



IS 감사 및 보증 표준 1207 부정 및 불법 행위

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 카테고리로 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 카테고리로 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 1207 부정 및 불법 행위

내용

- 1207.1** IS 감사 및 보증 전문가는 업무 중에 부정 및 불법 행위를 고려해야 합니다.
- 1207.2** IS 감사 및 보증 전문가는 업무 중에 전문가로서의 비판적 태도를 유지해야 합니다.
- 1207.3** IS 감사 및 보증 전문가는 일체의 중요한 부정 또는 불법 행위를 문서화하고 해당 당사자에게 적시에 전달해야 합니다.
-

주요 특성

IS 감사 및 보증 전문가는 다음을 수행해야 합니다.

- 업무를 계획하고 수행하면서 다음을 통해 감사 위험을 허용 가능한 수준으로 낮추어야 합니다.
 - 부정 및 불법 행위의 위험을 평가해도 부정 및 불법 활동에 의한 중요한 오류, 통제 결함 또는 문서상의 오류가 존재할 수 있다는 점을 인식합니다.
 - 활동 주제 사안, 범위, 목표와 관련된 부정 및 불법 행위를 예방 또는 적발하기 위한 내부 통제 등 기업과 기업 환경에 대한 이해력을 갖습니다.
 - 경영진 혹은 기업 내 구성원들이 실제로 발생되었거나 의심이 가는 부정 및 불법 행위에 대해 알고 있는지를 판단하기 위해 충분하고 적절한 증거를 수집합니다.
- 감사 절차를 수행할 때, 부정 및 불법 행위로 인한 중요한 오류, 통제 결함, 문서상의 오류 위험을 나타낼 수 있는 이례적이거나 예상치 않은 연관관계를 고려합니다.
- 내부 통제의 적합성과 관리진이 부정 및 불법 행위 예방 또는 적발을 의도한 통제책을 기각할 위험성을 테스트하기 위한 절차를 설계 및 수행합니다.
- 식별된 오류, 통제 결함 또는 문서상의 오류가 부정 또는 불법 행위를 나타낼 수 있는지 여부를 평가합니다. 만약 그런 암시가 있을 경우, 관련된 업무의 다른 부분, 특히 경영진의 진술과 관련해 어떤 의미가 내포되어 있는지 고려해야 합니다.
- 업무에 따라 관리진에게서 연간 최소 1 회 또는 그 이상 서면 기술서를 획득해서 다음을 수행합니다.
 - 부정 및 불법 행위를 예방하고 발견하기 위한 내부적 통제의 계획과 수행에 대한 관리진의 책임 인식
 - 부정 또는 불법 행위의 결과로 인해 오류, 통제 결함 또는 문서상의 오류가 존재할 수 있음이 내포된 위험 평가의 관련 결과를 공개
 - 내부 통제에 중요한 역할을 맡고 있는 관리진 및 직원과 관련하여 기업에 영향을 주는 부정 및 불법 행위에 대한 관리진의 지식 공개
 - 직원, 전 직원, 규제자, 그 밖의 관련자에 의해 전달된 대로 기업에 영향을 주는 제기 또는 의심된 부정 및 불법 행위에 대한 관리진의 지식 공개
- 적시에 다음 내용을 수행합니다.
 - 중요한 부정 또는 불법 행위가 존재할 수 있다고 파악하거나 입수한 정보를 적합한 관리진 직위에 전달합니다.

IS 감사 및 보증 표준 1207 부정 및 불법 행위

- 주요 특성
계속
- 내부 통제에 중요한 역할을 맡고 있는 관리진 또는 직원과 관련된 일체의 중요한 부정 및 불법 행위를 관리 책임자에게 전달합니다.
 - 범위에 속하지 않더라도, 업무 중에 파악된 부정 및 불법 행위 예방 및 방지를 위한 내부 통제를 설계하고 구현할 때, 중요한 취약성을 관리 책임자에게 보고합니다.
 - 상황에 적절한 합법적이며 전문적인 보고 요건을 고려합니다.
 - 중요한 오류, 통제 결함, 문서상의 오류, 또는 불법 행위가 업무의 지속적 수행에 영향을 미칠 경우, 업무에서 제외할 것을 고려합니다.
 - 관리진, 관리 책임자, 규제자, 그 밖의 관련자에게 보고된 중요한 부정 및 불법 행위에 대한 모든 전달 사항, 계획, 결과, 평가 및 결론 문서화합니다.

용어

용어	정의
부정	수립된 관리진 정책 또는 규제 요건을 위반하는 행위. 부정은 중과실 또는 비의도적인 불법 행위로서 감사 중인 분야 또는 기업에 관한 정보의 고의적인 문서상의 오류나 누락으로 구성될 수 있습니다.
중요한 문서상의 오류	감사의 결과에 측정 가능한 범위까지 영향을 주는 우발적 또는 의도적인 허위 진술
전문적 비판성	문제를 제기하는 태도, 감사 증거의 중대한 평가 등에 해당되는 태도. 출처 American Institute of Certified Public Accountants (AICPA) AU 230.07

표준 및 지침 연계

유형	제목
표준	1008 기준
표준	1202 계획 시 위험 평가
표준	1205 증거
지침	2206 다른 전문가의 작업 사용
지침	2207 부정 및 불법 행위

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