

정보 시스템(IS) 감사 및 보증과 해당 업무 수행에 필요한 기술의 특수한 특성상 IS 감사 및 보증에는 특별히 적용되는 표준이 필요합니다. 감사 커뮤니티에 대해 ISACA®가 담당하는 전문적 역할 중 가장 중요한 것은 바로 IS 감사 및 보증 표준의 개발과 보급입니다.

IS 감사 및 보증 표준에는 IS 감사 및 보고와 다음 사항을 알리는 것에 대한 의무 사항이 정의되어 있습니다.

- ISACA의 직무윤리규정에 정의된 전문직 종사자 책임에 맞는 IS 감사인 및 보증 전문가의 최소 업무 능력
- 초보자의 작업에 대한 관리 및 다른 전문가의 예상
- Certified Information Systems Auditor® (CISA®) 소지자 지명 요건 CISA 보유자의 업무에 대해 조사하여 표준에 부합하지 않으면 ISACA 감독 위원회 또는 상응하는 ISACA 위원회에서 징계 조치를 취하게 됩니다.

IS 감사 및 보증 전문가는 해당될 경우 활동이 ISACA IS 감사 및 보증 표준 또는 다른 해당 전문 표준에 따라 수행되었다는 진술서를 업무에 포함시켜야 합니다.

IS 감사 및 보증 전문가의 ITAF™ 프레임워크는 복합적인 수준의 가이드입니다.

- **표준:** 3개 카테고리 분류:
  - 일반 표준(1000 시리즈)—IS 감사 및 보증 작업 수행을 권장하는 원칙입니다. 전체 과제 수행에 적용되고 IS 감사 및 보증 전문가의 윤리, 독립성, 객관성, 의무를 비롯한 지식, 역량, 기술 거래를 다룹니다. 표준 내용은(굵게 표시)는 의무 사항입니다.
  - 수행 표준(1200 시리즈)—기획, 감독, 범주 작업, 위험, 중요성, 자원 동원, 감독, 할당 관리, 감사 및 보증 증거, 전문적 판단 및 의무 행사 등 할당 행위를 다룹니다.
  - 보고 표준(1400 시리즈)—보고서 유형, 소통 방식, 소통된 정보를 다룹니다.
- **지침:** 표준을 지원하고, 역시 3개 카테고리 분류:
  - 일반 지침(2000 시리즈)
  - 수행 지침(2200 시리즈)
  - 보고 지침(2400 시리즈)
- **도구 및 기법:** IS 감사 및 보증 전문가를 위한 추가 가이드, 예: 백서, IS 감사/보증 프로그램, COBIT® 5 제품군

ITAF에서 사용되는 온라인 용어집은 [www.isaca.org/glossary](http://www.isaca.org/glossary)에 나와 있습니다.

**책임의 한계:** ISACA는 ISACA의 직무윤리규정에 정의된, 전문직 종사자로서의 책임에 맞는 IS 감사인의 최소 업무 능력에 대한 지침을 정의했습니다. ISACA의 내용이 항상 성공적인 결과를 가지고 오는 것은 아닙니다. 출판된 내용에는 적합한 절차와 테스트가 포함되어 있지 않으며 동일한 결과를 가져올 수 있는 다른 절차와 테스트가 존재한다는 사실을 고려해야 합니다. 어떤 절차나 테스트가 적합한지 판단하는 데 있어서, 통제 전문가는 자신의 전문적 판단을 특정 시스템이나 IS 환경에 있는 특수한 제어 환경에 적용해야 합니다.

ISACA 전문 표준 및 경력 관리 위원회(PSCMC)는 표준과 가이드 준비 시 포괄적인 컨설팅을 제공합니다. 문서를 발행하기 전에, 일반인의 의견을 듣기 위해 국제적 초안이 발행됩니다. 의견이 있으시면 전문 표준 개발 디렉터를 수신인으로 하여 이메일([standards@isaca.org](mailto:standards@isaca.org)), 팩스(+1.847. 253.1443) 또는 우편(ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA)으로 보내 주십시오.

#### ISACA 2012-2013 전문 표준 및 경력 관리 위원회

<b>Steven E. Sizemore, CISA, CIA, CGAP, Chairperson</b>	텍사스 보건 및 인적 서비스 위원회, 미국
<b>Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP</b>	HP 엔터프라이즈 보안 서비스, 영국
<b>Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA</b>	Myers and Stauffer LC, 미국
<b>Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP</b>	브리티시 아메리칸 토바코 IT 서비스, 말레이시아
<b>Alisdair McKenzie, CISA, CISSP, ITCP</b>	IS 보증 서비스, 뉴질랜드
<b>Katsumi Sakagawa, CISA, CRISC, PMP</b>	JIEC Co. Ltd., 일본
<b>Ian Sanderson, CISA, CRISC, FCA</b>	NATO, 벨기에
<b>Timothy Smith, CISA, CISSP, CPA</b>	LPL 파이낸셜, 미국
<b>Rodolfo Szuster, CISA, CA, CBA, CIA</b>	Tarshop S.A., 아르헨티나

## IS 감사 및 보증 표준 1401 보고

### 내용

- 1401.1** IS 감사 및 보증 전문가는 업무 완료 시 결과를 전달하기 위해 다음의 내용이 포함된 보고서를 제공해야 합니다.
- 기업의 설명, 의도된 사용자, 내용 및 배포상의 제한 사항
  - 범위, 업무 목표, 해당 기간, 성격, 시기, 수행된 업무의 범위
  - 결과물, 결론, 권고 사항
  - IS 감사 및 보증 전문가가 활동과 관련하여 갖고 있는 범위상의 자격 또는 제약
  - 감사 약정 또는 계약서의 조건에 따른 서명, 날짜, 배포
- 1401.2** IS 감사 및 보증 전문가는 감사보고서의 결과물이 충분하고 적합한 증거에 의해 뒷받침되도록 해야 합니다.
- 

### 주요 특성

- IS 감사 및 보증 전문가는 다음을 수행해야 합니다.
- 활동의 중요 분야, 발생한 문제와 해결책, 피감사자에 의한 표명이 상세히 기록된 관련 서면 기술서를 피감사자로부터 획득합니다.
  - 활동과 관련한 피감사자의 책임 인정을 명시할 수 있도록 피감사자 기술서에 피감사자의 서명과 날짜가 있도록 합니다.
  - 활동 수행 과정 중에 받은 모든 서면 또는 구두 기술서를 업무 문서로 작성하고 보관합니다. 증명 활동 시, 오해 가능성을 줄일 수 있도록 피감사자의 서면 기술서가 획득되어야 합니다.
  - 수행된 활동의 유형을 뒷받침할 수 있도록 다음과 같이 보고서의 형식과 내용을 맞춤화합니다.
    - 감사(직접 또는 입증)
    - 검토(직접 또는 입증)
    - 합의된 절차
  - 중요한 취약성과 이것이 활동 목표 달성에 미치는 영향을 보고서에서 설명합니다.
  - 마무리 및 발표 전에 보고서 초안 내용을 주제 분야의 관리진과 논의하고, 해당될 경우 최종 보고서에 결과물, 결론, 권고 사항에 대한 관리진의 응답을 포함시킵니다.
  - 통제 환경에서 중요한 결함과 중요한 취약성을 관리 책임자(해당될 경우 담당 기관)에게 전달하고, 이러한 내용이 전달되었음을 보고서에서 공개합니다.
  - 참조는 최종 보고서에서 별도로 보고합니다.
  - 중요한 정도는 아니나 사소하다고 볼 수 없는 내부 통제 결함을 피감사자 관리진에게 전달합니다. 이러한 경우, 관리 책임자 또는 담당 기관에게 해당 내부 통제 결함이 피감사자 관리진에게 전달되었음을 통보합니다.
  - 업무 수행 시 적용된 표준을 파악하고, 해당될 경우 이러한 표준의 비준수 사항을 전달합니다.
-

## IS 감사 및 보증 표준 1401 보고

용어

용어	정의
관련 정보	통제와 관련하여, 기초 통제 또는 통제 요소 운영에 관해 평가자에게 의미 있는 내용을 내포하는 정보. 통제의 운영이 가장 적합함을 직접 확정하는 정보. 통제 운영과 간접적으로 연관된 정보도 해당될 수 있지만, 직접 정보보다는 적절성이 낮음. COBIT 5 정보 품질 목표를 참조하십시오.
신뢰 가능한 정보	정확하고 확인 가능하며 객관적인 출처에서 발생한 정보. COBIT 5 정보 품질 목표를 참조하십시오.
충분한 정보	정보가 충분한 시기는 평가자가 합리적인 결론을 도출할 수 있을 정도로 충분한 내용이 수집되었을 때임. 그러나 정보가 충분하기 위해서는 먼저 적합해야 함. COBIT 5 정보 품질 목표를 참조하십시오.
적합한 정보	적절성(예: 의도된 목적과 부합하는가), 신뢰성(예: 정확하고 확인 가능하며 객관적인 출처에서 발생), 적시성(예: 적합한 일정 내에서 생성 및 사용됨)을 갖춘 정보. COBIT 5 정보 품질 목표를 참조하십시오.
적시적 정보	기업 입장에서 통제 결함의 중요성이 높아지기 전에 통제 결함을 예방 또는 적발하는 것이 가능하도록 일정 내에서 생성 및 사용되는 정보. COBIT 5 정보 품질 목표를 참조하십시오.

표준 및  
지침 연계

유형	제목
지침	2401 보고

적용일

이 ISACA 표준은 2013년 11월 1일부터 모든 감사 및 보증 활동에 대해 시행됩니다.