IS 감사 및 보증 표준
1202 계획 시 위험 평가

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.

- ISACA 의 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**: 3 개 카테고리로 분류:
  - 일반 표준(1000 시리즈)—IS 감사 및 보증 작업 수행을 관장하는 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 3 개 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

ITAF 에서 사용되는 온라인 용어집은 *www.isaca.org/glossary* 에 나와 있습니다.

책임의 한계: ISACA 는 ISACA 의 직무윤리규정에 정의된, 전문직 종사자로서의 책임에 맞는 IS 감사인의 최소 업무 능력에 대한 지침을 정의했습니다. ISACA 의 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 어메리칸 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 1202 계획 시 위험 평가

내용

1202.1 IS 감사 및 보증 담당자는 적절한 위험 평가 접근 방식과 제반 방법을 사용하여 전반적인 IS 감사 계획서를 수립하고 IS 감사 자원의 효과적 할당을 위한 우선순위를 결정해야 합니다.

1202.2 IS 감사 및 보증 전문가는 개별 업무를 계획할 때, 검토 중인 분야와 관련된 위험을 파악하고 평가해야 합니다.

1202.3 IS 감사 및 보증 전문가는 주제 사안 위험, 감사 위험, 기업으로의 관련 노출을 고려해야 합니다.

주요 특성

지속적인 활동을 계획할 때, IS 감사 및 보장 담당자는 다음을 수행해야 합니다.

- 원활한 IS 감사 계획서 수립을 위해 1년에 1회 이상 위험 평가를 수행하고 문서화해야 합니다.
- 위험 평가의 일환으로 조직상의 전략 계획과 목표, 기업 위험 관리 프레임워크 및 계획을 포함해야 합니다.
- 각각의 IS 감사 및 보증 업무에 대해, 업무 요건 충족에 필요한 IS 감사 자원의 양을 측정하고 판단해야 합니다.
- 감사 이해가 있는 분야 및 항목 선택과 특정한 IS 감사 및 보증 업무를 설계하고 수행하기 위한 결정에 있어 위험 평가를 사용해야 합니다.
- 감사 이해관계자 및 기타 적절한 대상으로부터 위험 평가의 승인을 구해야 합니다.
- 위험 평가를 바탕으로 IS 감사 및 보증 업무의 우선 순위를정하고 일정을 수립해야 합니다.
- 위험 평가를 바탕으로 다음과 같은 계획서를 수립해야 합니다.
  - IS 감사 및 보증 활동을 위한 프레임워크의 역할을 할 수 있는 계획서
  - 비 IS 감사 및 보증 요건과 활동이 고려된 계획서
  - 지배구조 책임자에 의해 1 년에 1 회 이상 수정 및 승인되는 계획서
  - 다음에 설정된 책임을 명시한 계획서: 감사 약정

개별 업무 계획 시, IS 감사 및 보증 전문가는 다음을 수행해야 합니다.

- 검토 중인 분야와 관련된 위험을 파악하고 평가해야 합니다.
- 각 업무에 대해 검토 중인 분야와 관련 있는 위험의 예비 평가를 수행해야 합니다. 각각의 구체적인 업무의 목표에는 예비 위험 평가의 결과가 반영되어야 합니다.
- 위험 분야를 고려하고 구체적인 업무를 계획할 때, 수정 조치 등 이전의 감사, 검토, 결과를 고려해야 합니다. 위원회의 전체적인 위험 평가 프로세스도 고려해야 합니다.
- IS 감사 계획 및 수행 중에 감사 위험을 적정 수준으로 감소하도록 시도하고, IS 주제 사안 및 관련 통제책을 적절하게 평가함으로써 감사 목표를 만족해야 합니다.
- 구체적인 IS 감사 절차를 계획할 때, 중요성 임계치가 낮을수록 감사 기대가 정밀해지고 감사 위험이 커진다는 점을 인식해야 합니다.
- 높은 중요성에 대한 위험을 감소시키기 위해, 통제 테스트를 확대하고(통제 위험 감소) 그리고/또는 실증 테스팅 절차를 확대하여(적발 위험 감소) 보상함으로써 추가 보증을 확보해야 합니다.

©2013 ISACA 전권 보유.

IS 감사 및 보증 표준 1202 계획 시 위험 평가

용어

용어	정의
감사 약정	내부 감사 활동의 목적, 권한, 책임이 정의되어 있고 지배구조 책임자가 승인한 문서 약정의 역할: • 내부 감사 담당자의 기업 내 직책 수립 • IS 감사 및 보증 업무 수행과 관련하여 기록, 직원, 물리적 특성으로의 액세스 승인 • 감사 담당자의 활동 범위 정의
감사 위험	감사 결과를 바탕으로 부정확한 결론에 도달할 수 있는 위험. 감사 위험의 3 가지 요소: • 통제 위험 • 적발 위험 • 고유 위험
감사 주제 관련 위험	검토 중인 분야에 관련된 위험: • 사업 위험(고객의 지급 능력, 신용 가치, 시장 요인 등) • 계약 위험(책임, 가격, 유형, 처벌 등) • 국가 위험(정치, 환경, 보안 등) • 프로젝트 위험(자원, 기술 세트, 방법, 제품 안정성 등) • 기술 위험(솔루션, 아키텍처, 하드웨어 및 소프트웨어 인프라 네트워크, 제공 채널 등) 고유 위험을 참조하십시오.
통제 위험	내부 통제 시스템에 의해 적기에 예방 또는 적발할 수 없는 중요한 오류가 존재하는 위험 (고유 위험 참조)
적발 위험	IS 감사 또는 보증 전문가의 실증 절차상 중요할 수 있는 오류가 개별적 또는 다른 오류와 결합되어 적발되지 않는 위험 감사 위험을 참조하십시오.
고유 위험	관리진이 취했거나 취할 수 있는 조치를 감안하지 않은 위험 수준 또는 노출(예: 통제책 이행). 통제 위험을 참조하십시오.
중요성	감사 대상의 기능에 대해 미치는 영향과 관련한 정보 항목의 중요성에 관한 감사 개념. 기업 전체의 문맥에서 상대적 중요성 또는 특정 사안의 중요도를 지칭한 표현.
위험 평가	위험과 위험의 가능한 영향을 식별하고 평가하는 데 사용되는 절차. 위험 평가는 IS 연간 감사 계획서에 포함하기 위해 최고의 위험, 취약성, 기업으로의 노출을 나타내는 항목이나 분야를 파악하는 데 사용됨. 프로젝트 이행 및 프로젝트 수익 위험을 관리할 때도 사용됨.
실증 테스팅	감사 기간 중에 활동이나 거래의 완전성, 정확성 또는 존재 여부에 대한 감사 증거를 확보하는 행위

IS 감사 및 보증 표준 1202 계획 시 위험 평가

지침 연계

유형	제목
지침	2202 계획 시 위험 평가

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