



CERTIFIED INFORMATION SECURITY MANAGER®

2012 CISM® 시험 및 자격증에
대한 응시자 안내서

2012년 CISM 시험 — 중요 일정 안내

시험 일자 — 2012년 6월 9일

조기 등록 마감일:	2012년 2월 8일
최종 등록 마감일:	2012년 4월 4일
시험 등록 변경:	4월 14일부터 4월 20일까지 변경 가능. US \$50의 비용이 부과되며 2012년 4월 20일 후에는 변경할 수 없습니다.
환불:	2012년 4월 13일까지 환불 가능. US \$100의 처리 비용이 부과되며 2012년 4월 13일 후에는 환불이 불가능합니다.
연기:	2012년 4월 20일 또는 그 이전에 접수된 연기 신청에 대해서는 US \$50의 처리 비용이 부과됩니다. 2012년 4월 21일부터 5월 24일 사이에 접수된 연기 신청에 대해서는 US \$100의 처리 비용이 부과됩니다. 2012년 5월 24일 후에는 연기할 수 없습니다.

시험 일자 — 2012년 12월 8일

조기 등록 마감일:	2012년 8월 15일
최종 등록 마감일:	2012년 10월 3일
시험 등록 변경:	10월 6일부터 10월 12일까지 변경 가능. US \$50의 비용이 부과되며 2012년 10월 12일 후에는 변경할 수 없습니다.
환불:	2012년 10월 5일까지 환불 가능. US \$100의 처리 비용이 부과되며 2012년 10월 5일 후에는 환불이 불가능합니다.
연기:	2012년 10월 12일 또는 그 이전에 접수된 연기 신청에 대해서는 US \$50의 처리 비용이 부과됩니다. 2012년 10월 13일부터 11월 21일 사이에 접수된 연기 신청에 대해서는 US \$100의 처리 비용이 부과됩니다. 2012년 11월 21일 이후에는 연기할 수 없습니다.

모든 마감일은 미국 일리노이주 시카고 시간 오후 5시(중부 표준시)를 기준으로 합니다.

2012 CISM® 시험 및 자격증에 대한 응시자 안내서
미국에서 인쇄됨

목차

소개.....	3
ISO/IEC 17024:2003에 따라 갱신되는 CISM 프로그램 인증.....	3
CISM 시험	3
CISM 시험 준비하기.....	3
CISM 시험 관리.....	4
CISM 시험 채점.....	6
CISM 시험의 문제 유형.....	6
CISM 자격증 신청	6
CISM 자격증 취득 요건.....	6
CISM 자격증 유지 요건.....	7
ISACA 직업윤리강령	7
CISM 자격증의 취소.....	7
CISM 업무 및 전문지식 내용	8

ISACA® 소개

ISACA(www.isaca.org)는 세계 160여 개 나라에 95,000명 이상의 회원을 가지고 있으며, 정보시스템(IS) 보증 및 보안, 기업의 IT 거버넌스와 경영, IT 관련 위험 및 규정 준수에 관한 지식, 자격제도 주관, 커뮤니티, 지원, 교육을 제공하는 세계적으로 인정 받는 리더입니다. ISACA는 1969년 비영리 및 독립적인 단체로 설립되어 국제회의를 개최하고 있으며, *ISACA® Journal* 발간, 국제 정보시스템 감사 및 통제 표준을 개발하여 구성원들이 정보시스템을 신뢰하고 가치를 얻는데 도움을 주고 있습니다. 이것은 또한 세계적으로 인정받고 있는 Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) 및 Certified in Risk and Information Systems Control™ (CRISC™) 자격증을 통해 IT 기술과 지식을 발전시키고 입증합니다. ISACA는 COBIT®을 지속적으로 업데이트 하여 특히 보증, 보안, 위험 치 통제 등의 분야에서 IT 전문가와 기업 리더가 IT 거버넌스 및 경영에 대한 책임을 완수하고 비즈니스에 가치를 전달할 수 있도록 도와주고 있습니다.

거부

ISACA와 CISM 자격심사위원회(Certification Committee)는 CISM 자격증을 취득하고자 하는 응시자를 위해서 *CISM® 시험 및 자격증에 대한 2012응시자 안내서*를 마련했습니다. 그러나 ISACA는 응시자가 본 안내서 또는 기타 관련 출판물을 사용할 경우 CISM 시험에 합격할 것이라는 어떠한 보장이나 진술을 하지 않습니다.

권리제한

Copyright © 2011 ISACA. ISACA의 사전 서면 허가 없이는 어떤 목적, 어떠한 형태로의 복사나 저장도 허용되지 않으며 본 저작물과 관련한 기타 어떠한 권리나 허가도 부여되지 않습니다. 모든 권리는 제한되어 있습니다.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
전화: +1.847.253.1545
팩스: +1.847.253.1443
이메일: exam@isaca.org
웹사이트: www.isaca.org

CISM® 시험 및 자격증에 대한 응시자 안내서

소개

CISM (Certified Information Security Manager) 자격 인증 프로그램은 경험 있는 정보 보안 관리자와 정보 보안 관리 책임을 담당하는 사람들을 위해 특별히 개발되었습니다.

CISM 자격증은 기업의 정보 보안을 관리하고 설계하며 감독하는 전문가를 위한 자격증으로서, 보안 관리에 중점을 두고 있으며 보안 관련 경력을 갖춘 IS 분야 종사자에게도 가치 있는 자격증입니다. CISM은 국제적 실무 능력을 증진시키고 이 자격증을 취득한 사람이 효과적인 보안 관리 및 컨설팅 서비스를 제공하기 위해 필요한 경험과 지식을 갖추고 있다는 확신을 최고 경영진에게 제공합니다. CISM 자격증을 취득한 개인은 동일한 종류의 자격을 갖춘 전문가 네트워크의 일원이 됩니다.

ISO/IEC 17024:2003에 따라 갱신되는 CISM 프로그램 인증

미 국립표준연구소(ANSI)는 ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons 에 따라 CISM 자격증을 인증했습니다. 민간 비영리 기구인 ANSI는 제3자 제품, 시스템 및 인적자원에 대한 인증기구로서 활동하는 타 기구에 인증을 부여하는 업무를 수행합니다.

ISO/IEC 17024에는 특정 요구사항에 따라 개인의 자격을 인증하는 기구가 준수해야 할 요건이 지정되어 있습니다. ANSI는 ISO/IEC 17024가 "전체적인 인증 커뮤니티의 표준을 장려하고, 국가 간의 이동성을 증대하며, 공공의 안전을 강화하고 소비자를 보호하는 데 있어 중요한 역할을 할 것으로 기대된다"고 설명합니다.



ANSI 공인 프로그램
인적자원 자격인증
#0694
ISO/IEC 17024

ANSI 인증의 의미는 다음과 같습니다.

- ISACA 자격증이 인증하는 독보적인 자격요건 및 전문성에 대한 공인
- 자격증의 무결성 보호 및 법적 대항력 부여
- 자격증 및 자격증 소지자에 대한 소비자 및 공공의 신뢰도 제고
- 국가간 또는 업계간 이동성 향상

ANSI의 인증은 ISACA의 절차가 개방성, 균형, 합치된 의견 및 공정한 프로세스를 요구하는 ANSI의 필수요건을 충족한다는 것을 의미합니다. ISACA는 본 인증을 계기로 전세계적 차원에서 CISM의 앞길에 더욱 넓은 기회의 장이 제공될 것으로 예상합니다.

CISM 시험

CISM 시험의 개발/설명

CISM 자격심사위원회(Certification Committee)가 시험 개발을 감독하고 시험 내용을 최신 상태로 유지합니다. CISM 시험 문제는 궁극적으로 시험의 수준을 향상시키도록 설계된 종합적인 프로세스를 통해 개발됩니다. 이 프로세스에는 출제자와 협력하여 문제를 개발하고 검토한 후에 CISM 자격심사위원회에 검토를 요청하는 시험개발분과위원회(Test Enhancement Subcommittee)가 포함됩니다.

실무 내용은 최근에 업데이트되었으며, 2012년 6월의 시험에 적용되며, 네 개의 영역으로 구성되어 있습니다. 영역, 관련 업무 및 전문지식 내용은 전세계 주제 전문가의 광범위한 연구 및 피드백의 결과입니다.

업무 및 전문지식 내용은 CISM에 의해 수행되는 업무 및 해당 업무를 수행하기 위해 필요한 지식을 가리킵니다. 응시자는 이러한 업무의 수행과 관련된 실무 지식을 기준으로 평가됩니다.

업데이트된 현재의 실무 분야 분석은 다음과 같은 영역 및 백분율로 구성됩니다:

- 정보보호 거버넌스(24%)
- 정보 위험성 관리 및 준수(33%)
- 정보보호 프로그램 개발 및 관리(25%)
- 정보 보안 사고 관리(18%)

유의사항: 각 영역과 함께 표시된 백분율은 해당 영역에서 시험에 출제될 중점 부문 및 문제의 비율을 나타냅니다. 각 영역의 업무 및 전문지식 내용에 대한 설명은 8-11 페이지를 참조하십시오.

시험은 1년에 두 차례 6월과 12월에 시행되며 4시간 동안 200개의 객관식 문항을 푸는 방식으로 진행됩니다. 응시자는 여러 언어 가운데 원하는 언어를 선택하여 시험을 치를 수 있습니다. 현재 제공되는 언어의 목록을 보려면 www.isaca.org/cismterminology를 방문하십시오.

CISM 시험 준비하기

체계적인 학습 계획을 통해서만 CISM 시험에 합격할 수 있습니다. ISACA는 응시자들이 성공적인 학습 계획을 수립하는 데 도움을 주기 위해 여러 가지 학습 교재 및 리뷰 과정을 제공합니다. 시험 준비에 도움이 되는 ISACA 학습 교재를 보려면 www.isaca.org/cismguide를 참조하십시오. 지리적 위치와 통관 절차에 따라 배송되는데 1-4주가 소요될 수 있으므로 조기 주문을 권장합니다. 현재의 배송 정보는 www.isaca.org/shipping을 참조하십시오.

CISM 리뷰 매뉴얼 2012(CISM Review Manual 2012)에는 시험 준비를 위해 학습에 필요한 풍부한 참고 목록이 제공되어 있습니다.

CISM® 시험 및 자격증에 대한 응시자 안내서

ISACA는 각 자격증에 해당하는 용어 뿐만 아니라 용어집을 관리합니다. 이 용어집은 www.isaca.org/glossary에서 제공됩니다.

ISACA나 CISM 자격심사위원회(Certification Committee)는 이러한 출판물이나 과정 또는 기타 관련 출판물이나 과정과 관련하여 응시자의 시험 합격에 대해 아무런 보장도 하지 않습니다.

CISM 시험 관리

ISACA는 국제적으로 인정 받은 전문적인 시험 대행 기관을 통해 CISM 시험을 구성, 관리 및 채점합니다.

시험 운영 상태에 대해 의견을 제시하고자 하는 응시자는 시험 세션 완료 시 “시험 운영 설문지(Test Administration Questionnaire)”를 작성하면 됩니다. 시험 운영 설문지는 문제지의 뒷면에 포함되어 있으며 설문지 응답 내용은 답안지 앞면에 있는 특수 코드 섹션(Grid 번호 4)의 P-S란에 기입해야 합니다.

시험장 상태나 시험 내용을 포함해 시험 운영에 대해 추가 의견이나 문제를 제시하고자 하는 응시자는 우편 또는 이메일(exam@isaca.org)로 ISACA 국제 본부에 연락해 주십시오. 이러한 의견이나 문제는 시험일로부터 2주 내에 ISACA에 수신되어야 합니다. 코멘트에는 다음과 같은 정보를 포함시켜 주십시오: 시험 ID 번호, 시험장, 시험일 및 특정 문제에 관한 관련 상세 사항. 시험 실시 후 첫 2주 동안 ISACA에 수신된 의견들만 시험의 최종 채점 과정에서 고려됩니다.

응시 허가증

CISM 시험일 약 2-3주 전에 ISACA에서 발송한 응시 허가증 및 전자티켓(e-ticket)을 받습니다. 시험 응시자는 웹 사이트의 www.isaca.org > MyISACA 페이지에서 응시 허가증을 다운로드할 수 있습니다. 티켓에는 날짜, 등록일 및 시험장 위치, 시험 당일 일정 및 CISM 시험을 치르기 위해 지참해야 하는 자료들에 관한 정보가 포함되어 있습니다. 연락처 정보가 변경된 경우를 제외하고, 응시자는 응시 허가증에 기입을 해서는 안됩니다.

유의사항: 응시 허가증을 받기 위해서는 모든 비용을 지불해야 합니다. 응시 허가증은 현재의 우편 주소 및 이메일 주소로 인쇄물 또는 파일로 보내 집니다. 응시 허가증 및 정부 발행 신분증을 지참한 응시자만이 시험을 치를 수 있으며, 응시 허가증의 이름은 정부 발행 신분증의 이름과 일치해야 합니다. 인쇄된 응시 허가증 또는 전자티켓으로 시험을 치를 수 있습니다. 응시자의 우편 및/또는 이메일 주소가 변경된 경우에는 ISACA 웹사이트(www.isaca.org)에서 프로파일을 업데이트하거나 exam@isaca.org로 연락하십시오.

응시자들은 응시 허가증에 기재되어 있는 등록 및 시험 시간을 숙지해야 합니다. 시험 개시 약 30분 전 시험 감독관이 지시 사항을 읽기 시작한 다음에는 어떤 응시자도 시험 센터에 입실할 수 없습니다. 지시 사항을 읽기 시작한 후에 도착한 응시자는 시험에 응시할 수 없으며 등록비는 환불되지 않습니다. 응시 허가증은 응시 허가증에 지정된 시험 센터에서만 사용할 수 있습니다. 시험 실시중에 신분증을 확인합니다.

특별 지원

요청이 있을 경우, ISACA는 진단서로 증명된 신체장애나 종교적인 요구사항을 가지고 있는 응시자에게 시험 절차와 관련하여 필요한 도움을 제공합니다. 이들 응시자는 시험장에서의 음식 및 음료의 섭취나 시험 형식, 표현 상의 합당한 변경 또는 시험 일정의 변경을 요청할 수 있습니다. 시험장에서의 음식이나 음료 요청은 의사의 소견이 있어야만 합니다. 그렇지 않은 경우 **어떤 시험장에서도 음식이나 음료의 반입이 허용되지 않습니다.** 2012년 6월 시험의 경우 2012년 4월 4일 전까지, 2012년 6월 시험의 경우 2012년 4월 4일 전까지, 2012년 12월 시험의 경우 2012년 10월 3일 전까지 구비서류를 첨부하여 ISACA 국제 본부에 서면으로 요청해야 합니다.

시간을 엄수하십시오.

등록은 각 센터에서 응시 허가증에 기재된 시간에 시작됩니다. 모든 응시자는 시험 감독관이 지시 사항을 읽기 시작하기 전에 등록을 마치고 시험 센터룸에 입실해야 합니다. **시험 개시 약 30분 전 시험 감독관이 지시 사항을 읽기 시작한 다음에는 어떤 응시자도 시험 센터에 입실할 수 없습니다.**

응시 허가증을 반드시 지참하십시오.

응시 허가증 및 전자티켓(e-ticket)은 지정된 시험 센터에서만 사용할 수 있습니다. 응시자는 유효한 응시 허가증과 인정되는 신분증(ID)을 소지하고 있어야 시험 센터에 입실이 가능합니다. 응시 허가증에 명시된 이름과 동일한, 응시자의 이름과 사진이 부착된 정부에서 발행한 원본 신분증만 허용됩니다. 수기로 작성된 정보가 포함된 ID는 허용되지 않습니다. 하나의 신분증에 이름과 사진이 모두 포함되어 있어야 합니다. 이러한 신분증의 예로는 여권, 운전 면허증, 전역증, 주 신분증(State ID), 영주권(Greencard) 및 주민등록증(National ID) 등이 포함됩니다(이에 국한되지는 않음). 허용되는 신분증을 제시하지 않는 응시자는 시험에 응시할 수 없으며 등록비는 환불되지 않습니다.

CISM® 시험 및 자격증에 대한 응시자 안내서

시험 센터의 규칙을 준수하십시오.

- 응시자는 지시 사항을 읽기 시작한 다음에는 시험 센터에 입실할 수 없습니다.
- 응시자는 2번 또는 HB 연필 여러 자루와 지우개를 지참해야 합니다. 시험 센터에서는 연필과 지우개를 제공하지 않습니다. 시험장이 다양하기 때문에 각 시험장에서는 적절한 온도 조절을 위해 최선을 다할 것입니다. 응시자는 본인이 편한 복장을 착용해야 합니다.
- 응시자는 참고 자료, 백지, 메모지 또는 사전들을 시험 센터에 반입할 수 없습니다.
- 응시자는 계산기를 시험 센터에 반입하거나 시험 센터에서 사용할 수 없습니다.
- 응시자는 어떤 종류의 통신기기(예: 휴대폰, PDA, BlackBerry)도 시험 센터에 반입할 수 없습니다. **시험 실시중에 그런 장치를 가진 응시자가 있다면 시험은 무효가 되며 시험장에서 즉시 퇴실하도록 요청을 받습니다.**
- 시험 센터에서는 방문자를 허용하지 않습니다.
- 시험 센터에는 음식이나 음료의 반입이 허용되지 않습니다(ISACA의 사전 승인이 없는 경우).

부정 행위

도움을 주고 받거나, 노트, 종이 또는 기타 보조물을 사용하거나, 다른 사람을 대신하여 시험을 치르거나, 시험 실시중에 휴대전화를 포함한 어떤 종류의 통신 장치를 사용하거나, 시험실로부터 시험 문제지, 답안지 또는 노트를 가져가는 등 어떤 종류의 부정 행위에 관여한 것으로 밝혀진 응시자는 자격이 박탈되며 법적 조치를 받게 됩니다. 시험 감독관의 허가 또는 동승없이 시험장을 벗어나는 응시자는 시험장에 복귀할 수 없으며, 시험 자격이 박탈됩니다. 시험 대행 기관은 이런 부정 행위를 ISACA의 CISM 자격심사위원회(CISM Certification Committee)에 보고할 것입니다.

개인 물품 관련 정책(Personal Belongings Policy)은 www.isaca.org/cismbelongings에서 확인할 수 있습니다. ISACA 및 시험 회사는 응시자의 개인 소지품에 대해 책임을 지지 않습니다.

답안지 작성 시 주의하십시오.

- 시험을 시작하기 전에 시험 센터의 시험 감독관이 답안지에 신상 정보를 기입하라는 지시 사항을 큰 소리로 읽습니다. 응시자의 식별 번호 및 기타 요구되는 모든 정보를 응시 허가증에 기재된 대로 정확하게 기입하십시오. 그렇지 않을 경우 채점 및 성적 통보가 지연될 수 있습니다.
- 각 시험 센터에는 해당 시험 센터에서 사용되는 기본 언어를 구사하는 시험 감독관이 있습니다. 응시자가 시험 센터의 기본 언어가 아닌 언어로 시험을 치르고자 할 경우 응시자가 선택한 언어로 시험 감독관과 의사 소통이 불가능할 수 있습니다. 그러나, 지시 사항은 시험 언어로 작성되어 제공됩니다.
- 응시자는 문제를 풀기 전에 모든 지시 사항을 주의깊게 읽고 이해해야 합니다. 지시 사항을 건너뛰거나 너무 빨리 읽을 경우 중요한 정보를 놓치고 감점될 수 있습니다.
- 모든 답은 답안지의 적절한 원에 표기해야 합니다. 응시자는 한 문제에 두 개 이상의 답을 표기하지 않도록 주의하고 정확한 행에 답을 표기해야 합니다. 답을 변경해야 할 경우에는 이전의 답을 완전히 지우고 새 답을 표기해야 합니다.
- 모든 문제에 답을 표기하십시오. **답이 틀려도 감점은 없습니다. 정답의 개수만을 기준으로 채점이 이루어지므로 답란을 비워두지 마십시오.**
- 답안 작성을 완료한 응시자는 문제지와 답안지를 제출해야 합니다.

시간을 적절하게 배분하십시오.

- 전체 시험 시간은 4시간으로 한 문제에 사용할 수 있는 시간은 1분이 조금 넘습니다. 응시자는 전체 시험을 완료하기 위해 속도를 적절히 조절해야 합니다. 한 시간에 평균 50개의 문제를 풀어야 합니다.
- 응시자는 답안지에 바로 답을 기입하는 것이 좋습니다. **문제지에 답을 표기한 경우 시험 시간이 경과한 후에는 답을 옮겨적을 시간이 따로 주어지지 않습니다.**

적절하게 행동하십시오.

- 시험을 안전하게 보호하고 점수의 유효성을 유지하기 위해 응시자는 답안지에 서명해야 합니다.
- CISM 자격심사위원회(Certification Committee)는 도움을 주고 받거나, 노트, 종이 또는 기타 보조물을 사용하거나, 다른 사람을 대신하여 시험을 치르거나, 시험 자료 또는 노트를 시험장 외부로 반출하는 등 모든 종류의 부정 행위 또는 시험 규정 위반에 관여한 것으로 밝혀진 응시자의 자격을 박탈할 수 있는 권한을 보유하고 있습니다. 시험 대행 기관은 이러한 부정 행위에 관한 기록을 CISM 자격심사위원회에서 검토하고 결정을 내릴 수 있도록 제출합니다.

퇴실 또는 자격 박탈 사유

- 시험 센터에 무단 입실한 경우
- 소란을 일으키거나 도움을 주고 받은 경우
- 시험 자료 또는 노트를 시험장 외부로 반출한 경우
- 다른 응시자를 사칭한 경우
- 허가되지 않은 물품을 시험 센터에 반입한 경우
- 시험 실시중에 응시자가 통신 장비(예를 들면 휴대전화, PDA, BlackBerry®)를 소지한 경우
- 응시자가 무단으로 시험장을 벗어나는 경우

시험 실시중에 응시자가 어떠한 장치(예를 들면 휴대전화, PDA, BlackBerry®)라도 가진 것이 밝혀진다면 시험은 무효화 되며 시험장에서 즉시 퇴실하도록 요청을 받습니다.

CISM® 시험 및 자격증에 대한 응시자 안내서

CISM 시험 채점

CISM 시험은 200개의 객관식 문항으로 구성됩니다. 응시자의 점수는 척도조정 점수로서 통보됩니다. 척도조정 점수는 응시자의 시험 점수를 공통 척도에 맞게 변환한 것입니다. 응시자는 시험에 합격하기 위해 450점 이상의 점수를 받아야 합니다. 예를 들어, 척도조정 점수 800점은 모든 문제를 맞춘 경우 즉, 만점을 가리키며 척도조정 점수 200점은 가장 낮은 점수로서 적은 수의 문제를 맞춘 경우를 가리킵니다. 450점은 CISM 자격심사위원회(Certification Committee)가 정립한 기준으로서 일관성 있는 최소한의 지식 수준을 의미합니다. 합격 점수를 받은 응시자는 기타 요구사항들이 모두 충족될 경우 자격증을 신청할 수 있습니다.

CISM 시험에는 연구와 분석용으로만 만들어진 문제가 일부 포함되어 있습니다. 이러한 문제는 별도로 표시되지 않으며 최종 점수 계산에 이용되지 않습니다.

시험일로부터 약 8주 후에 공식적인 시험 결과가 응시자에게 발송됩니다. 또한, 응시자가 등록 과정에서 동의한 경우, 응시자의 합격/불합격 상태와 점수가 포함된 이메일이 응시자에게 발송됩니다. 이 이메일 통지는 시험 결과의 최초 발표 시에 응시자의 프로파일에 명시된 주소로만 발송됩니다. 점수의 기밀을 보장하기 위해 전화나 팩스로는 시험 결과가 통보되지 않습니다. 이메일 통지가 스팸 폴더로 보내지는 것을 방지하기 위해 응시자들은 exam@isaca.org를 주소록, 허용 목록 또는 안전한 발송자 목록에 추가해야 합니다.

응시자는 영역별 부분 점수가 포함된 시험 성적표를 받게 됩니다. 시험에 합격한 응시자에게는 CISM 자격증 신청 방법에 대한 정보가 시험 성적표와 함께 발송됩니다.

시험 영역 점수는 불합격한 응시자가 다시 시험을 치르기 전에 어떤 영역에서 추가 학습이 필요한지 확인하는 데 유용합니다. 단, 시험 영역 점수의 평균이나 가중 평균을 계산하더라도 전체 척도조정 점수는 알 수 없습니다.

시험에 불합격한 응시자는 답안지의 수동 채점을 요청할 수 있습니다. 수동 채점을 통해 답안지에 잘못된 표기, 다중 응답 또는 기타 컴퓨터 채점에 방해가 되는 문제가 없는지 확인할 수 있습니다. 그러나, 모든 점수는 통보 전에 여러 번의 확인 절차를 거치기 때문에 다시 채점해도 점수가 변경되는 경우는 거의 없습니다. 수동 채점은 시험 결과 통보 후 90일 내에 자격증 관리부서에 서면으로 요청해야 합니다. 마감일 후에 수동 채점을 요청하는 경우에는 처리되지 않습니다. 모든 요청에는 응시자의 이름, 시험 식별 번호 및 우편 주소가 포함되어야 합니다. 요청시마다 US \$75의 비용을 지불해야 합니다.

CISM 시험의 문제 유형

CISM 시험 문제는 실무 지식과 일반 개념 및 표준의 적용 수준을 측정하고 평가하기 위한 의도에서 개발됩니다. 모든 문제는 객관식이며 정답이 하나만 있도록 만들어 집니다.

각각의 CISM 문제에는 하나의 기본 질문과 네 개의 보기가 있습니다. 응시자는 보기 가운데 정답 또는 가장 적합한 답을 선택해야 합니다. 질문은 의문형 또는 미완성 문장의 형태입니다. 일부의 경우 시나리오 또는 서술 문제가 포함될 수도 있습니다. 이러한 질문에는 일반적으로 상황에 대한 설명이 포함되며 응시자는 제공된 정보를 바탕으로 두 개 이상의 문제를 풀어야 합니다. 응시자는 각 질문을 주의깊게 읽어야 합니다. CISM 시험 문제에서 응시자는 **가장 적합한** 또는 **최적의**와 같은 한정어를 기준으로 정답을 선택해야 합니다. 모든 경우, 응시자는 질문을 주의깊게 읽고 확실한 오답을 제외한 다음 최대한 가장 적합한 답을 선택해야 합니다. www.isaca.org/cismassessment에 CISM 시험 문제의 견본이 나와 있습니다.

CISM 자격증 신청

시험에 합격한다고 해서 바로 CISM이 되는 것은 아닙니다. CISM 시험에 합격한 경우 시험일로부터 5년 내에 자격증을 신청할 수 있습니다. 시험에 합격한 응시자는 자격증 신청서를 작성하고 신청서에 포함된 적절한 양식을 사용하여 경력을 증명해야 합니다. **응시자는 자격증 신청서가 접수되고 승인되기 전에는 CISM 자격증을 사용할 수 없습니다.** 자격증 신청 거절을 할 수 있는 승인 절차가 남아 있으므로 신청서에 대한 결정이 최종 결정이 아님을 주지하십시오. 자격증 거절에 관한 문의 사항은 certification@isaca.org 로 이메일을 보내십시오. 인증이 완료되면, 새로운 CISM은 자격증과 CISM 인증 편을 받게 됩니다. 신청자는 또한 자격증 신청 시 ISACA가 신청자의 CISM 상태를 발표하거나 다른 방법으로 공개할 수 있는 권리를 보유하고 있음을 인정해야 합니다. 단, ISACA가 CISM 상태를 반드시 공개해야 할 의무는 없습니다. CISM 자격증 신청시 50달러의 취급 수수료를 납부해야 합니다.

CISM 자격증 취득 요건

CISM 자격증 취득은 CISM 시험에 합격하고 다음과 같은 경력 요건을 충족한 경우에 부여됩니다.

CISM 자격증은 세 개 이상의 실무 분야에서 3년 이상의 정보 보안 관리 경력을 가지고 있는 5년 이상의 정보 보안 경력자에게만 부여됩니다. 일반 정보 보안 경력은 대체가 가능하지만 정보 보안 관리 경력은 대체할 수 없습니다.

CISM® 시험 및 자격증에 대한 응시자 안내서

경력 대체

다른 보안 자격증 및 정보 시스템 관리 경력을 사용하여 최대 2년의 정보 보안 관리 경력을 대체할 수 있습니다.

다음 중 한 가지 자격을 취득한 경우 2년의 정보 보안 관리 경력을 대체할 수 있습니다.

- 유효한 CISA (Certified Information Systems Auditor) 자격증
- 유효한 CISSP (Certified Information Systems Security Professional) 자격증
- 정보 보안 또는 관련 분야(예: 경영학(business administration), 정보 시스템(information systems), 정보 보증(information assurance))의 석사(Postgraduate) 학위

또는

다음과 같은 경력이 있는 경우 1년의 정보 보안 관리 경력을 대체할 수 있습니다.

- 만 1년의 정보 시스템 관리 경력
- 만 1년의 일반 보안 관리 경력
- 기술 기반 보안 자격증[예: SANS' GIAC(Global Information Assurance Certification), MCSE(Microsoft Certified Systems Engineer), CompTIA Security+, Disaster Recovery Institute CBCP(Certified Business Continuity Professional), ESL IT Security Manager]

예를 들어, CISA나 CISSP 자격증을 보유한 지원자는 해당 자격증으로 최대 2년 간의 경력을 대체할 수 있습니다. 그러나, 이 경우 지원자는 4가지 실무 분야 중 3가지 분야에서 최소 3년 간의 정보 보안 관리 능력을 가지고 있어야 합니다.

예외: 정보 보안 관리 분야 전임강사 경력의 경우 매 2년의 경력이 1년의 정보 보안 관리 경력으로 대체됩니다.

경력은 CISM 자격증 신청일 전 10년 이내 또는 최초로 시험에 합격한 날로부터 5년 이내의 경력이어야 합니다. 시험에 합격한 날로부터 5년 안에 CISM 자격증 신청서를 모두 제출하지 않은 경우에는 다시 시험을 치르고 시험에 합격해야 합니다.

중요한 것은 지원자들이 경력 요건을 충족하기 전에 CISM 시험을 치를 수 있다는 것입니다. 모든 요구사항을 충족하기 전에는 CISM 자격증이 부여되지 않지만 이러한 방법은 허용되며 동시에 장려됩니다.

CISM 자격증 유지 요건

CISM은 자격증을 유지하기 위해 다음과 같은 요건을 충족해야 합니다.

- 연간 20시간 이상의 CPE 교육 이수 및 보고 및 3년의 보고 기간 동안 120시간 이상의 CPE 교육 이수 및 보고. 자세한 내용은 www.isaca.org/cismcpepolicy의 CISM CPE 정책 페이지를 방문하십시오.
- 매년 ISACA 국제 본부에 CISM CPE 유지비 납부
- 연례 감사 대상으로 선정된 경우 보고한 시간을 입증하기 위해 필요한 CPE 활동 서류 제출
- ISACA 직업윤리강령 준수

이러한 일반 요건을 준수하지 못할 경우 CISM 자격증이 취소될 수 있습니다. 모든 자격증의 소유권은 ISACA에 있습니다. 개인이 자격증 승인을 받은 후에 이것이 취소된 경우, 자격증을 소유한 개인은 자격증을 폐기해야 합니다.

ISACA 직업윤리강령

ISACA는 아래와 같은 직업윤리강령(Code of Professional Ethics)을 통해 협회 회원 및 자격증 소지자의 직업적이고 개인적인 행위에 대한 지침을 제시합니다. 이러한 직업윤리강령(Code of Professional Ethics)을 준수하지 못할 경우 회원 및/또는 자격증 소지자의 행위에 대한 조사에 이어 궁극적으로 징계 조치가 취해질 수 있습니다. 직업윤리강령 준수에 대한 ISACA 코드는 www.isaca.org/ethics에서 참조하실 수 있습니다.

CISM 자격증의 취소

CISM 자격심사위원회(Certification Committee)는 다음과 같은 경우 적절하고 철저한 검토를 거친 후 재량에 따라 CISM 자격증을 취소할 수 있습니다.

- CISM CPE 정책을 준수하지 못한 경우
- ISACA 직업윤리강령(Code of Professional Ethics)의 조항을 위반한 경우
- 관련 정보를 위조하거나 고의로 제공하지 않은 경우
- 중요한 사실을 고의적으로 잘못 진술한 경우
- CISM 시험 또는 인증 프로세스에 관련하여 부정적이거나, 인가되지 않거나 부적절한 행위에 관여하거나 다른 사람을 도운 경우

CISM® 시험 및 자격증에 대한 응시자 안내서

CISM 실무 분야에 대한 설명

CISM 업무 및 전문지식 내용

영역(부문)
영역 1—정보 보안 거버넌스(24%) —정보 보안 전략이 비즈니스 목적과 목표에 부합하고, 정보 위험성이 적절히 관리되고, 프로그램 리소스가 책임감 있게 관리될 수 있도록 정보 보안 거버넌스 기본 구조 및 지원 절차를 확립하고 관리합니다.
업무 내용
1.1 정보 보안 프로그램의 확립 및 현행 관리를 안내하기 위한 비즈니스 목적과 목표에 부합하는 정보 보안 전략을 확립하고 관리합니다.
1.2 정보 보안 전략을 지원하는 활동을 안내하기 위한 정보 보안 거버넌스 기본 구조를 확립하고 관리합니다.
1.3 정보 보안 프로그램에 의해 비즈니스 목표와 목적이 지원될 수 있도록 정보 보안 거버넌스를 기업 거버넌스에 통합합니다.
1.4 경영진의 지시를 전달하고 표준, 절차 및 지침의 개발을 안내하기 위한 정보 보안 정책을 확립하고 관리합니다.
1.5 정보 보안 부문의 투자를 지원할 수 있는 비즈니스 사례를 개발합니다.
1.6 조직에 대한 내부적 및 외부적 영향(예를 들어, 기술, 비즈니스 환경, 위험 허용수준, 지리적 위치, 법적 및 규정 요건)을 파악해서 이러한 요인이 정보 보안 전략에 의해 해결되도록 합니다.
1.7 정보보안 전략의 성공적인 실현 가능성을 극대화하기 위해 고위 경영진의 참여와 기타 이해관계자로부터의 지원을 이끌어낸다.
1.8 명확한 책임과 권한 수준을 정립하기 위해 조직 전반에 걸쳐 정보보안의 역할과 책임을 정의해야 한다.
1.9 정보보안 전략의 효율성과 관련된 정확한 정보를 경영진에게 제공하기 위해 측정기준(예를 들어, 핵심 목표 지표[KGI], 핵심성과지표[KPI], 핵심 위험 지표[KRI])을 확립, 모니터, 평가 및 보고한다.
전문지식 내용
KS1.1 정보 보안 전략을 개발하는 방법에 대한 지식
KS1.2 보안 및 비즈니스 목표, 목적, 기능, 절차 및 사례 사이의 관계에 대한 지식
KS1.3 정보 보안 거버넌스 프레임워크를 구현하는 방법에 대한 지식
KS1.4 거버넌스에 대한 기본적인 개념과 정보 보안과의 관련성에 대한 지식
KS1.5 정보 보안 거버넌스를 기업 거버넌스에 통합하는 방법에 대한 지식
KS1.6 정보 보안 거버넌스 및 전략 개발과 관련하여 세계적으로 널리 알려진 표준, 프레임워크 및 우수 사례 등에 대한 지식
KS1.7 정보 보안 정책을 개발하는 방법에 대한 지식
KS1.8 비즈니스 사례를 개발하는 방법에 대한 지식
KS1.9 전략적 예산 기획 및 보고 방법에 대한 지식
KS1.10 조직에 대한 내부적 및 외부적 영향(예를 들어, 기술, 비즈니스 환경, 위험 허용수준, 지리적 위치, 법적 및 규정 요건) 및 이러한 요인이 정보 보안 전략에 미치는 영향에 대한 지식
KS1.11 고위 경영진의 참여와 기타 이해관계자로부터의 지원을 이끌어 내는 방법에 대한 지식
KS1.12 정보 보안 관리 역할 및 책임에 대한 지식
KS1.13 조직적 구조 및 권한 계통에 대한 지식
KS1.14 조직 전반에 걸쳐 보고 및 통신 채널을 구축하거나 기존의 것을 이용하는 방법에 대한 지식
KS1.15 측정 기준(예를 들어, 핵심 목표 지표[KGI], 핵심 성과 지표[KPI], 핵심 위험 지표[KRI])을 선택, 구현 및 해석하는 방법에 대한 지식
영역 2—정보 위험성 관리 및 준수(33%) —조직의 사업 및 준수 요건을 충족할 수 있도록 정보 위험성을 허용 가능한 수준으로 관리합니다.
업무 내용
2.1 자산을 보호하기 위해 취해진 조치가 비즈니스 가치에 비례하도록 정보 자산 분류를 위한 프로세스를 구축하고 관리합니다.
2.2 규정 위반의 위험성을 허용 가능한 수준으로 유지할 수 있도록 법률, 규제, 조직 및 기타 해당 요건을 파악합니다.
2.3 조직의 정보에 대한 위험성을 파악하기 위해 위험성 평가, 취약성 평가 및 위협 분석 등이 정기적이고 지속적으로 실시되도록 합니다.
2.4 위험성을 허용 가능한 수준으로 관리할 수 있도록 적절한 위험성 처리 옵션을 결정합니다.
2.5 정보 보안 통제가 적절한지 여부와 이것이 위험성을 허용 가능한 수준으로 효과적으로 완화하는지 평가합니다.

CISM® 시험 및 자격증에 대한 응시자 안내서

영역(부문)
영역 2—정보 위험성 관리 및 준수(계속)
2.6 위험성을 허용 가능한 수준으로 관리하기 위해 현재의 위험성과 원하는 위험성 수준 사이의 격차를 파악합니다.
2.7 조직 전반에 걸쳐 지속적이고 포괄적인 정보 위험성 관리 프로세스를 촉진하기 위해 정보 위험성 관리를 비즈니스 및 IT 프로세스(예를 들어, 개발, 조달, 프로젝트 관리, 합병 및 인수)에 통합합니다.
2.8 변경 사항이 적절하게 식별되고 관리될 수 있도록 기존 위험성을 모니터링합니다.
2.9 위험성 관리 의사 결정 프로세스를 지원하기 위해 규정 위반 및 정보 위험성의 기타 변동 사항을 해당 경영진에게 보고합니다.
전문지식 내용
KS2.1 비즈니스 목적에 부합되는 정보 자산 분류 모델을 확립하기 위한 방법에 대한 지식
KS2.2 정보 자산 및 위험성의 책임과 소유권을 할당하기 위해 사용되는 방법에 대한 지식
KS2.3 불법 이벤트가 비즈니스에 미치는 영향력을 평가하는 방법에 대한 지식
KS2.4 정보 자산 평가 방법론에 대한 지식
KS2.5 정보 보안과 관련된 법률, 규제, 조직 및 기타 요건에 대한 지식
KS2.6 새로 발생하는 정보 보안 위협 및 취약성에 관한 정보의 저명하고, 믿을 수 있고, 시기 적절한 공급원에 대한 지식
KS2.7 정보 보안 프로그램 요소의 위험성 평가 및 변경을 요구하는 이벤트에 대한 지식
KS2.8 정보 위협, 취약성 및 노출과 이것의 발전 성격에 대한 지식
KS2.9 위험성 평가 및 분석 방법론에 대한 지식
KS2.10 위험성 우선 순위에 사용되는 방법에 대한 지식
KS2.11 위험성 보고 요건(예를 들어, 주기, 대상, 구성 요소)에 대한 지식
KS2.12 위험성을 모니터링하기 위해 사용되는 방법에 대한 지식
KS2.13 위험성 처리 전략과 이것을 적용하는 방법에 대한 지식
KS2.14 기준 모델링 및 이러한 모델링의 위험성 기반 평가와의 관계에 대한 지식
KS2.15 정보 보안 통제 및 대응책과 이것의 효과성 및 효율성을 분석하기 위한 방법에 대한 지식
KS2.16 정보 보안과 관련된 격차 분석 기술에 대한 지식
KS2.17 위험 관리를 비즈니스 및 IT 프로세스에 통합하기 위한 기술에 대한 지식
KS2.18 규정 준수 보고 프로세스 및 요건에 대한 지식
KS2.19 위험성 처리 옵션을 평가하기 위한 비용 효익 분석에 대한 지식
영역 3—정보 보안 프로그램 개발 및 관리(25%) —정보 보안 전력을 구현하기 위한 정보 보안 프로그램을 작성 및 관리합니다.
업무 내용
3.1 정보 보안 전략을 구현하기 위한 정보 전략 프로그램을 작성 및 관리합니다.
3.2 비즈니스 프로세스와의 통합을 지원할 수 있도록 정보 보안 프로그램과 기타 비즈니스 기능(예를 들어, 인사[HR], 회계, 조달 및 IT) 간의 연결을 보증합니다.
3.3 정보 보안 프로그램을 실행하기 위해 내부 및 외부 자원에 대한 요건을 식별, 구입, 관리 및 정의합니다.
3.4 정보 보안 프로그램을 실행하기 위한 정보 보안 아키텍처(인력, 프로세스, 기술)를 확립하고 관리합니다.
3.5 정보 보안 정책의 규정 준수를 지원하고 안내하기 위해 조직의 정보 보안 표준, 절차, 지침 및 기타 문서를 확립, 전달 및 관리합니다.
3.6 보안 환경 및 효과적인 보안 문화를 홍보하는 정보 보안 인식 및 훈련을 위한 프로그램을 확립하고 관리합니다.
3.7 조직의 보안 기준을 유지할 수 있도록 정보 보안 요건을 조직의 프로세스(예를 들어, 변경 관리, 합병 및 인수, 개발, 사업 기회, 재난 복구)에 통합합니다.
3.8 조직의 보안 기준을 유지하기 위해 정보 보안 요건을 제3자의 계약 및 활동(예를 들어, 공동 사업, 아웃소싱 제공업체, 사업 파트너, 고객)에 통합합니다.
3.9 정보 보안 프로그램의 효과성 및 효율성을 평가하기 위해 프로그램 관리 및 운영의 측정 기준을 확립하고, 모니터링하고, 정기적으로 보고합니다.

CISM® 시험 및 자격증에 대한 응시자 안내서

영역(부문)
전문지식 내용
KS3.1 정보 보안 프로그램 요건을 다른 사업 기능과 연계하는 방법에 대한 지식
KS3.2 내부 및 외부 자원에 대한 요건을 파악, 구매, 관리 및 정의하기 위한 방법에 대한 지식
KS3.3 정보 보안 기술, 최신 동향(예를 들어, 클라우드 컴퓨팅, 모바일 컴퓨팅) 및 배경 개념에 대한 지식
KS3.4 정보 보안 통제를 설계하는 방법에 대한 지식
KS3.5 정보 보안 아키텍처(예를 들어, 인력, 프로세스, 기술) 및 이것을 적용하는 방법에 대한 지식
KS3.6 정보 보안 표준, 절차 및 지침을 개발하는 방법에 대한 지식
KS3.7 정보 보안 정책, 표준, 절차 및 지침을 구현하고 전달하는 방법에 대한 지식
KS3.8 효과적인 정보 보안 인식 및 훈련 프로그램을 정립하는 방법에 대한 지식
KS3.9 정보 보안 요건을 조직 프로세스에 통합하는 방법에 대한 지식
KS3.10 기업 정보 보안 요건을 계약자 및 제3자 관리 프로세스에 통합하는 방법에 대한 지식
KS3.11 조직 정보 보안 측정 기준을 설계, 구현 및 보고하는 방법에 대한 지식
KS3.12 정보 보안 통제의 효과성 및 적응성을 테스트하는 방법에 대한 지식
영역 4—정보 보안 사고 관리(18%) —비즈니스에 최소한의 영향을 미칠 수 있도록 정보 보안 사고를 감지, 조사, 대응 및 복구하는 역량을 계획, 개발 및 관리합니다.
업무 내용
4.1 사고의 정확한 식별 및 대응을 위해 정보 보안 사고의 조직적 정의 및 심각도 계층 구조를 정립하고 관리합니다.
4.2 정보 보안 사고에 대한 효과적이고 시기 적절한 대응을 위해 사고 대응 계획을 정립하고 관리합니다.
4.3 정보 보안 사고의 시기 적절한 식별을 보장하는 프로세스를 개발하고 구현합니다.
4.4 법률, 규제 및 조직 요건을 준수하면서 적절하게 대응하고 그 원인을 파악할 수 있도록 정보 보안 사고를 조사하고 문서화하는 프로세스를 정립하고 관리합니다.
4.5 해당 이해관계자가 사고 대응 관리에 참여할 수 있도록 사고 대응 및 통지 프로세스를 정립하고 관리합니다.
4.6 정보 보안 사고에 시기 적절하게 효과적으로 대응할 수 있도록 팀을 구성 및 훈련하고 장비를 갖추습니다.
4.7 정보 보안 사고에 대한 효과적인 대응을 보장하고 대응 능력을 개선하기 위해 사고 대응 계획을 주기적으로 테스트 및 검토합니다.
4.8 내부 및 외부 기관의 의사소통을 관리하기 위한 의사소통 계획 및 프로세스를 확립 및 관리합니다.
4.9 정보 보안 사고의 근본적인 원인을 확인하고, 수정 조치를 개발하고, 위험도를 재평가하고, 대응 효과성을 평가하고, 적절한 조치를 취할 수 있도록 사후 검토를 실시합니다.
4.10 사고 대응 계획, 재해 복구 계획 및 비즈니스 연속성 계획 등의 사이에 통합성을 정립하고 관리합니다.

CISM® 시험 및 자격증에 대한 응시자 안내서

영역(부문)
전문지식 내용
KS4.1 사고 대응 계획의 구성요소에 대한 지식
KS4.2 사고 관리 개념 및 사례의 지식
KS4.3 비즈니스 연속성 계획(BCP) 및 재해 복구 계획(DRP)과 이것의 사고 대응 계획에 대한 관계의 지식
KS4.4 사고 분류 방법에 대한 지식
KS4.5 손해 억제 방법에 대한 지식
KS4.6 통보 및 단계적 확대 프로세스에 대한 지식
KS4.7 정보 보안 사고를 식별 및 관리하는 역할과 책임에 대한 지식
KS4.8 사고 대응 팀에게 적절하게 장비를 갖추기 위해 필요한 도구와 장비의 유형 및 출처에 대한 지식
KS4.9 증거의 수집, 보존 및 제시를 위한 포렌식(Forensic) 요건 및 능력(예: 허용성, 증거의 품질 및 완결성, 보관 절차)에 대한 지식
KS4.10 내부 및 외부 사고 보고 요건 및 절차에 대한 지식
KS4.11 원인을 식별하고 수정 조치를 결정하기 위한 사후사고 검토 업무 및 조사 방법에 대한 지식
KS4.12 정보 보안 사고로 인해 발생한 손해, 비용 및 기타 비즈니스 영향을 정량화하기 위한 기법에 대한 지식
KS4.13 정보 보안 이벤트를 감지, 기록 및 분석하는 기술 및 프로세스에 대한 지식
KS4.14 정보 보안 사고를 조사하기 위해 사용 가능한 내부 및 외부 자원에 대한 지식



2012 년 CISM 시험을 준비하십시오.

시험 준비 및 전문성 개발을 위한 2012년 CISM 학습 교재

CISM® (Certified Information Systems Auditor®) 수험생은 체계적인 학습 계획을 세우면 CISM® 시험을 성공적으로 준비할 수 있습니다. ISACA®는 개개인에게 효과적인 학습 계획을 개발하여, 다음과 같이 수험생에게 다양한 학습 도구와 복습할 수 있는 과정을 제공합니다.

학습 보조 문서

- 2012 CISM® 리뷰 매뉴얼
- 2012 CISM® 리뷰 문제, 정답 및 설명 매뉴얼
- 2012 CISM® 리뷰 문제, 정답 및 설명 매뉴얼 붙임
- CISM® Practice Question Database v12

www.isaca.org/cismbooks에서 주문하십시오.

복습 과정

- 챕터에서 지원하는 복습 과정을 찾거나

당신이 있는 지역에서 등록을 하려면 www.isaca.org/cismreview 를 방문하십시오.