CISA 자격증 신청서
2016 년 이후 CISA 시험에 합격한 지원자

Certified Information Systems Auditor®
An ISACA® Certification

이 신청서를 전자 파일 형식으로 작성하는 경우 Adobe Reader 를 사용하십시오.

지원자 정보

지원자 이름 _____ ISACA ID _____

이메일 _____ 전화번호 _____

1단계. 시험 합격

CISA 지원자는 지난 5 년 안에 CISA 시험에 합격했어야 합니다.

아직 CISA 시험에 합격하지 못한 경우, 온라인으로 등록하십시오(*www.isaca.org/examreg*).

시험 합격 연도 _____

2단계. 업무 경험 신고

CISA 자격을 갖추려면 신청서를 제출한 날짜를 기준으로 지난 10 년 내에 적어도 5 년간의 정보 시스템 감사, 통제, 보증 또는 보안 업무 경험이 있어야 합니다. 이 경력은 CISA 실무 영역 분야(V-2 페이지 참조) 중 최소 하나에 해당해야 합니다. 2A 항에서 제시한 5 년간의 경력 요구 사항에 부합하지 않는 경우에도 2B 및/또는 2C 항에 따라 경력 대체 확인서를 제출하기로 선택할 수 있습니다(최장 3 년까지).

A 항: 정보 시스템 감사, 통제, 보증 또는 보안 업무 경력(*필수*)

현직 또는 가장 최근의 직책부터 시작하여 관련 업무 경험을 아래에 나열하십시오.
날짜를 비워두지 마십시오. 현재 직장에 채용된 상태인 경우 종료일에 오늘 날짜를 기재하십시오.

		고용 기간 (MM/YY)		CISA 업무 수행 경력 기간		CISA 실무 영역 분야 (해당되는 항목 모두 선택)				
#	회사 이름	시작일	종료일	연수	개월수	1	2	3	4	5
1										
2										
3										
4										

(최소 2 년 필요) **A 항 경력 총계:** _____

B 항: 일반 업무 경력 대체(*선택*)

일반 정보 시스템 또는 일반 감사 업무 분야에서 업무 경력 대체를 신청하려면 아래 상세 정보를 작성하십시오.
이는 A 항에서 언급한 고용 기간 중에 쌓은 경력일 수 없으며, 1 년간의 경력 대체에 해당합니다.

경력 대체 유형(*해당되는 경우 하나만 선택*) ☐ 일반 감사 ☐ 일반 정보 시스템

회사 이름 _____ 시작일(*MM/YY*) _____ 종료일(*MM/YY*) _____

(최장 1 년) **B 항 경력 총계:** _____

C 항: 학력 대체(*선택*)

학력 대체를 신청하려면 아래의 해당 확인란에 체크 표시하고 학교 정보를 기입하십시오(해당되는 경우).
**신청서와 함께 전문대학 또는 대학교에서 발급한 학위증, 성적증명서 또는 서신 사본을 첨부하십시오.*
***신청서에 CIMA 또는 ACCA 자격증 사본을 첨부하십시오.*

☐ 준학사 학위증: 1 년 경력 대체
☐ 학사, 석사 또는 박사 학위증: 2 년 대체(전공 분야 무관)
☐ 정보 시스템 또는 관련 전공 분야 석사 학위증: 3 년 대체 *
☐ CIMA(Chartered Institute of Management Accountants) 자격 증서: 2 년 대체(전체 자격증) **
☐ ACCA(Association of Chartered Certified Accountants) 회원 지위: 2 년 대체 **

학교 이름: _____ 학위 유형: _____ 전공 분야: _____

(최장 3 년) **C 항 경력 총계:** _____

D 항: 경력 총계

A, B 및 C 항의 경력 총계가 **5** 년 이상이어야만 CISA 자격증을 신청할 수 있습니다.

(A 항+B 항+C 항) **경력 총계:** _____

ISACA®

CISA 자격증 신청서
2016 년 이후 CISA 시험에 합격한 지원자

이 신청서를 전자 파일 형식으로 작성하는 경우 Adobe Reader 를 사용하십시오.

3단계. 업무 경험 확인

경력 확인서(본 신청서의 V-1 및 V-2 페이지)를 사용하여 고용주에게 2 단계의 경력을 모두 확인하도록 요청하십시오. 입증자가 한 명 이상 필요한 경우 www.isaca.org/cisaapp 에서 추가로 경력 확인서를 획득할 수 있습니다. C 항에서 서술한 자격증 또는 학위증의 경우 자격증, 학위증 또는 성적증명서 사본을 제출하십시오.

4단계. 신청 처리 수수료 납부

모든 지원자는 US $50.00 의 신청 처리 수수료를 납부해야 합니다. 수수료를 접수한 후에만 신청서를 완전히 처리할 수 있습니다. 수수료는 다음 링크를 통해 납부할 수 있습니다: www.isaca.org/cisapay.

5단계. 이용약관 동의서 검토 및 서명

계속 교육(CPE) 정책
본인은 ISACA 의 절차 및 정책에 따라 ISACA 에 국제 공인 정보 시스템 감사사(CISA) 자격증을 신청합니다. 본인은 자격증 신청서 및 신청 당시 유효한 계속 교육(CPE) 정책에 명시된 자격증 프로세스 및 CPE 정책 관련 약관을 읽었으며 이에 동의합니다.

윤리강령
본인은 다음의 윤리강령에 동의합니다. 자격 요건에 부합한다는 증거 자료를 제출하고, ISACA 에 신청서에 따라 제출한 모든 정보의 정확성을 확인하거나 심층적으로 입증할 권한을 허가하며(제출한 정보를 확인해줄 전문직업인에게 직접 연락을 취하는 조치를 포함하며 이에 국한되지 않음), 자격증을 취득하여 유지하는 데 필요한 모든 요구사항을 준수하고(ISACA 윤리강령, 표준 및 정책을 준수하고 갱신된 요구사항을 충족하기 위한 한 사람의 CISA 로서의 책무를 이행하는 자격 요건 포함), 본인이 자격증 요구사항을 준수할 수 없게 되는 경우 즉시 ISACA 자격증 담당 부서에 그러한 사실을 알리고, 자격증이 인가된 범위에 관해서만 자격이 있음을 주장하고, CISA 자격증 또는 로고나 마크를 오해의 소지가 있거나 ISACA 지침에 반하는 방식으로 이용하지 않겠습니다.

정보의 진실성
본인은 이 신청서에 본인이 제공한 진술 또는 답변 중 어느 것이라도 허위이거나 시험 규칙 또는 자격증 요구사항 중 어느 하나라도 위반한 경우, 자격증 신청이 거부되고 ISACA 에서 본인에게 인가한 각종 자격증명이 철회 및 몰수됨을 이해하며 이에 동의합니다. 본인은 자격증은 모두 ISACA 의 소유임을 이해하며, 본인의 자격증이 인가되었다가 차후 철회되는 경우 자격증을 폐기하고 사용을 중단하며 자격증에 대한 본인의 권리 주장을 모두 철회한다는 사실을 이해합니다. 본인은 ISACA 에 본인의 자격증명을 확인하고 전문직업인으로서의 지위를 확인하기 위해 필요하다고 간주되는 각종 질의 및 조사를 이행할 수 있도록 권한을 부여합니다.

제 3 자 정보 공유
본인은 본인이 자격증을 인가받는 경우, 본인의 자격증 취득 상태가 공개되고 ISACA 에서는 이에 대한 질의를 제기하는 제 3 자에게 이를 공개할 수 있다는 사실을 인지합니다. 본인은 본인의 신청이 승인되지 않는 경우, ISACA 에 문의하여 해당 결정에 이의를 제기할 수 있다는 사실을 이해합니다. 자격증 시험 응시자, 자격증 신청자 또는 자격을 취득한 개인이 제기한 이의 신청은 협회 재량에 따라 실시되며, 해당 비용은 시험 응시자 또는 신청자가 부담합니다. 본인은 아래에 서명함으로써 ISACA 에 본인의 자격증 취득 상태를 공개할 권한을 부여합니다. 본 연락처 정보는 본인의 자격증 관련 질의사항 및 요청에 부응하는 데 사용됩니다.

연락처 정책
본인은 아래에 서명함으로써 ISACA 에 본 서류에 기재한 주소 및 번호로 연락을 취할 수 있도록 허가하며 본인이 제공한 정보는 본인의 소유이고 정확한 사실임을 밝힙니다. 본인은 ISACA 에 법률상 필요한 경우 또는 ISACA 의 개인정보 보호정책에 설명된 바에 따라 기밀 정보인 자격증 신청서와 자격증 정보를 공개하도록 허가합니다. ISACA 에서 귀하가 이 양식에 제공한 정보를 사용하는 방식에 대해 자세히 알아보려면 www.isaca.org/privacy 의 개인정보 보호정책을 읽어보십시오.

사용 동의
본인은 ISACA 에 협회의 임원, 이사, 시험 감독관, 직원, 에이전트 및 지원 단체의 구성원이 본 신청서, 신청 절차, 본인에게 자격증을 발급해주지 않는 행위 또는 그러한 자격증의 몰수 또는 재배송 요구와 관련한 행위 또는 부작위로 인해 발생하는 각종 불만, 청구 또는 손해 등으로 피해를 입지 않도록 면책하는 데 동의합니다. 상기 내용과는 별도로, 본인은 본 신청서에 의한 또는 이와 관련된 모든 소송은 미국 일리노이주 쿡 카운티(Cook County)의 순회법원에 제기해야 하며, 미국 일리노이주 법률을 따른다는 점을 이해하고 이에 동의합니다.

본인은 본인이 자격증을 취득할 자격이 있는지 여부를 판단할 독점적 결정권은 ISACA 에만 있으며 ISACA 의 결정은 최종적이라는 사실을 이해합니다.

본인은 이와 같은 고지문을 읽고 이해했으며 본 고지문의 법적 구속력을 따르고자 합니다.

지원자 서명: _____ 날짜: _____

6단계. 신청서 제출

신청서, 추가 확인서(필요한 경우) 및 각종 증빙 서류는 https://support.isaca.org 를 통해 온라인으로 제출해주시기 바랍니다.

자격증 및 자격증 프로그램(Certifications & Certificate Programs)을 선택하고 **신청서 제출(Submit an Application)**을 선택하십시오.

제출된 신청서를 처리하는 데는 약 2 주~3 주가 소요됩니다. 신청서가 승인되면 이메일을 통해 알림을 발송합니다. 승인 서신, CISA 자격증 및 금속 소재의 CISA 배지를 포함한 자격증 패키지를 귀하의 ISACA 프로필에 등록된 기본 주소지로 우편 발송합니다. 배송하는 데는 약 4 주~8 주가 소요될 수 있습니다.

CISA 경력 확인서
2016 년 이후 CISA 시험에 합격한 지원자

이 신청서를 전자 파일 형식으로 작성하는 경우 Adobe Reader 를 사용하십시오.

지원자 상세 정보

지원자 이름 _____ ISACA ID _____

양식 작성 지침

지원자(위에 기명)는 ISACA 를 통해 CISA 자격증을 신청합니다. ISACA 에서는 지원자의 업무 경력을 지원자와 함께 근무한 감독관 또는 관리자에 의해 객관적으로 입증하도록 요구합니다. 입증자는 지원자와 직계 또는 방계 가족 관계이거나 인사부 소속이어서는 안 됩니다.

본 양식을 작성함으로써 귀하는 지원자의 업무 경험이 해당 인물의 첨부한 신청서(A-1 페이지)에 기재된 것과 같고 CISA 실무 영역 분야 및 직무 내역(V-2 페이지)에 설명된 내용에 상응한다는 사실을 증언하는 것이 됩니다.

이 확인서를 신청자에게 반환하여 신청자 본인이 제출할 수 있도록 하시기 바랍니다. 궁금한 사항은 ISACA 에 https://support.isaca.org 또는 +1.847.660.5505 번으로 문의하십시오.

입증자 정보

입증자 이름 _____

회사 이름 _____ 직책 _____

이메일 _____ 전화번호 _____

입증자 문항

1. 본인은 본문의 A-1 페이지에 기재된 대로 신청자가 다음과 같은 업무 경력을 획득하였음을 증명합니다. *(해당되는 항목 모두 선택)*

☐ A 항: 회사 1 ☐ A 항: 회사 3

☐ A 항: 회사 2 ☐ A 항: 회사 4

2. 본인은 A-1 페이지, B 항 및 C 항에 기재된 다음의 업무 대체가 사실임을 증명합니다. *(해당되는 항목 모두 선택)*

☐ B 항: 업무 경력 대체 ☐ C 항: 학위

3. 본인은 다음 기간에 대하여 지원자의 업무 경력을 증명합니다.

시작일 _____ 종료일 _____

4. 본인은 지원자에게 다음과 같은 역할을 수행했습니다.

☐ 감독관 ☐ 관리자 ☐ 동료 ☐ 고객

5. 본인의 증언이 A 항의 경력에 대한 것인 경우, 본인은 이 양식의 V-2 페이지에 나열된 직무가 실제로 지원자가 수행한 것이며 이는 본인이 아는 한 올바른 정보라는 사실도 증명할 수 있습니다.

☐ 예 ☐ 아니요

입증자 동의서

본인은 본문 V-1 및 V-2 페이지에 기입한 정보는 본인이 아는 한 올바른 정보이며 이 지원자가 정보 시스템 감사사 자격을 얻지 못할 이유가 없다는 사실을 확인하는 바입니다. 또한 본인은 필요한 경우 위의 정보에 대한 ISACA 의 질문에 기꺼이 답할 의향이 있습니다.

입증자 서명: _____ 날짜: _____

CISA 경력 확인서
2016 년 이후 CISA 시험에 합격한 지원자

이 신청서를 전자 파일 형식으로 작성하는 경우 Adobe Reader 를 사용하십시오.

실무 영역 지침

지원자는 입증자가 확인해야 할, 본인이 완수한 직무 영역에 모두 체크 표시해야 합니다.

☐ 영역 1 - 정보 시스템 감사 프로세스

IS 감사 표준에 따라 감사 서비스를 제공하여 조직으로 하여금 정보 시스템을 보호 및 통제하도록 지원합니다.

직무 내역:

- IS 감사 표준을 준수하여 위험 기반 IS 감사 전략을 시행해 핵심 위험 영역을 감사합니다.
- 구체적인 감사 활동을 계획하여 정보 시스템이 보호, 통제되고 있으며 조직에 가치를 창출하고 있는지 판단합니다.
- IS 감사 표준을 따라 감사를 실시하여 계획한 감사 목표를 달성합니다.
- 회의를 통해 주요 이해관계자에게 감사 결과를 전달하고 권장 사항을 제시하며 감사 보고서를 작성해 필요한 경우 변화를 촉진합니다.
- 후속 조치 감사를 실시하여 경영진이 적시에 적절한 조치를 취했는지 판단합니다.

☐ 영역 2 - IT 의 거버넌스 및 관리

목표를 달성하고 조직의 전략을 지원하기 위해 필요한 리더십 및 조직 구조와 프로세스가 마련되어 있다는 보증을 제공합니다.

직무 내역:

- IT의 방향을 비롯한 IT 전략을 평가하고 전략의 개발, 승인, 구현 및 유지보수 프로세스가 조직의 전략과 목표의 방향성과 일치하는지 판단합니다.
- IT 거버넌스 구조의 효율성을 평가하여 IT 의사결정, 방향 및 성과 등이 조직의 전략과 목표를 지원하는지 판단합니다.
- IT 조직 구조 및 인사(직원) 관리 현황을 평가하여 이러한 요소가 조직의 전략 및 목표를 지원하는지 판단합니다.
- 위험 관리 실무 현황을 평가하여 조직의 IT 관련 위험 요소를 파악, 평가, 모니터링, 보고 및 관리하고 있는지 판단합니다.
- IT 관리 및 통제 모니터링 현황(예: 지속적인 모니터링, 품질 보증[QA] 등)을 평가하여 조직의 정책, 표준 및 절차를 준수하는지 판단합니다.
- 조직의 IT 정책, 표준 및 절차를 평가하고 이들의 개발, 승인, 공개/게시, 구현 및 유지보수 프로세스를 평가하여 이들 요소가 IT 전략을 지원하고 규제 및 법적 요구사항을 준수하는지 판단합니다.
- 투자, 우선순위 선정, 할당 및 사용률 등 IT 리소스 관리 현황을 평가하여 조직의 전략과 목표에 부합하는지 판단합니다.
- 투자, 우선순위 선정 및 할당 등 IT 포트폴리오 관리 현황을 평가하여 조직의 전략과 목표에 부합하는지 판단합니다.
- IT 핵심 성과 지표(KPI)의 모니터링 및 보고 현황을 평가하여 경영진이 충분한 정보를 적시에 입수하고 있는지 판단합니다.
- 조직의 비즈니스 연속성 계획(BCP)을 평가합니다. 예를 들어 IT 재해복구계획(DRP)이 BCP에 부합하는지 평가하여 조직이 IT 업무가 중단된 기간에도 필수적인 비즈니스 운영을 지속할 역량이 되는지 판단합니다.

☐ 영역 3 - 정보 시스템 획득, 개발 및 구현

정보 시스템의 획득, 개발, 테스트 및 구현 실무가 조직의 전략과 목표에 부합하고 있다는 보증을 제공합니다.

직무 내역:

- 정보 시스템 획득, 개발, 유지보수 및 이후의 사용 중단에 이르기까지 투자 제안을 위한 비즈니스 사례를 평가하여 해당 비즈니스 사례가 비즈니스 목표에 부합하는지 판단합니다.
- IT 공급업체 선정 및 계약 관리 프로세스를 평가하여 조직의 서비스 수준 및 필수적인 통제 요소에 부합하도록 합니다.
- 프로젝트 관리 프레임워크 및 통제 현황을 평가하여 비즈니스 요구사항을 비용효율적인 방식으로 달성하는 동시에 조직에 대한 위험이 잘 관리되고 있는지 판단합니다.
- 시스템을 구현한 뒤 사후 검토를 실시하여 프로젝트 산출물, 통제 요소 및 조직의 요구사항에 부합하는지 판단합니다.
- 검토를 실시하여 프로젝트가 프로젝트 계획에 따라 진행되고 있고 문서로 적절히 지원되고 있으며, 적시에 정확한 상태 보고가 이루어지고 있는지 판단합니다.
- 정보 시스템의 요구사항 수립, 획득, 개발 및 테스트 등 각 단계를 거치면서 통제 요소를 평가하여 조직의 정책, 표준, 절차 및 관련 사외 요구사항을 준수하는지 판단합니다.
- 정보 시스템이 프로덕션 환경을 위해 구현 및 마이그레이션할 준비를 마쳤는지 평가하여 프로젝트 산출물, 통제 요소 및 조직의 요구사항에 부합하는지 판단합니다.

☐ 영역 4 - 정보 시스템 운영, 유지보수 및 서비스 관리

정보 시스템의 획득, 개발, 테스트 및 구현 실무가 조직의 전략과 목표에 부합하고 있다는 보증을 제공합니다.

직무 내역:

- IT 서비스 관리 프레임워크 및 실무(사내 또는 제3자)를 평가하여 조직에서 기대하는 통제 및 서비스 수준을 준수하고 있으며 전략적 목표에 부합하는지 판단합니다.
- 정기적으로 정보 시스템 검토를 실시하여 시스템이 지속적으로 전사적 아키텍처(EA) 내 조직 목표에 부합하는지 판단합니다.
- IT 운영 현황(예: 업무 일정 예약, 구성 관리, 용량 및 성능 관리)을 평가하여 이들이 효과적으로 통제되고 있으며 조직의 목표를 지속적으로 지원하고 있는지 판단합니다.
- IT 유지보수(패치, 업그레이드) 업무를 평가하여 이들이 효과적으로 통제되고 있으며 조직의 목표를 지속적으로 지원하고 있는지 판단합니다.
- 데이터베이스 관리 실무를 평가하여 데이터베이스 무결성 및 최적화 여부를 판단합니다.
- 데이터 품질 및 수명 주기 관리를 평가하여 이들이 계속해서 전략적 목표에 부합하는지 판단합니다.
- 문제 및 사고 관리 실무를 평가하여 문제점과 사고를 예방, 탐지, 분석 및 보고하고 적시에 해결하여 조직의 목표를 지원하는지 판단합니다.
- 변경 및 릴리스 관리 실무를 평가하여 시스템과 애플리케이션에 적용되는 변경 사항이 적절히 통제되고 문서로 기록되고 있는지 판단합니다.
- 최종 사용자 컴퓨팅 현황을 평가하여 프로세스가 효과적으로 통제되고 있으며 조직의 목표를 지원하는지 판단합니다.
- IT 연속성 및 복원력(백업/복원, 재해복구계획[DRP])을 평가하여 이들이 효과적으로 통제되고 있으며 조직의 목표를 계속해서 지원하는지 판단합니다.

☐ 영역 5 - 정보 자산의 보호

조직의 정책, 표준, 절차 및 통제 요소가 정보 자산의 기밀성, 무결성 및 가용성을 보장하고 있다는 보증을 제공합니다.

직무 내역:

- 정보 보안 및 개인정보 보호정책, 표준 및 절차가 완전하고 일반적으로 인정되는 실무와 일치하며 관련 사외 요구사항을 준수하는지 평가합니다.
- 물리적, 환경적 통제 요소의 설계, 구현, 유지보수, 모니터링 및 보고 현황을 평가하여 정보 자산이 적절히 보호되고 있는지 판단합니다.
- 정보 보안 프로그램을 평가하여 효과성 및 조직의 전략과 목표에 부합하는지 판단합니다.
- 시스템과 논리적 보안 통제 요소의 설계, 구현, 유지보수, 모니터링 및 보고 현황을 평가하여 정보의 기밀성, 무결성 및 가용성을 검증합니다.
- 데이터 분류 프로세스와 절차의 설계, 구현 및 모니터링 현황을 평가하여 조직의 정책, 표준, 절차 및 관련 사외 요구사항에 부합하는지 판단합니다.
- 자산을 저장, 검색, 전송 및 폐기하는 데 쓰이는 프로세스 및 절차를 평가하여 정보 자산이 적절히 보호되고 있는지 판단합니다.