



IS 감사 및 보증 표준 1008 기준

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

IS 감사 및 보증 표준 1008 기준

내용

- 1008.1** IS 감사 및 보증 전문가는 주제 사안이 평가될 때 바탕으로 되는 객관적이고, 온전하며, 적절하고, 측정 가능하고, 이해 가능하며, 널리 인식되고, 권한이 있고, 보고서의 모든 독자 및 사용자가 이해할 수 있고 이들이 이용할 수 있는 기준을 선택해야 합니다.
- 1008.2** IS 감사 및 보증 전문가는 기준의 출처를 고려하고, 덜 알려진 기준을 수락하기 전에는 적합한 권한이 있는 기구에서 발행한 기준에 초점을 맞춰야 합니다.
-

주요 특성

IS 감사 및 보증 전문가는 다음을 수행해야 합니다.

- **기준 선택**을 신중하게 고려하고, 해당 선택을 정당화할 수 있어야 합니다.
- 전문가로서의 판단을 바탕으로, 기준 사용으로 독자나 사용자를 호도하지 않는 공정하고 객관적인 의견 또는 결론이 수립되도록 해야 합니다. 관리진이 전체 요건을 모두 충족하는 기준을 수립하지 않을 수도 있습니다.
- 업무 요건 파악 시 기준의 적합성 및 가용성을 고려해야 합니다.
- 기준이 쉽게 이용 가능하지 않거나, 불완전하거나, 해석이 필요한 경우, 보고서가 공정하고 객관적이며 이해 가능하고, 기준이 사용된 문맥이 보고서에 포함되도록 하는 데 필요한 설명과 기타 정보를 포함시켜야 합니다.

주제 사안 평가 기준의 적합성 및 적절성은 다음의 5 가지 적합성 기준에 대해 평가되어야 합니다.

- **객관성**—기준은 전문가의 결과 및 결론에 부정적인 영향을 줄 수 있고, 이에 따라 보고서 사용자를 호도할 수 있는 편협성으로부터 배제되어야 합니다.
- **완전성**—기준은 주제 사안에 관한 전문가의 결론에 영향을 줄 수 있는 모든 기준이 IS 감사 또는 보증 업무 수행 시 식별 및 사용될 수 있도록 충분히 완전해야 합니다.
- **적절성**—기준은 주제 사안에 적절해야 하고, IS 감사 또는 보증 활동의 목표를 충족시키는 결과 및 결론에 기여해야 합니다.
- **측정 가능성**—기준은 유사 상황에서 다른 전문가가 적용할 때 주제 사안의 일관적인 측정 및 일관적인 결론 수립을 허용해야 합니다.
- **이해 가능성**—기준은 분명하게 커뮤니케이션되어야 하고, 의도적인 사용자에게 적합한 해석의 대상이 되어서는 안 됩니다.

사용자가 보증 활동의 편향성과 결과 및 결론의 적절성을 이해할 수 있도록, 기준의 수락성은 전문가 보고서의 사용자에게 대한 기준의 가용성에 의해 영향을 받습니다. 출처에는 다음 특성이 포함될 수 있습니다.

- **인정**—대상자가 기준을 충분히 인정하여 기준 사용에 대한 문제가 제기되지 않도록 해야 합니다.
- **권위**—특정 분야 내의 권위적 성명을 반영하고 주제 사안에 적합한 기준을 추구해야 합니다. 예를 들어, 권위적 성명은 전문가 기구, 업계 그룹, 정부, 규제 기관으로부터 발생할 수 있습니다.
- **대중적 이용**—기준은 전문가 보고서의 사용자가 이용할 수 있어야 합니다. 예를 들면, ISACA, 국제 회계사 협회(IFAC), 기타 인정되는 정부 또는 전문가 기구 등 전문 회계 및 감사 기구가 수립한 표준이 해당됩니다.

주요 특성 계속

- **전체 사용자 이용성**—기준이 대중적으로 이용 가능하지 않은 경우, 기준은 전문가 보고서의 일부를 형성하는 표명을 통해 전체 사용자에게 커뮤니케이션되어야 합니다. 표명은 감사가 가능하도록 적합한 기준 요건이 만족되는 주제 사안에 관한 진술서로 구성됩니다.

적합성 및 이용성에 더하여, IS 보증 기준 선택 시 기준의 사용 및 가능한 대상층의 관점에서 출처도 고려되어야 합니다. 예를 들어, 정부 규제 사안의 경우 주제 사안에 적용되는 법률 및 규정으로부터 수립된 표명을 바탕으로 한 기준이 가장 적합한 선택입니다. 그렇지 않을 경우, 업계 또는 거래 협회 기준이 적합할 수 있습니다. 고려할 수 있는 가능한 기준 출처:

- **ISACA 수립기준**—이 기준은 대중적으로 이용 가능한 기준 및 표준으로서, IT 거버넌스, 통제, 보안, 보증 분야에서 인정 받는 국제 전문가에 의해 동료 검토, 철저한 가치평가실사 절차를 거쳤습니다.
- **다른전문가기구수립기준**—ISACA 표준 및 기준과 유사한 이 기준은 주제 사안과 적절하고 다양한 분야의 전문가에 의해 수립되며, 동료 검토, 철저한 가치평가실사 절차를 거칩니다.
- **법률 및 규정 수립 기준**—법률과 규정이 기준의 근거가 될 수 있으나, 적용 시에는 주의를 기울여야 합니다. 많은 경우, 표현 문구들이 복잡하고 구체적인 법적 의미를 내포하고 있습니다. 여러 경우에, 요건을 표명으로 재명시해야 할 수도 있습니다. 또한, 보통 법률에 관한 의견을 개진하는 것은 전문 법률 전문가로 제한되어 있습니다.
- **공정한 프로세스를 준수하지 않는 기업의 수립 기준**—여기에는 공정한 프로세스를 준수하지 않고 공개적 컨설팅 및 논쟁의 대상이 되지 않은 다른 기업에 의해 수립된 관련 기준이 포함됩니다.
- **IS 감사 또는 보증 활동을 위해 특별히 수립된 기준**—IS 감사 또는 보증 활동을 위해 특별히 수립된 기준이 적합할 수는 있으나, 이러한 기준이 적합성 기준, 특히 완전성, 측정 가능성, 객관성을 충족하도록 특별한 주의를 기울여야 합니다. IS 감사 또는 보증 활동을 위해 특별히 수립된 기준은 표명의 형태를 띠니다.

선택 기준은 신중하게 고려되어야 합니다. 지역 법률 및 규정을 준수하는 것은 중요하고 의무 사항으로 고려되어야 하나, 많은 IS 감사 및 보증 활동에 변경 관리, IT 일반 통제 및 액세스 통제 등 법률이나 규정에서 다루지 않은 분야가 포함되어 있습니다. 이에 더하여, 결제 카드 업계 등 일부 업계에서는 반드시 충족되어야 하는 의무 요건을 두고 있습니다. 법률 요건이 원칙 중심일 경우, 전문가는 선택된 기준이 업무 목표를 만족하도록 해야 합니다.

활동이 진행됨에 따라, 추가적인 정보로부터 목표 달성에 필요하지 않은 특정 기준이 발생할 수 있습니다. 이러한 경우, 기준과 관련된 추가 작업은 필요하지 않습니다.

IS 감사 및 보증 표준 1008 기준

용어

용어	정의
기준	<p>주제 사안을 측정하고 제시하는 데 사용되고 IS 감사자가 주제 사안을 평가할 때 바탕으로 하는 표준 및 잣대</p> <p>기준의 요건:</p> <ul style="list-style-type: none"> • 객관성—편향적이지 않음 • 완전성—결론 도달을 위한 모든 적절한 요소가 포함됨 • 적절성—주제 사안과 관련됨 • 측정 가능성—일관적인 측정이 가능함 <p>증명 업무 시, 주제 사안에 관한 관리진의 서면 표명이 바탕으로 한 잣대가 평가될 수 있습니다. 실무자는 적합한 기준을 지칭함으로써 주제 사안에 관한 결론을 형성합니다.</p>

지침 연계

유형	제목
지침	2008 기준

적용일

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