

Verwenden Sie bitte Adobe Reader zum elektronischen Ausfüllen dieses Antrags.

INFORMATIONEN FÜR ANTRAGSTELLER

NAME DES ANTRAGSTELLERS _____ ISACA ID _____

E-MAIL _____ TELEFONNUMMER _____

SCHRITT 1. PRÜFUNG BESTEHEN

CISA-Antragsteller müssen in den letzten fünf Jahren die CISA-Prüfung bestanden haben.

Wenn Sie die CISA-Prüfung noch nicht bestanden haben, können Sie sich online unter www.isaca.org/examreg anmelden.

JAHR DER BESTANDENEN PRÜFUNG _____

SCHRITT 2. BERUFSERFAHRUNG ANGEBEN

Zur Qualifizierung als CISA müssen Sie 5 Jahre Berufserfahrung in Prüfung, Kontrolle, Assurance oder Sicherheit von Informationssystemen innerhalb der letzten 10 Jahre vor dem Antragstellungstermin haben. Diese Erfahrung muss in mindestens einem Bereich der CISA-Berufspraxisdomänen liegen, verfügbar zur Ansicht auf Seite V-2. Falls Sie die Voraussetzungen einer 5-jährigen Erfahrung in Abschnitt 2A nicht erfüllen, haben Sie ebenfalls die Wahl, Ausnahmeregelungen für Erfahrung in Abschnitt 2B und/oder 2C (bis zu höchstens 3 Jahren) einzureichen.

Abschnitt A: Berufserfahrung in Prüfung, Kontrolle, Assurance oder Sicherheit von Informationssystemen (erforderlich)

Führen Sie bitte relevante Berufserfahrung im Folgenden auf. Beginnen Sie mit Ihrer gegenwärtigen oder letzten Stelle. Lassen Sie keine Angaben frei. Wenn Sie gegenwärtig angestellt sind, schreiben Sie bitte das Datum der Antragsstellung als Enddatum.

| # | Name des Unternehmens | Berufskategorie (MM/JJ) | | Dauer der Erfahrung in CISA-Aufgaben | | CISA-Berufspraxisdomänen markieren) | | | | |
|---|-----------------------|----------------------------|----------|---|--------|--|---|---|---|---|
| | | Startdatum | Enddatum | Jahr | Monate | 1 | 2 | 3 | 4 | 5 |
| 1 | | | | | | | | | | |
| 2 | | | | | | | | | | |
| 3 | | | | | | | | | | |
| 4 | | | | | | | | | | |

(mindestens 2 Jahre erforderlich) **ABSCHNITT A GESAMTERFAHRUNG:** _____

Abschnitt B: Ausnahmeregelung für allgemeine Berufserfahrung (optional)

Für einen Antrag auf eine Ausnahmeregelung für Berufserfahrung zur Tätigkeit in allgemeinen Informationssystemen oder allgemeiner Prüfung geben Sie bitte die Einzelheiten im Folgenden an. Diese Erfahrung kann nicht während der bereits in Abschnitt A angegebenen Anstellungsdaten erworben worden sein. Es gilt eine 1-jährige Ausnahmeregelung.

Art der Ausnahmeregelung für Erfahrung (Ggf. eine Antwort auswählen) Allgemeine Prüfung Allgemeine Informationssysteme

Name des Unternehmens _____ Startdatum (MM/JJ) _____ Enddatum (MM/JJ) _____

(höchstens 1 Jahr) **ABSCHNITT B GESAMTERFAHRUNG:** _____

Abschnitt C: Ausnahmeregelungen für Ausbildungserfahrung (optional)

Für einen Antrag auf eine Ausnahmeregelung auf Basis der Ausbildungserfahrung markieren Sie bitte das entsprechende Kästchen unten und geben Sie ggfs. die Informationen der Lehranstalt ein.

*Eine Kopie Ihres Studienabschlusses, Leistungsnachweises oder Brief Ihres Colleges oder Ihrer Universität bitte dem Antrag beifügen.

**Eine Kopie Ihres CIMA- oder ACCA-Zertifikats bitte dem Antrag beifügen.

- 1-jährige Ausnahmeregelung für einen Associate-Abschluss
- 2-jährige Ausnahmeregelung für einen Bachelor, Magister oder Doktor in einem Studienfach
- 3-jährige Ausnahmeregelung für einen Magister in Informationssystemen oder einem fachbezogenen Bereich *
- 2-jährige Ausnahmeregelung für CIMA – Chartered Institute of Management Accountants, volle Zertifizierung **
- 2-jährige Ausnahmeregelung für ACCA-Mitgliedsstatus der Association of Chartered Certified Accountants **

NAME DER LEHRANSTALT: _____ STUDIENFACH: _____

(höchstens 3 Jahr) **ABSCHNITT C GESAMTERFAHRUNG:** _____

Abschnitt D: Gesamterfahrung

Gesamterfahrung aus Abschnitte A, B und C muss für den Antrag auf CISA-Zertifizierung 5 Jahre oder mehr betragen.

(Abschnitt A + Abschnitt B + Abschnitt C) **GESAMTERFAHRUNG:** _____

Verwenden Sie bitte Adobe Reader zum elektronischen Ausfüllen dieses Antrags.

SCHRITT 3. BERUFSERFAHRUNG BESTÄTIGEN

Mit dem Formular zu Erfahrungsgutachten (Seiten V-1 und V-2 dieses Antrags), bitten Sie einen Arbeitgeber, alle Erfahrungen in Schritt 2 zu bestätigen. Wenn mehr als ein Gutachter notwendig ist, können Sie zusätzliche Formulare zu Erfahrungsgutachten im Folgenden erhalten: www.isaca.org/cisaapp. Für in Abschnitt C angegebene Zertifikate oder Abschlüsse reichen Sie bitte eine Kopie des Zertifikats, Abschlusses oder Leistungsnachweises ein.

SCHRITT 4. EINREICHEN DER ZAHLUNG ZUR ANTRAGSBEARBEITUNG

Alle Antragsteller müssen eine Gebühr von USD 50,00 zur Antragsbearbeitung bezahlen, bevor der Antrag vollständig bearbeitet werden kann. Die Zahlung kann unter Folgendem geleistet werden: www.isaca.org/cisapay

SCHRITT 5. ÜBERPRÜFUNG UND UNTERZEICHNEN DER GESCHÄFTSBEDINGUNGEN

Richtlinie für die kontinuierliche berufliche Weiterbildung

Ich beantrage hiermit bei ISACA die Zertifizierung zum Certified Information Systems Auditor (CISA) gemäß den Verfahren und Richtlinien der ISACA. Ich habe die Bedingungen, die im Antrag auf Zertifizierung und in der zum Zeitpunkt meines Antrags geltenden Richtlinie für die kontinuierliche berufliche Weiterbildung (CPE-Richtlinie) festgelegt sind, gelesen und erkläre mich damit einverstanden.

Ethikkodex

Ich erkläre mich einverstanden: Nachweise für die Erfüllung der Zulassungsvoraussetzungen einzureichen; ISACA zu gestatten, Klarstellung oder weitere Bestätigung aller im Rahmen des Antrags eingereichten Informationen zu verlangen, einschließlich, aber nicht beschränkt auf direkte Kontaktaufnahme eines Experten zur Bestätigung der eingereichten Informationen; die Anforderungen zur Erlangung und Erhaltung der Zertifizierung zu erfüllen, einschließlich der Zulassungsvoraussetzungen für die Durchführung der Aufgaben eines CISA, der Einhaltung von Ethikkodex, Standards und Richtlinien der ISACA und der Vollziehung der Erneuerungsanforderungen; die ISACA Zertifizierungsabteilung umgehend zu benachrichtigen, wenn ich die Anforderungen zur Zertifizierung nicht erfüllen kann; die Aufgaben eines CISA auszuführen; Ansprüche auf die Zertifizierung nur im Rahmen, in dem die Zertifizierung gewährt wurde, geltend zu machen und das CISA-Zertifikat oder die Logos und Markenzeichen nicht auf irreführende Weise oder entgegen der ISACA-Richtlinien zu verwenden.

Richtigkeit der Informationen

Ich verstehe und erkläre mich damit einverstanden, dass mein Zertifizierungsantrag abgelehnt wird und alle mir von ISACA gewährten Berechtigungsnachweise widerrufen und hinfällig werden, falls eine der von mir abgegebenen Aussagen oder Antworten in diesem Antrag falsch sind oder falls ich gegen eine der Prüfungsregeln oder Zertifizierungsanforderungen verstoße. Ich verstehe, dass alle Zertifikate im Besitz von ISACA sind, und, wenn mir das Zertifikat gewährt und dann widerrufen wird, ich das Zertifikat zerstöre, dessen Nutzung einstelle und alle Ansprüche auf mein Anrecht auf die Zertifizierung zurückziehe. Ich bevollmächtige ISACA, alle Nachfragen und Untersuchungen anzustellen, die für die Bestätigung meiner Berechtigungsnachweise und meiner professionellen Stellung als notwendig angesehen werden.

Informationsaustausch mit Dritten

Ich erkenne an, dass, wenn mir die Zertifizierung gewährt wird, mein Zertifizierungsstatus veröffentlicht wird und von ISACA unter Umständen anfragenden Dritten mitgeteilt wird. Ich verstehe, dass ich bei Ablehnung meines Antrags bei ISACA Einspruch gegen die Entscheidung erheben kann. Wird durch einen Teilnehmer einer Zertifizierungsprüfung, einen Antragsteller auf Zertifizierung oder eine zertifizierte Person Einspruch erhoben, so erfolgt dieses nach Ermessen und auf Kosten des Prüfungsteilnehmers oder des Antragstellers. Durch Unterzeichnung dieses Dokuments bevollmächtige ich ISACA, meinen Zertifizierungsstatus bekannt zu geben. Diese Kontaktinformationen werden zur Erfüllung meiner Zertifizierungsanfragen und -anforderungen verwendet.

Kontaktrichtlinie

Durch Unterzeichnung dieses Dokuments bevollmächtige ich ISACA, Kontakt zu mir unter der angegebenen Anschrift und den angegebenen Telefonnummern aufzunehmen, und bestätige, dass die von mir angegebenen Informationen meine eigenen und richtig sind. Ich bevollmächtige ISACA, vertrauliche Informationen zum Zertifizierungsantrag und zur Zertifizierung freizugeben, wenn es gesetzlich vorgeschrieben oder in der Datenschutzrichtlinie von ISACA beschrieben ist. Mehr darüber, wie wir die von Ihnen in diesem Formular angegebenen Informationen nutzen, entnehmen Sie bitte unserer Datenschutzrichtlinie, die Sie unter www.isaca.org finden.

Nutzungsvereinbarung

Ich erkläre mich hiermit einverstanden, ISACA, ihre leitenden Angestellten, Direktoren, Prüfer, Mitarbeiter, Vertreter und die ihrer unterstützenden Organisationen von jeglicher Beschwerde, Forderung oder Schaden freizustellen, die sich aus irgendeiner Handlung oder Unterlassung durch irgendeinen von diesen in Verbindung mit diesem Antrag ergeben; der Antragsprozess; das Versäumnis, mir irgendein Zertifikat auszustellen; oder jede Forderung nach Verwirkung oder Neulieferung eines solchen Zertifikats. Ungeachtet der vorstehenden Erklärung verstehe ich und bin damit einverstanden, dass jede Klage, die sich aus oder im Zusammenhang mit diesem Antrag ergibt, beim Circuit Court of Cook County im US-Bundesstaat Illinois eingereicht werden muss und unter die Gesetze des US-Bundesstaates Illinois fällt.

Ich verstehe, dass die Entscheidung, ob ich mich für die Zertifizierung qualifiziere, einzig und allein bei ISACA liegt und dass die Entscheidung von ISACA endgültig ist.

Ich habe diese Erklärungen gelesen und verstanden und ich beabsichtige, sie als rechtsverbindlich anzuerkennen.

UNTERSCHRIFT DES ANTRAGSTELLERS: _____ DATUM: _____

SCHRITT 6. EINREICHEN DES ANTRAGS

Reichen Sie bitte Ihren Antrag, zusätzliche Formulare zum Nachweis (falls erforderlich) und alle Belegdokumente online unter <https://support.isaca.org> ein.

Wählen Sie **Certifications & Certificate Programs** und **Submit an Application** aus.

Die Bearbeitung von eingereichten Anträgen dauert etwa zwei bis drei Wochen. Nach der Zulassung werden Sie per E-Mail benachrichtigt. Ein Zertifizierungspaket, einschließlich eines Zulassungsbriefs, eines CISA-Zertifikats und einer CISA-Anstecknadel aus Metall, wird Ihnen per Post an die primäre Adresse in Ihrem ISACA- Profil geschickt. Die Auslieferung kann vier bis acht Wochen dauern.

Verwenden Sie bitte Adobe Reader zum elektronischen Ausfüllen dieses Antrags.

ANGABEN ZUM ANTRAGSTELLER

NAME DES ANTRAGSTELLERS _____ ISACA ID _____

ANLEITUNG ZUM FORMULAR

Der Antragsteller (oben genannt) beantragt eine CISA-Zertifizierung über ISACA. ISACA verlangt, dass die Berufserfahrung des Antragstellers von einem Vorgesetzten oder Manager, mit dem er gearbeitet hat, unabhängig bestätigt wird. Prüfer können weder Mitglieder aus dem engsten oder erweiterten Familienkreis noch Mitarbeiter der Personalabteilung sein.

Durch Ausfüllen dieses Formulars bestätigen Sie die Berufserfahrung des Antragstellers, wie im beigefügten Antragsformular angegeben (Seite A-1) und wie anhand von CISA-Berufspraxisdomänen und Aufgabenangaben beschrieben (Seite V-2).

Schicken Sie bitte dieses Formular zur Bestätigung an den Antragsteller zum Einreichen. Bei Fragen wenden Sie sich bitte an ISACA unter <https://support.isaca.org> oder +1.847.660.5505.

INFORMATIONEN ZUM PRÜFER

NAME DES PRÜFERS _____

NAME DES UNTERNEHMENS _____ BERUFSBEZEICHNUNG _____

E-MAIL _____ TELEFONNUMMER _____

FRAGEN FÜR DEN PRÜFER

1. Ich bescheinige die folgende Berufserfahrung des Antragstellers, siehe Seite A-1 (*alles Zutreffende markieren*):

Abschnitt A: Unternehmen 1

Abschnitt A: Unternehmen 3

Abschnitt A: Unternehmen 2

Abschnitt A: Unternehmen 4

2. Ich bescheinige die folgenden Ausnahmeregelungen, siehe Seite A-1, Abschnitte B und C (*alles Zutreffende markieren*):

Abschnitt B: Ausnahmeregelung für Berufserfahrung

Abschnitt C: Bildungsabschluss

3. Ich bescheinige die Berufserfahrung des Antragstellers während der folgenden Zeitspanne:

STARTDATUM _____

ENDDATUM _____

4. Ich habe in der folgenden Rolle (in den folgenden Rollen) mit dem Antragsteller gearbeitet:

Vorgesetzter

Manager

Kollege

Klient

5. Wenn ich eine Erfahrung in Abschnitt A bescheinige, bescheinige ich ebenfalls nach bestem Wissen, dass die vom Antragsteller ausgeführten Aufgaben, wie auf Seite V-2 dieses Formulars aufgeführt, richtig sind.

Ja

Nein

VEREINBARUNG MIT DEM PRÜFER

Ich bestätige hiermit nach bestem Wissen, dass die Informationen auf Seite V-1 und V-2 richtig sind und kein Grund vorliegt, diesen Antragsteller nicht als Prüfer für Informationssysteme zu zertifizieren. Ich bin auch bereit, ggf. Fragen von ISACA über die obigen Informationen zu beantworten.

UNTERSCHRIFT DES PRÜFERS: _____

DATUM: _____

Verwenden Sie bitte Adobe Reader zum elektronischen Ausfüllen dieses Antrags.

ANLEITUNG ZU BERUFSPRAXISDOMÄNEN

Der Antragsteller muss für jede Domäne, in der eine oder alle Aufgaben ausgefüllt wurden, sicherstellen, dass sie vom Prüfer bestätigt wurde.

DOMÄNE 1 - Verfahren zur Prüfung von Informationssystemen

Prüfungsdienstleistungen gemäß IS-Prüfungsstandards bereitstellen, um die Organisation bei Schutz und Kontrolle von Informationssystemen zu unterstützen

Aufgabenangaben:

- Eine risikobasierte IS-Prüfungsstrategie gemäß IS-Prüfungsstandards ausführen, um zu gewährleisten, dass wesentliche Risikobereiche geprüft werden.
- Spezifische Prüfungen planen, um festzustellen, ob die Informationssysteme geschützt sind und kontrolliert sind sowie für die Organisation einen Wert darstellen.
- Prüfungen gemäß IS-Prüfungsstandards durchführen, um geplante Prüfungsziele zu erreichen.
- Prüfungsergebnisse mitteilen und wichtigen Interessensvertretern in Besprechungen und Prüfungsberichten Vorschläge machen, um ggfs. Änderungen voranzutreiben.
- Folgeprüfungen durchführen oder Statusberichte erstellen, um sicherzustellen, dass das Management entsprechende Maßnahmen zeitnah ergriffen hat.

DOMÄNE 2 - IT-Governance und IT-Management

Gewährleisten, dass die notwendige Führung und Struktur und Prozesse der Organisation vorhanden sind, um die Ziele zu erreichen und die Strategie der Organisation zu unterstützen.

Aufgabenangaben:

- Die Effektivität der Struktur der IT-Governance bewerten, um festzustellen, ob IT-bezogene Entscheidungen, Richtungen und Leistung die Strategien und Ziele der Organisation unterstützen.
- Die organisatorische Struktur von IT und Management des Personals bewerten, um festzustellen, ob sie die Strategien und Ziele der Organisation unterstützen.
- Die IT-Strategie, einschließlich der IT-Leitung, und die Prozesse für die Entwicklung, Genehmigung, Implementierung und Wartung im Hinblick auf die Ausrichtung auf die Strategien und Ziele der Organisation bewerten.
- Die IT-Richtlinien, Standards und Verfahren, sowie die Prozesse für ihre Entwicklung, Genehmigung, Implementierung, Wartung und Überwachung bewerten, um festzustellen, ob sie die IT-Strategie unterstützen und die regulatorischen und gesetzlichen Anforderungen erfüllen.
- Die Angemessenheit des Qualitätsmanagementsystems bewerten, um festzustellen, ob es die Strategien und Ziele der Organisation kostengünstig unterstützt.
- IT-Management und IT-Überwachung von Kontrollen (z.B. kontinuierliche Überwachung, Qualitätssicherung [QA]) hinsichtlich der Erfüllung der Richtlinien, Standards und Verfahren der Organisation bewerten.
- IT-Management von Ressourcen, einschließlich Investitionen, Praktiken für Nutzung und Zuteilung, einschließlich Priorisierungskriterien, hinsichtlich der Ausrichtung auf die Strategien und Ziele der Organisation bewerten.
- Die vertraglichen Strategien und Richtlinien von IT und Praktiken zum Vertragsmanagement bewerten, um festzustellen, ob sie die Strategien und Ziele der Organisation unterstützen.
- Risikomanagementpraktiken bewerten, um festzustellen, ob die IT-bezogenen Risiken der Organisation ordnungsgemäß verwaltet werden.
- Überwachungs- und Sicherungspraktiken bewerten, um festzustellen, ob der Vorstand und die Führung ausreichende und zeitnahe Informationen über IT-Leistung erhalten.
- Den Business-Continuity-Plan der Organisation bewerten, um die Fähigkeit der Organisation festzustellen, während einer IT-Unterbrechung wichtige Geschäftstätigkeiten fortzusetzen.

DOMÄNE 3 - Beschaffung, Entwicklung und Implementierung von Informationssystemen

Gewährleisten, dass die Praktiken für Beschaffung, Entwicklung, Testen und Implementierung von Informationssystemen den Strategien und Zielen der Organisation entsprechen.

Aufgabenangaben:

- Den Business Case für die geplanten Investitionen zur Beschaffung, Entwicklung, Wartung und anschließenden Stilllegung von Informationssystemen bewerten, um festzustellen, ob er den Geschäftszielen entspricht.
- Die Praktiken und Kontrollen des Projektmanagements bewerten, um festzustellen, ob die Geschäftsanforderungen kostengünstig erreicht wurden, während Risiken für die Organisation verwaltet wurde.
- Überprüfungen durchführen, um festzustellen, ob ein Projekt in Übereinstimmung mit den Projektplänen Fortschritte macht, ausreichend durch Dokumentation unterstützt wird und Statusmeldungen aktuell sind.
- Kontrollen für Informationssysteme während der Phasen für Anforderungen, Beschaffung, Entwicklung und Erprobung zur Erfüllung der Richtlinien, Standards, Verfahren und entsprechende, externe Anforderungen bewerten.
- Die Bereitschaft von Informationssystemen zur Implementierung und Migration in die Produktion bewerten, um festzustellen, ob Arbeitsergebnisse des Projekts, Kontrollen und Anforderungen der Organisation erfüllt wurden.
- Überprüfungen nach der Implementierung der Systeme durchführen, um festzustellen, ob Arbeitsergebnisse des Projekts, Kontrollen und Anforderungen der Organisation erfüllt wurden.

DOMÄNE 4 - Betriebsabläufe, Wartung und Support von Informationssystemen

Gewährleisten, dass die Prozesse für Betriebsabläufe von Informationssystemen, Wartung und Support die Strategien und Ziele der Organisation erfüllen.

Aufgabenangaben:

- Regelmäßige Überprüfungen von Informationssystemen durchführen, um festzustellen, ob sie weiterhin die Ziele der Organisation erfüllen.
- Die Praktiken des Servicelevel-Managements bewerten, um festzustellen, ob das Serviceneiveau von internen und externen Dienstleistern definiert ist und verwaltet wird.
- Managementpraktiken von Dritten bewerten, um festzustellen, ob die von der Organisation erwarteten Kontrollstufen vom Dienstleister eingehalten werden.
- Betriebsabläufe und Verfahren von Endbenutzern bewerten, um festzustellen, ob geplante und nicht geplante Prozesse bis zum Ende gemanagt werden.
- Den Prozess der Wartung von Informationssystemen bewerten, um festzustellen, ob sie effektiv kontrolliert werden und weiterhin die Ziele der Organisation unterstützen.
- Praktiken zur Datenverwaltung bewerten, um die Integrität und Optimierung der Datenbanken festzustellen.
- Die Nutzung der Kapazität und Leistung der Überwachungshilfsmittel und -techniken bewerten, um festzustellen, ob IT-Services die Ziele der Organisation erfüllen.
- Praktiken zu Problem- und Störungsmanagement bewerten, um festzustellen, ob Störungen, Probleme und Fehler zeitnah erfasst, analysiert und gelöst werden.
- Praktiken zu Change-, Konfigurations- und Release-Management bewerten, um festzustellen, ob geplante oder nicht geplante, an der Produktionsumgebung der Organisation vorgenommene Änderungen angemessen kontrolliert und dokumentiert werden.
- Die Angemessenheit der Bestimmungen zu Backups und Wiederherstellungen bewerten, um die Verfügbarkeit der zur Fortsetzung der Verarbeitung erforderlichen Informationen festzustellen.
- Den Disaster-Recovery-Plan der Organisation bewerten, um festzustellen, ob er die Wiederherstellung der IT-Verarbeitungsfähigkeiten im Falle eines Notfalls aktiviert.

DOMÄNE 5 – DOMÄNE 5 – Schutz von Informationen

Gewährleisten, dass die Richtlinien, Standards, Verfahren und Kontrollen der Organisation Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sicherstellen.

Aufgabenangaben:

- Die Informationssicherheitsrichtlinien, Standards und Verfahren hinsichtlich Vollständigkeit und Ausrichtung auf allgemein akzeptierte Praktiken bewerten.
- Design, Implementierung und Überwachung von Systemkontrollen und logischen Sicherheitskontrollen bewerten, um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu bestätigen.
- Design, Implementierung und Überwachung der Datenklassifizierungsprozesse und -verfahren hinsichtlich der Ausrichtung auf die Richtlinien, Standards, Verfahren und entsprechenden, externen Anforderungen der Organisation bewerten.
- Design, Implementierung und Überwachung von physischem Zugriff und umweltbedingten Kontrollen bewerten, um festzustellen, ob Informationen angemessen geschützt sind.
- Die Prozesse und Verfahren zum Speichern, Abrufen, Transport und Löschen von Informationen (z. B. Backupmedien, externe Speicherung, Papier/Druckdaten und Datenmedien) bewerten, um festzustellen, ob Informationen angemessen geschützt sind.