sich brieflich oder per E-Mail (exam@isaca.org) an den internationalen ISACA-Hauptsitz wenden. Derartige Anmerkungen oder Bedenken müssen bis spätestens zwei Wochen nach dem Examensdatum bei ISACA eingegangen sein und folgende Angaben enthalten: Identifikationsnummer, Prüfungsort, Prüfungsdatum und detaillierte Darstellung der fraglichen Angelegenheit. Bei der endgültigen Examensbewertung können nur Anmerkungen berücksichtigt werden, die innerhalb von zwei Wochen nach der Prüfung bei ISACA eingegangen sind.

Prüfungszulassung

Etwa zwei bis drei Wochen vor dem für das CISA-Examen angesetzten Termin erhalten die Kandidaten eine schriftliche Prüfungszulassung sowie eine E-Zulassung von ISACA. Die Examenskandidaten können auch eine Kopie der Prüfungszulassung von der Website www.isaca.org > Seite „MyISACA“ herunterladen. Auf der Prüfungszulassung sind Datum und Uhrzeit der Einschreibung, Prüfungsort, der Ablaufplan für diesen Tag und Materialien angegeben, das Sie zum CISA-Examen mitbringen müssen. Außer bei einer Änderung der Anschrift oder sonstiger Kontaktinformationen darf auf die Prüfungszulassung nicht geschrieben werden.

Wichtiger Hinweis: Sie erhalten Ihre Prüfungszulassung nur, wenn sämtliche Gebühren bezahlt wurden. Prüfungszulassungen werden per Post und per E-Mail an die uns vorliegende Postanschrift bzw. E-Mail-Adresse verschickt. Nur Kandidaten mit Prüfungszulassung und einem akzeptablem, von einer Behörde ausgestellten Ausweisdokument erhalten Einlass zur Prüfungsteilnahme. Dabei muss der Name auf der Prüfungszulassung mit dem Namen auf dem Ausweisdokument übereinstimmen. Es kann sowohl die postalisch übersandte Prüfungszulassung als auch ein Ausdruck der E-Zulassung vorgelegt werden. Wenn sich Ihre Postanschrift und/oder die E-Mail-Adresse ändert, müssen Sie Ihr Profil auf der ISACA-Website (www.isaca.org) aktualisieren oder die Änderung per E-Mail an exam@isaca.org melden.

Beachten Sie unbedingt die auf Ihrer Prüfungszulassung angegebene Uhrzeit für die Einschreibung und den Examensbeginn. NACHDEM DER PRÜFUNGSLEITER ETWA 30 MINUTEN VOR BEGINN DES EXAMENS MIT DEM VERLESEN DER ANWEISUNGEN BEGONNEN HAT, WERDEN KEINE KANDIDATEN MEHR IN DAS PRÜFUNGSZENTRUM EINGELASSEN. Kandidaten, die nach Beginn der Anweisungsverlesung eintreffen, werden nicht zum Examen zugelassen, und ihre gezahlten Examensgebühren verfallen. Die Prüfungszulassung ist nur für das darauf angegebene Prüfungszentrum gültig. Die Ausweise werden während des Examens überprüft.

Sonderabsprachen

Auf Nachfrage berücksichtigt ISACA für Kandidaten, die nachweislich behindert sind oder religiöse Regeln befolgen müssen, angemessene Sonderwünsche. Diese Kandidaten können angemessene Änderungen des Examensformats, der Präsentation, der Speisen und Getränke im Prüfungsraum und der Terminansetzung beantragen. Anträge auf Speisen oder Getränke im Prüfungsraum müssen durch ein ärztliches Attest begründet werden, **ansonsten sind Speisen und Getränke im Prüfungszentrum nicht erlaubt.** Ein entsprechender schriftlicher Antrag ist zusammen mit den entsprechenden Nachweisen bis spätestens 4. April 2012 für das Examen im Juni 2012 bzw. 3. Oktober 2012 für das Examen im Dezember 2012 bei der internationalen Hauptstelle von ISACA einzureichen.

Seien Sie pünktlich

Die Einschreibung in den einzelnen Zentren beginnt zu der Uhrzeit, die auf der Prüfungszulassung angegeben ist. Wenn der Prüfungsleiter mit der Verlesung der Anweisungen beginnt, müssen alle Kandidaten eingeschrieben sein und sich im Prüfungsraum befinden. **NACHDEM DER PRÜFUNGSLEITER ETWA 30 MINUTEN VOR BEGINN DES EXAMENS MIT DER VERLESUNG DER ANWEISUNGEN BEGONNEN HAT, WERDEN KEINE KANDIDATEN MEHR IN DAS PRÜFUNGSZENTRUM EINGELASSEN.**

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung

Denken Sie an die Prüfungszulassung

Ihre Prüfungszulassung (die E-Prüfungszulassung oder die gedruckte Prüfungszulassung) ist nur für das darauf angegebene Prüfungszentrum gültig. Es werden nur Kandidaten in das Prüfungszentrum eingelassen, die über eine gültige Prüfungszulassung verfügen und sich eindeutig ausweisen können. Ein eindeutiger Ausweis ist ein gültiger, von einer Behörde ausgestellter Original-Ausweis mit Foto, in dem der Name des Kandidaten in der auf der Prüfungszulassung angegebenen Form eingetragen ist. Die Angaben im Ausweis dürfen nicht handgeschrieben sein. Das Ausweispapier muss sämtliche hier aufgeführten Merkmale erfüllen. Beispiele hierfür sind z. B. ein Reisepass, Führerschein, Militärausweis, Personalausweis, eine Greencard sowie ein bundesstaatlicher Ausweis. Kandidaten, die keine akzeptablen Ausweis-papiere vorlegen, werden nicht zum Examen zugelassen, und ihre gezahlte Anmeldegebühr verfällt.

Halten Sie die Regeln des Prüfungszentrums ein

- Nachdem die Verlesung der Prüfungsanweisungen begonnen hat, werden keine Kandidaten mehr in das Prüfungszentrum eingelassen.
- Die Kandidaten müssen mehrere angespitzte Bleistifte, Härtegrad 2 oder HB (weich) und einen guten Radiergummi mitbringen. Im Prüfungszentrum stehen keine Bleistifte und Radiergummis zur Verfügung. Da die Prüfungen an unterschiedlichen Orten stattfinden, werden wir uns bemühen, die Klimaanlage an jedem Prüfungsort so angenehm wie möglich einzustellen. Die Kandidaten werden gebeten, nach Wunsch in bequemer Kleidung zu erscheinen.
- Die Prüfungskandidaten dürfen keine Nachschlagewerke, keine leeren Blätter oder Notizblöcke und keine Sprachwörterbücher mit in das Prüfungszentrum nehmen.
- Die Prüfungskandidaten dürfen keinen Taschenrechner in das Prüfungszentrum bringen oder im Prüfungszentrum verwenden.
- Die Prüfungskandidaten dürfen keinerlei Kommunikationsgeräte (z. B. Mobiltelefone, PDAs, Blackberries usw.) mit in das Prüfungszentrum nehmen. **Werden Kandidaten während des Exams mit einem derartigen Gerät erwischt, so wird ihr Examen für nichtig erklärt und sie werden aufgefordert, den Prüfungsraum unverzüglich zu verlassen.**
- Im Prüfungszentrum sind keine Besucher erlaubt.
- Im Prüfungszentrum sind (ohne vorherige Genehmigung durch ISACA) keine Speisen oder Getränke erlaubt.

Betrugsversuche

Prüfungskandidaten, die eines Betrugsversuchs überführt werden, werden von der Prüfung ausgeschlossen und evtl. angezeigt. Als Betrugsversuch gelten u.a. die Leistung bzw. Entgegennahme von Hilfe, der Gebrauch von Notizen, Papieren oder anderen Hilfsmitteln, der Versuch, das Examen für eine andere Person abzulegen, die Benutzung von Kommunikationsgeräten (einschließlich Mobiltelefonen) während des Exams, bzw. die Mitnahme des Prüfungshefts, Antwortbogens oder Notizen aus dem Prüfungsraum. Prüfungskandidaten, die den Prüfungsraum ohne Erlaubnis oder Begleitung durch eine Aufsichtsperson verlassen, dürfen nicht wieder in den Prüfungsraum zurückkehren und werden disqualifiziert. Derartige Vorfälle werden dem CISA-Zertifizierungsausschuss von ISACA durch den Prüfungsveranstalter gemeldet.

Die vollständigen Richtlinien für persönliche Gegenstände finden Sie unter www.isaca.org/cisabelongings. Weder ISACA noch der Prüfungsveranstalter sind für persönliche Gegenstände der Prüfungskandidaten zuständig.

Füllen Sie den Antwortbogen sorgfältig aus

- Vor dem Beginn des Exams verliest der Prüfungsleiter die Anweisungen zum Eintragen der Identifikationsangaben auf dem Antwortbogen. Sie müssen die auf der Prüfungszulassung angegebene Identifikationsnummer und alle weiteren erforderlichen Informationen fehlerfrei eintragen, da es andernfalls zu Verzögerungen oder Fehlern bei der Auswertung kommen kann.
- In jedem Prüfungszentrum ist eine Aufsichtsperson anwesend, die die Hauptsprache spricht. Wenn ein Kandidat das Examen in einer anderen als der Hauptsprache des Prüfungszentrums ablegen möchte, ist die Aufsichtsperson dieser Sprache möglicherweise nicht mächtig. Die schriftlichen Anweisungen sind jedoch in der Prüfungssprache verfügbar.
- Sie sollten sämtliche Anweisungen unbedingt gründlich lesen und verstehen, bevor Sie mit der Beantwortung der Frage beginnen. Wenn Sie Anweisungen überspringen oder nur flüchtig lesen, könnten Ihnen wichtige Informationen und damit möglicherweise Punkte entgehen.
- Alle Antworten müssen in dem entsprechenden Kreis auf dem Antwortbogen markiert werden. Achten Sie sorgfältig darauf, nur eine Antwort pro Frage zu markieren, und vergewissern Sie sich, dass Sie die richtige Antwortzeile auswählen. Wenn Sie eine Antwort ändern möchten, müssen Sie die falsche Antwort vollständig ausradieren, bevor Sie die neue Antwort markieren.
- Sie sollten alle Fragen beantworten. **Es gibt keinen Abzug für falsche Antworten. Die Punktwertungen richten sich ausschließlich nach der Anzahl der korrekt beantworteten Fragen, Sie sollten daher keine Frage unbeantwortet lassen.**
- Nach Abschluss der Prüfung müssen Sie Ihren Antwortbogen und die Prüfungsbroschüre abgeben.

Teilen Sie sich die Zeit gut ein

- Bei der vierstündigen Prüfung haben Sie etwas mehr als eine Minute pro Frage Zeit. Teilen Sie sich die Zeit daher so ein, dass Sie die gesamte Prüfung schaffen. Dafür müssen Sie etwa 50 Fragen pro Stunde beantworten.
- Sie sollten Ihre Antworten sofort auf dem Antwortbogen eintragen. **Nach Ablauf der Prüfungsdauer wird keine zusätzliche Zeit gewährt, evtl. in der Prüfungsbroschüre markierte Antworten in den Prüfungsbogen zu übertragen.**

Befolgen Sie die Regeln

- Um die Sicherheit des Exams und die Gültigkeit der Bewertungen zu gewährleisten, werden die Kandidaten aufgefordert, den Antwortbogen zu unterschreiben.
- Der CISA-Zertifizierungsausschuss behält sich das Recht vor, Kandidaten von der Prüfung auszuschließen, die eines Betrugsversuchs oder Verstoßes gegen die Prüfungsordnung überführt werden, z. B. der Leistung bzw. Entgegennahme von Hilfe, dem Gebrauch von Notizen, Papieren oder anderen Hilfsmitteln, dem Versuch, das Examen für eine andere Person abzulegen oder der Mitnahme von Prüfungsmaterialien oder Notizen aus dem Prüfungsraum. Die Prüfungsagentur legt dem CISA-Zertifizierungsausschuss einen Bericht über derartige Vorfälle zur Prüfung und Entscheidung vor.

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung

Ausschluss- bzw. Disqualifizierungsgründe

- Unbefugtes Betreten des Prüfungszentrums.
- Der Kandidat stört den Ablauf oder gibt bzw. empfängt Hilfe.
- Der Kandidat versucht, Testmaterialien oder Notizen aus dem Prüfungszentrum mitzunehmen.
- Der Kandidat gibt sich für einen anderen Kandidaten aus.
- Der Kandidat bringt verbotene Gegenstände in das Prüfungszentrum mit.
- Der Kandidat befindet sich während des Exams im Besitz eines Kommunikationsgeräts (z. B. Mobiltelefone, PDAs, Blackberries usw.).
- Der Kandidat verlässt den Prüfungsraum ohne Erlaubnis.

Werden Kandidaten während des Exams mit einem Kommunikationsgerät (z. B. Mobiltelefon, PDA, Blackberries® usw.) erwischt, so wird ihr Examen für nichtig erklärt, und sie werden aufgefordert, den Prüfungsraum unverzüglich zu verlassen.

Bewertung des CISA-Exams

Das CISA-Examen umfasst 200 Multiple-Choice-Fragen. Die Punktzahl der Kandidaten wird als skaliertes Punktwert angegeben. Der skalierte Punktwert ergibt sich durch die Umrechnung der erzielten Punktzahl eines Kandidaten in eine gebräuchliche Skala. ISACA verwendet zur Punktbewertung eine Skala von 200 bis 800. Ein skaliertes Punktwert von 800 bedeutet dabei den Höchstwert, bei dem sämtliche Fragen korrekt beantwortet wurden, ein skaliertes Punktwert von 200 hingegen ist der geringstmögliche Punktwert und bedeutet, dass kaum Fragen korrekt beantwortet wurden. Sie müssen einen Punktwert von mindestens 450 erzielen, um das Examen zu bestehen. Ein Punktwert von 450 Punkten stellt die Untergrenze des geforderten Wissensstandes gemäß den Richtlinien des CISA-Zertifizierungsausschusses dar. Ein Kandidat mit einem zum Bestehen des Exams ausreichenden Punktwert kann daraufhin einen Antrag auf Zertifizierung stellen, sofern alle weiteren Voraussetzungen erfüllt sind.

Das CISA-Examen enthält einige Fragen, die ausschließlich zu Forschungs- und Analyse Zwecken dienen. Diese Fragen sind nicht speziell gekennzeichnet und werden nicht in die Berechnung des endgültigen Punktwerts einbezogen.

Die Prüfungsergebnisse werden etwa acht Wochen nach dem Prüfungstermin an die Prüfungsteilnehmer versendet. Bei entsprechender Einwilligung des Kandidaten bei der Anmeldung kann sich der Kandidat außerdem per E-Mail darüber benachrichtigen lassen, ob und mit welcher Punktzahl die Prüfung bestanden wurde. Diese E-Mail-Benachrichtigung wird nur an die Adresse gesendet, die zum Zeitpunkt der ursprünglichen Bekanntgabe der Ergebnisse im Profil des Prüfungsteilnehmers angegeben ist. Prüfungsergebnisse werden nicht telefonisch oder per Fax mitgeteilt, um die Vertraulichkeit der Auswertung zu wahren. Um zu verhindern, dass die E-Mail-Benachrichtigung als Spam eingestuft wird, empfiehlt es sich, die Adresse *exam@isaca.org* in das Adressbuch, die Liste zulässiger Adressen bzw. die Liste sicherer Absender aufzunehmen.

Die Prüfungsteilnehmer erhalten eine Auswertung mit den Punktwerten für die einzelnen Fachgebiete. Teilnehmer, welche die Prüfung bestanden haben, erhalten außerdem ausführliche Informationen zur Beantragung des CISA-Zertifikats.

Die Einzelpunktwerte zeigen die Fachgebiete auf, die vor dem erneuten Ablegen des Exams wiederholt und vertieft werden sollten. Hinweis für Kandidaten, die das Examen nicht bestanden haben: Der skalierte Gesamtpunktwert lässt sich nicht aus dem einfachen oder gewichteten Mittelwert der Einzelpunktwerte errechnen.

Prüfungsteilnehmer, die das Examen nicht bestanden haben, können eine manuelle Neuauswertung ihres Antwortbogens anfordern. Damit können sie sichergehen, dass die Computerauswertung nicht durch falsch erkannte Markierungen, Mehrfachantworten o. ä. verfälscht wurde. Wir versichern Ihnen aber, dass alle Bewertungen vor der Versendung verschiedenen Qualitätskontrollen unterzogen wurden. Eine erneute Auswertung führt daher in den seltensten Fällen zu einer tatsächlichen Änderung des Ergebnisses. Eine manuelle Auswertung muss schriftlich innerhalb von 90 Tagen nach Ausgabe des Examensergebnisses bei der Zertifikationsabteilung angefordert werden. Nach Ablauf dieses Zeitraums werden keine Anträge für eine manuelle Auswertung mehr angenommen. Im Antrag müssen der Name, die Identifikationsnummer und die Postanschrift des Kandidaten angegeben werden. Für den Antrag fällt eine Gebühr von 75 USD an.

Arten der Fragen im CISA-Examen

Mit den im CISA-Examen gestellten Fragen sollen die praktischen Fähigkeiten und die Kenntnisse der grundlegenden Konzepte und Standards erfasst und überprüft werden. Für jede Frage gibt es eine am besten zutreffende Antwort.

Jede CISA-Frage setzt sich aus einem Stamm (Frage) und vier Optionen (Antwortmöglichkeiten) zusammen. Sie müssen die korrekte oder am besten zutreffende Antwort aus diesen Antwortmöglichkeiten auswählen. Der Stamm kann eine Frage oder eine unvollständige Aussage sein. In einigen Fällen ist auch ein Szenario angegeben. Bei derartigen Fragen wird eine Situation beschrieben, und Sie müssen anhand der angegebenen Informationen zwei oder mehr Fragen dazu beantworten. Lesen Sie jede Frage sorgfältig durch. Bei dem CISA-Examen müssen Sie die zutreffende Antwort möglicherweise anhand gemäß eines bestimmten Kriteriums auswählen, z. B. **AM EHESTEN** oder **AM BESTEN**. Lesen Sie sich jede grundsätzlich Frage genau durch, schließen Sie falsche Antworten aus, und wählen Sie unter den verbleibenden die beste Antwort aus. Beispiele für Prüfungsfragen im CISA-Examen finden Sie unter www.isaca.org/cisaassessment.

Bewerbung für die CISA-Zertifizierung

Wenn Sie das CISA-Examen bestehen, führen Sie nicht automatisch den Berufstitel CISA. Sie haben ab dem Examenstag fünf Jahre Zeit, sich für die Zertifizierung zu bewerben. Dafür füllen Sie den Antrag auf Zertifizierung aus und legen die entsprechenden Formulare zum Nachweis Ihrer Arbeitserfahrung bei. **Sie sind erst dann zertifiziert und können den Titel CISA führen, nachdem der ausgefüllte Antrag eingegangen ist und genehmigt wurde.** Die Entscheidungen bezüglich Bewerbungen gelten nicht als endgültig, da bei abgelehnten Zertifizierungsbewerbungen ein Widerspruch möglich ist. Anfragen hinsichtlich abgelehnter Zertifizierungen senden Sie bitte an certification@isaca.org. Als zertifizierter CISA erhalten Sie ein Zertifikat sowie eine CISA-Zertifizierungs-Anstecknadel. Bei der Beantragung müssen Sie zustimmen, dass ISACA sich das Recht vorbehält, jedoch nicht dazu verpflichtet ist, Ihren CISA-Status zu veröffentlichen oder anderweitig offen zu legen. Die Bearbeitungsgebühr für die CISA-Zertifizierungsbewerbung beträgt 50 USD.

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung

Voraussetzungen für die CISA-Erstzertifizierung

Die Zertifikat wird Einzelpersonen zuerkannt, die das CISA-Examen bestanden haben und die folgende Arbeitserfahrung vorweisen können.

Mindestens fünf Jahre Berufserfahrung auf dem Gebiet der Informationssystem-Prüfung, -Steuerung, -Gewährleistung und Sicherheit sind Voraussetzung für die Zertifizierung. Diese Arbeitserfahrung kann unter folgenden Bedingungen entfallen oder ersetzt werden:

- Maximal ein Jahr Prüfungserfahrung im Bereich von Informationssystemen ODER außerhalb des Bereichs von Informationssystemen kann ein Jahr Berufserfahrung ersetzen.
- 60 bis 120 anerkannte Stunden durch abgeschlossene Universitätssemester (dies entspricht einem Hochschulabschluss nach einer Studienzeit von zwei bzw. vier Jahren), die nicht länger als 10 Jahre vor der Antragstellung liegen, können jeweils ein bzw. zwei Jahre Berufserfahrung ersetzen. Inhaber von mehreren akademischen Abschlüssen können maximal zwei Jahre in Anspruch nehmen.
- Ein Abschluss (Bachelor's oder Master's Degree) von einer Universität, an der die unter der Schirmherrschaft der ISACA stehenden Modelllehrpläne obligatorisch sind, kann ein Jahr Berufserfahrung ersetzen. Ein Verzeichnis dieser Hochschulen finden Sie unter www.isaca.org/modeluniversities. Diese Möglichkeit kann nicht wahrgenommen werden, wenn bereits eine dreijährige Erfahrung ersetzt und eine Ausbildungsverzichterklärung in Anspruch genommen wurde.
- Ein Abschluss (Master's Degree) der Studienfächer Informationssicherheit oder Informationstechnologie von einer akkreditierten Universität kann ein Jahr Berufserfahrung ersetzen.

Ausnahme: Zwei Jahre Berufserfahrung als Vollzeitlehrkraft an einer Universität in einem artverwandten Fach (d. h. Informatik, Rechnungswesen, Informationssystemprüfung) können jeweils ein Jahr Berufserfahrung ersetzen.

Die Berufserfahrung muss innerhalb von zehn Jahren vor dem Datum der Antragstellung zum Erwerb der CISA-Zertifizierung oder innerhalb von fünf Jahren ab dem Datum erworben werden, an dem das Examen ursprünglich bestanden wurde. Wird innerhalb von fünf Jahren ab dem Tag des Bestehens des Examens kein vollständiger Antrag auf CISA-Zertifizierung eingereicht, muss das Examen erneut abgelegt und bestanden werden.

Viele Personen legen das CISA-Examen ab, bevor Sie über die nötige Arbeitserfahrung verfügen. Dies ist zulässig und wird gefördert, der Berufstitel CISA wird jedoch erst verliehen, wenn alle Bedingungen erfüllt sind.

Voraussetzungen zur Aufrechterhaltung der CISA-Zertifizierung

Als CISA müssen Sie folgende Anforderungen erfüllen, um das Zertifikat aufrechtzuerhalten:

- Jährlich mindestens 20 Stunden berufliche Fortbildung belegen und nachweisen, sowie über einen Zeitraum von drei Jahren mindestens 120 Stunden berufliche Fortbildung belegen und nachweisen. Weitere Einzelheiten finden Sie in der CISA CPE-Richtlinie unter www.isaca.org/cisacpepolicy.
- Die jährlich anfallenden Verwaltungsgebühren für berufliche Fortbildung in voller Höhe an die internationale Hauptstelle von ISACA überweisen.
- Wenn Sie für die jährliche Überprüfstichprobe ausgewählt werden: Antworten und die erforderlichen Belege über gemeldete berufliche Weiterbildungsaktivitäten einreichen.
- Den ISACA-Berufsehrenkodex einhalten.

Eine Nichteinhaltung dieser allgemeinen Richtlinien führt zum Entzug des Berufstitels CISA des jeweiligen Inhabers. Alle Zertifikate sind Eigentum von ISACA. Wird einem Teilnehmer zuerst eine Zertifizierung erteilt, diese aber nachträglich entzogen, muss das Zertifikat vom Teilnehmer zerstört werden.

ISACA-Berufsehrenkodex

Der von ISACA aufgestellte Berufsehrenkodex gibt Richtlinien für das berufliche und persönliche Verhalten der Verbandsmitglieder und/oder Zertifikatsinhaber vor. Bei Nichteinhaltung dieses Berufsehrenkodex können Ermittlungen gegen das Mitglied und/oder den Zertifikatsinhaber und ggf. Disziplinarmaßnahmen veranlasst werden. Den Berufsehrenkodex von ISACA finden Sie online unter www.isaca.org/ethics.

Entzug der CISA-Zertifizierung

Der CISA-Zertifizierungsausschuss kann einer Einzelperson im eigenem Ermessen nach angemessener und gründlicher Abwägung das CISA-Zertifikat aus einem der folgenden Gründe entziehen:

- Nichteinhaltung der CISA-Vorschriften zur beruflichen Weiterbildung
- Verletzung einer oder mehrerer Bestimmungen des ISACA-Berufsehrenkodex
- Verfälschung oder vorsätzliche Unterlassung der Angabe wichtiger Informationen
- Vorsätzliche Falschdarstellung einer wichtigen Tatsache
- Beteiligung an oder Hilfe bei betrügerischem, unbefugtem oder unangemessenem Verhalten im Zusammenhang mit dem CISA-Examen oder dem Zertifikationsprozess

Beschreibung der CISA-Arbeitsbereiche Tätigkeitsfelder und Fachkenntnisse eines CISA

INHALTSBEREICH (Fachgebiet)	
Fachgebiet 1: Das Verfahren zur Prüfung von Informationssystemen — Hier geht es darum, im Einklang mit den IT-Prüfungsstandards Prüfungsleistungen zu erbringen, die Organisationen dabei helfen, ihre Informationssysteme zu schützen und zu steuern.	
Fachgebiet 1: Tätigkeiten	
T1.1	Entwicklung und Umsetzung einer risikobasierten IT-Prüfungsstrategie gemäß den etablierten IT-Prüfungsstandards, um zu gewährleisten, dass alle wichtigen Bereiche abgedeckt sind
T1.2	Planung konkreter Prüfungshandlungen anhand derer festgestellt werden kann, ob Informationssysteme ausreichend geschützt sind, adäquaten Kontrollen unterliegen und für die Organisation von Wert sind
T1.3	Durchführung von Prüfungen gemäß den IT-Prüfungsstandards, um die vorgesehenen Prüfungsziele zu erreichen
T1.4	Mitteilung der Prüfungsergebnisse an die Hauptbeteiligten und ggf. Abgabe von Empfehlungen zur Einführung von Änderungen
T1.5	Durchführung von Nachprüfungen oder Erstellung von Zwischenberichten, um zu gewährleisten, dass die erforderlichen Maßnahmen zeitnah durch das Management eingeleitet wurden
Fachgebiet 1: Kenntnisse	
KS1.1	Kenntnis der ISACA Normen, Richtlinien, Instrumente und Techniken in Bezug auf IT-Prüfungen und IT-Sicherung, sowie des ISACA-Berufsehenkodexes und sonstiger maßgeblicher Standards
KS1.2	Kenntnis der Konzepte, Instrumente und Techniken der Risikobewertung im Prüfungskontext
KS1.3	Kenntnis der Steuerungsziele und -möglichkeiten in Bezug auf Informationssysteme
KS1.4	Kenntnis der Techniken für Prüfungsplanung und Prüfungsmanagement, einschließlich Nachkontrollen
KS1.5	Kenntnis der grundlegenden Geschäftsprozesse (z. B. Einkauf, Lohn- und Gehaltswesen, Kreditoren- und Debitorenbuchhaltung) einschließlich der entsprechenden Informationstechnik
KS1.6	Kenntnis der geltenden Gesetze und Vorschriften, die sich auf den Umfang, die Belegerfassung und -aufbewahrung sowie die Häufigkeit von Prüfungen auswirken
KS1.7	Kenntnis der Techniken zur Belegerfassung (z. B. Beobachtung, Befragung, Einsichtnahme, Gespräche, Datenanalyse), die bei der Erfassung, Sicherung und Aufbewahrung von Prüfungsbelegen eingesetzt werden
KS1.8	Kenntnis der unterschiedlichen Methoden zur Stichprobenentnahme
KS1.9	Kenntnis von Berichts- und Kommunikationstechniken (z. B. Vermittlung, Verhandlung, Konfliktlösung, Aufbau von Prüfungsberichten)
KS1.10	Kenntnis von Verfahren und Rahmensystemen zur Qualitätssicherung bei Prüfungen
Fachgebiet 2: IT-Governance und -Management — Hier soll sichergestellt werden, dass die zur Umsetzung der Ziele und Unterstützung der Strategie der Organisation erforderlichen Führungs- und Organisationsstrukturen und -abläufe vorhanden sind.	
Fachgebiet 2: Tätigkeiten	
T2.1	Beurteilung der Wirksamkeit der IT-Governance-Struktur im Hinblick darauf, ob die Entscheidungen, Anweisungen und Leistungen im IT-Bereich den Strategien und Ziele der Organisation förderlich sind
T2.2	Beurteilung der IT-Organisationsstruktur und des Personalmanagements im Hinblick darauf, ob diese den Strategien und Zielen der Organisation förderlich sind
T2.3	Beurteilung der IT-Strategie - einschließlich der eingeschlagenen Richtung - und der Vorgehensweise bei der Entwicklung, Genehmigung, Umsetzung und laufenden Ausrichtung der IT-Strategie auf die Strategien und Zielen der Organisation
T2.4	Beurteilung der IT-Richtlinien, -Standards und -Verfahren der Organisation sowie der entsprechenden Verfahren zu deren Entwicklung, Genehmigung, Umsetzung, Pflege und Kontrolle im Hinblick darauf, ob diese die IT-Strategie fördern und die geltenden aufsichtsrechtlichen und gesetzlichen Bestimmungen erfüllen
T2.5	Beurteilung der Tauglichkeit des Qualitätsmanagementsystems im Hinblick darauf, ob dieses die Strategien und Ziele der Organisation auf kostengünstige Weise fördert
T2.6	Beurteilung des IT-Managements und der Überwachung der Kontrollmechanismen (z. B. laufende Überwachung, Qualitätssicherung [QS]) im Hinblick auf Einhaltung der Richtlinien, Standards und Verfahren der Organisation
T2.7	Beurteilung der Investitions-, Nutzungs- und Zuordnungspraktiken für IT-Ressourcen im Hinblick auf deren Übereinstimmung mit den Strategien und Zielen der Organisation
T2.8	Beurteilung der Strategien und Richtlinien bei der Beauftragung von IT-Leistungen sowie der Praktiken beim Vertragsmanagement, jeweils im Hinblick darauf, ob diese den Strategien und Zielsetzungen der Organisation förderlich sind
T2.9	Beurteilung der Praktiken beim Risikomanagement im Hinblick darauf, ob die IT-bezogenen Risiken der Organisation angemessen gehandhabt werden
T2.10	Beurteilung der Überwachungs- und Sicherungspraktiken im Hinblick darauf, ob der Vorstand und das Management zeitnah ausreichende Informationen über die IT-Performance erhalten
T2.11	Beurteilung des Betriebskontinuitätsplans der Organisation im Hinblick darauf, ob deren zentrale Geschäftsabläufe während eines IT-Ausfalls ungestört weiterlaufen können

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung

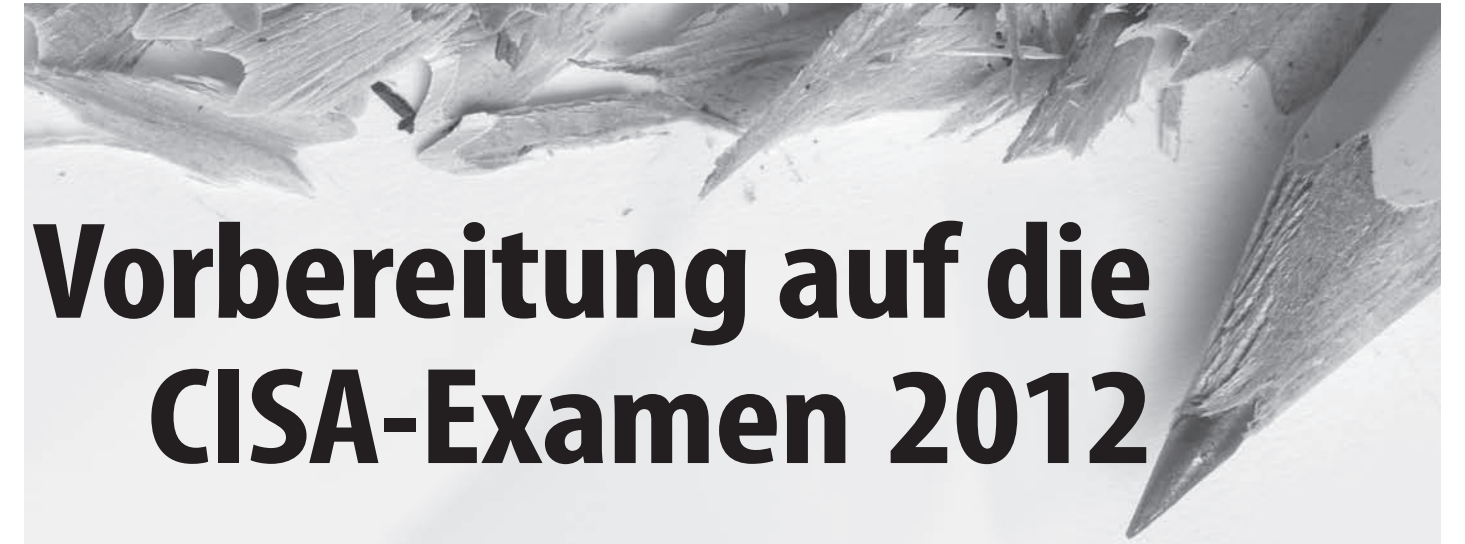
INHALTSBEREICH (Fachgebiet)	
Fachgebiet 2: Kenntnisse	
KS2.1	Kenntnis der Rahmenbedingungen in Bezug auf IT-Governance, -Management, -Sicherheit und -Steuerung, sowie der damit verbundenen Standards, Richtlinien und Praktiken
KS2.2	Kenntnis des Zwecks der für eine Organisation erarbeiteten IT-Strategie, -Grundsätze, -Standards und -Verfahren sowie der wesentlichen Bestandteile dieser einzelnen Elemente
KS2.3	Kenntnis der Organisationsstruktur, Rollen und Aufgaben im IT Bereich
KS2.4	Kenntnis der Prozesse bei der Entwicklung, Implementierung und Pflege der IT-Strategie, -Grundsätze, -Standards und -Verfahren
KS2.5	Kenntnis der technischen Ausrichtung und IT-Architektur der Organisation sowie der Auswirkungen derselben auf die Aufstellung langfristiger strategischer Ziele
KS2.6	Kenntnis der die Organisation betreffenden Gesetze, Vorschriften und Branchenstandards
KS2.7	Kenntnis von Qualitätsmanagementsysteme
KS2.8	Kenntnis und Anwendung von Reifegradmodellen
KS2.9	Kenntnis von Techniken zur Prozessoptimierung
KS2.10	Kenntnis der Investitions- und Zuordnungspraktiken für IT-Ressourcen einschließlich Priorisierungskriterien (z. B. Portfoliomanagement, Value Management, Projektmanagement)
KS2.11	Kenntnis der Prozesse bei der Auswahl und Leistungskontrolle von IT-Lieferanten sowie dem damit verbundenen Vertragsmanagement und Supplier Relationship Management; hierunter fallen auch die Beziehungen zwischen externen Vertragsnehmern und deren jeweiligen Subunternehmern
KS2.12	Kenntnisse in Bezug auf Enterprise Risk Management
KS2.13	Kenntnis der Überwachungs- und Berichterstellungspraktiken für die IT-Performance (z. B. Balanced Scorecards und wichtige Leistungskennzahlen [KPIs])
KS2.14	Kenntnis der Personalmanagement-Praktiken zur Unterstützung des Betriebskontinuitätsplans
KS2.15	Kenntnis von Business Impact Analysen (BIA) im Zusammenhang mit dem Betriebskontinuitätsplan (BKP)
KS2.16	Kenntnis der Standards und Verfahren zur Entwicklung und Pflege des Betriebskontinuitätsplans (BKP) einschließlich Prüfverfahren
Fachgebiet 3: Anschaffung, Entwicklung und Implementierung von Informationssystemen — Hier soll sichergestellt werden, dass die Praktiken für die Anschaffung, Entwicklung, Prüfung und Implementierung von Informationssystemen den Strategien und Zielen der Organisation entsprechen.	
Fachgebiet 3: Tätigkeiten	
T3.1	Beurteilung des Business Case für geplante Investitionen in die Anschaffung, Entwicklung, Pflege und spätere Außerbetriebnahme von Informationssystemen im Hinblick darauf, ob diese den geschäftlichen Zielen der Organisation entsprechen
T3.2	Beurteilung der Projektmanagementpraktiken und -steuerungsmechanismen im Hinblick darauf, ob die geschäftlichen Ziele kostengünstig erreicht und Risiken sinnvoll abgewogen werden
T3.3	Durchführung von Überprüfungen im Hinblick darauf, ob ein Projekt plangemäß voranschreitet, angemessen dokumentiert ist und der berichtete Projektstand den tatsächlichen Gegebenheiten entspricht
T3.4	Beurteilung von Steuerungsmechanismen für Informationssysteme während der Bedarfsanalyse-, Entwicklungs- und Testphase im Hinblick auf die Einhaltung der Grundsätze, Standards und Verfahren der Organisation sowie aller maßgeblichen externen Anforderungen
T3.5	Beurteilung von Informationssystemen im Hinblick auf deren Implementierungsfähigkeit und Bereitschaft zur Überführung in die Produktion, insbesondere indem geprüft wird, ob alle zu dem Projekt gehörenden Lieferobjekte und Kontrollen erbracht und die Anforderungen der Organisation erfüllt werden
T3.6	Überprüfung der Systeme nach der Implementierung um sicherzustellen, dass alle zu dem Projekt gehörenden Lieferobjekte und Kontrollen erbracht und die Anforderungen der Organisation erfüllt wurden
Fachgebiet 3: Kenntnisse	
KS3.1	Kenntnis von Erfolgsermittlungspraktiken (z. B. Projektstudien, Business-Case-Studien, Total Cost of Ownership [TCO], ROI)
KS3.2	Kenntnis von Projektsteuerungsverfahren (z. B. Lenkungsausschuss, Projektaufsichtsgremium, Projektmanagementbüro)
KS3.3	Kenntnis von Rahmenbedingungen, Praktiken und Werkzeugen beim Projektmanagement
KS3.4	Kenntnis von bei Projekten angewandten Risikomanagement-Praktiken
KS3.5	Kenntnis der IT-Architektur hinsichtlich Daten, Anwendungen und Technologie (z. B. verteilte Anwendungen, webbasierte Anwendungen, Web-Dienste und mehrschichtige Anwendungen)
KS3.6	Kenntnis von Beschaffungspraktiken (z. B. Bewertung von Lieferanten, Lieferantenmanagement und Treuhandvereinbarungen)
KS3.7	Kenntnis von Bedarfsanalyse- und Bedarfsmanagementpraktiken (z. B. Bedarfsermittlung, Rückverfolgbarkeit, Lückenanalyse, Schwachstellenmanagement, Sicherheitsanforderungen)
KS3.8	Kenntnis der Projekterfolgskriterien und -risiken

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung

INHALTSBEREICH (Fachgebiet)	
Fachgebiet 3: Kenntnisse (Fortsetzung)	
KS3.9	Kenntnis der Steuerungsziele und -techniken, welche die Vollständigkeit, Genauigkeit, Gültigkeit und Berechtigung von Transaktionen und Daten sicherstellen
KS3.10	Kenntnis von Systementwicklungsmethoden und -werkzeuge einschließlich ihrer Stärken und Schwächen (z. B. agile Entwicklungsverfahren, Prototypenherstellung, Rapid Application Development [RAD] und objektorientierte Entwurfsverfahren)
KS3.11	Kenntnis von Testmethoden und Praktiken in Verbindung mit der Entwicklung von Informationssystemen
KS3.12	Kenntnisse im Bereich des Konfigurations- und Freigabemanagements in Verbindung mit der Entwicklung von Informationssystemen
KS3.13	Kenntnis von Praktiken bei der Systemmigration und Aufstellung der Infrastruktur, sowie von Datenumwandlungswerkzeugen, -techniken und -verfahren
KS3.14	Kenntnis der Ziele und Praktiken bei Prüfungen nach der Implementierung (z. B. Projektabschluss, Kontrollenimplementierung, Erfolgsermittlung und Leistungsmessung)
Fachgebiet 4: Betrieb, Pflege/Instandhaltung und Unterstützung von Informationssystemen — Hier soll sichergestellt werden, dass die Prozesse im Zusammenhang mit dem Betrieb, der Pflege/Instandhaltung und der Unterstützung von Informationssystemen den Strategien und Zielen der Organisation entsprechen.	
Fachgebiet 4: Tätigkeiten	
T4.1	Regelmäßige Überprüfung der Informationssysteme im Hinblick darauf, ob diese weiterhin den Zielen der Organisation entsprechen
T4.2	Beurteilung der Service-Level-Management-Praktiken im Hinblick darauf, ob die jeweiligen Service Levels der von internen und externen Dienstleistern erbrachten Leistungen definiert und verwaltet werden
T4.3	Beurteilung der Managementpraktiken von externen Dienstleistern im Hinblick darauf, ob diese die von der Organisation erwarteten Leistungskontrollen befolgen
T4.4	Beurteilung der Betriebs- und Anwenderverfahren im Hinblick darauf, ob planmäßige und außerplanmäßige Prozesse bis zur vollständigen Durchführung durchgehend gemanagt werden
T4.5	Beurteilung der Prozesse zur Pflege/Instandhaltung von Informationssystemen im Hinblick darauf, ob diese effektiv gesteuert werden und die Ziele der Organisation weiterhin unterstützen
T4.6	Beurteilung der Datenverwaltungspraktiken im Hinblick auf die Integrität und Optimierung von Datenbanken
T4.7	Beurteilung der zur Kapazitäts- und Leistungsüberwachung eingesetzten Werkzeuge und Techniken im Hinblick darauf, ob die IT-Leistungen den Zielen der Organisation entsprechen
T4.8	Beurteilung der Problem- und Vorfällemanagementpraktiken im Hinblick darauf, ob Vorfälle, Probleme und Fehler zeitnah erfasst, analysiert und gelöst bzw. behoben werden
T4.9	Beurteilung der Praktiken beim Änderungs-, Konfigurations- und Freigabemanagement im Hinblick darauf, ob in der Produktionsumgebung der Organisation vorgenommene planmäßige und außerplanmäßige Änderungen angemessen kontrolliert und dokumentiert werden
T4.10	Beurteilung der Angemessenheit von Maßnahmen zur Datensicherung und -wiederherstellung im Hinblick auf die Verfügbarkeit der zur Wiederaufnahme der Datenverarbeitung erforderlichen Informationen
T4.11	Beurteilung des Notfallplans der Organisation im Hinblick darauf, ob die Wiederherstellung der Datenverarbeitungsfunktionen im Falle einer Katastrophe gewährleistet ist
Fachgebiet 4: Kenntnisse	
KS4.1	Kenntnis von Service-Level-Management-Praktiken und der Bestandteile eines Service Level Agreements
KS4.2	Kenntnis von Techniken zur Überwachung der Einhaltung interner Kontrollen der Organisation durch Dritte
KS4.3	Kenntnis von Betriebs- und Anwenderverfahren zur Handhabung von planmäßigen und außerplanmäßigen Prozessen
KS4.4	Kenntnis der technologischen Konzepte im Zusammenhang mit Hardware- und Netzwerkkomponenten, Systemsoftware und Datenbankmanagementsystemen
KS4.5	Kenntnis von Kontrollverfahren zur Gewährleistung der Integrität von Systemschnittstellen
KS4.6	Kenntnis von Softwarelizenzierungs- und Softwarebestandsaufnahmepraktiken
KS4.7	Kenntnis von Werkzeugen und Techniken zum Schutz vor Systemausfällen (z. B. fehlertolerante Hardware, Verhinderung einer einzelnen Fehlerstelle, Clustering)
KS4.8	Kenntnis von Praktiken bei der Datenbankadministration
KS4.9	Kenntnis von Werkzeugen und Techniken zur Kapazitätsplanung und -überwachung
KS4.10	Kenntnis von Prozessen, Werkzeugen und Techniken zur Systemleistungsüberwachung (z. B. Netzwerkanalyseprogramme, Systemnutzungsberichte, Lastenausgleich)

Handbuch für Kandidaten für das CISA®-Examen und für die CISA®-Zertifizierung

INHALTSBEREICH (Fachgebiet)	
Fachgebiet 4: Kenntnisse (Fortsetzung)	
KS4.11	Kenntnis von Problem- und Vorfallmanagementpraktiken (z. B. Helpdesk, Eskalationsverfahren, Nachverfolgung)
KS4.12	Kenntnis von Prozessen zur Handhabung von planmäßigen und außerplanmäßigen Änderungen an den Produktionssystemen bzw. der Infrastruktur, einschließlich Change-, Konfigurations-, Freigabe- und Patch-Management
KS4.13	Kenntnis von Praktiken bei der Datensicherung, -speicherung, -pflege, -aufbewahrung und -wiederherstellung
KS4.14	Kenntnis von behördlichen, gesetzlichen, schuldrechtlichen und versicherungsrechtlichen Aspekten im Zusammenhang mit Disaster Recovery
KS4.15	Kenntnis von Business Impact Analysen (BIA) im Zusammenhang mit der Notfallplanung (Disaster Recovery Planung)
KS4.16	Kenntnis im Hinblick auf die Entwicklung und Pflege von Notfallplänen
KS4.17	Kenntnis der Arten von Ausweichverarbeitungsstandorten und -methoden, die zur Überwachung der vertraglichen Vereinbarungen verwendet werden (z. B. Hot Sites, Warm Sites, Cold Sites)
KS4.18	Kenntnis von Prozessen zum Aktivieren der Notfallpläne
KS4.19	Kenntnis von Disaster Recovery Testmethoden
Fachgebiet 5: Schutz von Informationswerten – Hier soll sichergestellt werden, dass die Sicherheitsgrundsätze, -standards, -verfahren und -kontrollen der Organisation die Vertraulichkeit, Integrität und Verfügbarkeit der Informationswerte gewährleisten.	
Fachgebiet 5: Tätigkeiten	
T5.1	Beurteilung der Informationssicherheitsgrundsätze, -standards und -verfahren im Hinblick auf deren Vollständigkeit und Übereinstimmung mit allgemein anerkannten Standards
T5.2	Beurteilung der Struktur, Implementierung und Überwachung von systembasierten und logikbasierten Sicherheitskontrollen im Hinblick auf die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
T5.3	Beurteilung der Struktur, Umsetzung und Überwachung der Datenklassifizierungsprozesse und -verfahren im Hinblick auf deren Übereinstimmung mit den Grundsätzen, Standards und Verfahren der Organisation sowie allen maßgeblichen externen Anforderungen
T5.4	Beurteilung der Struktur, Umsetzung und Überwachung der physischen und umgebungsbasierten Zugriffskontrollen im Hinblick darauf, ob die Informationswerte angemessen geschützt und gesichert sind
T5.5	Beurteilung der Prozesse und Verfahren zur Speicherung, Abrufung, Überführung und Vernichtung vertraulicher Informationswerte (z. B. Speichermedien, Auslagerung, Ausdrucke und elektronische Datenträger) im Hinblick darauf, ob die Informationswerte angemessen geschützt und gesichert sind
Fachgebiet 5: Kenntnisse	
KS5.1	Kenntnis der Techniken zur Gestaltung, Implementierung und Überwachung von Sicherheitskontrollen, einschließlich Schulungen zur Steigerung des Sicherheitsbewusstseins
KS5.2	Kenntnis der Prozesse bezüglich Überwachung und Reaktion auf Sicherheitsvorfälle (z. B. Eskalationsverfahren und Notfall-Interventionsteams)
KS5.3	Kenntnis der logikbasierten Zugriffskontrollen zur Benutzeridentifizierung und -authentifizierung und zur Beschränkung des Zugriffs auf autorisierte Funktionen und Daten
KS5.4	Kenntnis der Sicherheitskontrollen im Zusammenhang mit Hardware, Systemsoftware (z. B. Anwendungen, Betriebssysteme) und Datenbankmanagementsystemen
KS5.5	Kenntnis von Risiken und Kontrollmechanismen im Zusammenhang mit der Virtualisierung von Systemen
KS5.6	Kenntnisse in Bezug auf Konfiguration, Implementierung, Betrieb und Pflege von Netzwerksicherheitskontrollen
KS5.7	Kenntnis von Netzwerk- und Internetsicherheitseinrichtungen, -protokollen und -techniken
KS5.8	Kenntnis von Methoden und Techniken zum Angreifen von Informationssystemen
KS5.9	Kenntnis von Erkennungswerkzeugen und Kontrolltechniken (z. B. Malware, Viruserkennung, Spyware)
KS5.10	Kenntnis von Sicherheitstestverfahren (z. B. Penetrationstests, Schwachstellen-Scans)
KS5.11	Kenntnis von Risiken und Kontrollmechanismen im Zusammenhang mit Datenlecks
KS5.12	Kenntnis von Verschlüsselungstechniken
KS5.13	Kenntnis der Bestandteile einer Public-Key-Infrastruktur (PKI) und der Techniken im Zusammenhang mit der digitalen Signatur
KS5.14	Kenntnis der Risiken und Kontrollmechanismen im Zusammenhang mit Peer-to-Peer-Systemen, Instant Messaging, und webbasierten Technologien (z. B. Social Networking, Internetforen, Blogs)
KS5.15	Kenntnis der Risiken und Kontrollmechanismen im Zusammenhang mit der Verwendung mobiler und drahtloser Geräte
KS5.16	Kenntnisse in Bezug auf sichere Sprachkommunikation (z. B. PBX, VoIP)
KS5.17	Kenntnis von bei forensischen Analysen eingesetzten Beweismittelsicherungstechniken und -prozessen (z. B. IT, Prozess, Chain of Custody)
KS5.18	Kenntnis der Datenklassifizierungsstandards und der entsprechenden Verfahren
KS5.19	Kenntnis der physischen Zugriffskontrollen zur Benutzeridentifizierung und -authentifizierung und zur Beschränkung des Zugriffs auf autorisierte Funktionen
KS5.20	Kenntnis von Einrichtungen und Praktiken zum Schutz der Systemumgebung
KS5.21	Kenntnisse der Prozesse und Verfahren für Speicherung, Abruf, Überführung und Vernichtung vertraulicher Informationswerte



Vorbereitung auf die CISA-Examen 2012

CISA-Unterlagen 2012 für die Examensvorbereitung und berufliche Weiterentwicklung

Das Examen zum Certified Information Systems Auditor® (CISA®) erfordert eine gründliche und gut organisierte Vorbereitung. Um Interessenten bei der Ausarbeitung eines erfolgreichen Studienplans zu unterstützen, bietet ISACA® für Examenskandidaten folgende Studienhilfen und Vorbereitungskurse an:

Studienhilfen

- *CISA® Review Manual 2012*
- *CISA®-Handbuch 2011 – Fragen, Antworten und Erläuterungen*
- *CISA® Review Questions, Answers & Explanations Manual 2011 Supplement*
- *CISA® Review Questions, Answers & Explanations Manual 2012 Supplement*
- CISA® Practice Question Database v12

Bestellung bei www.isaca.org/cisabooks.

Examensvorbereitungskurse

- Von der lokalen ISACA®-Stelle angebotene Vorbereitungskurse (www.isaca.org/cisareview)
- Online CISA-Vorbereitungskurs (www.isaca.org/elearning)