

정보 시스템(IS) 감사를 수행하는 데 필요한 특수한 특성 및 기술에는 특별히 적용할 표준이 필요합니다. ISACA®(Information Systems Audit and Control Association®)의 목표 중 하나는 이 같은 국제적 표준을 만드는 것입니다. 감사 커뮤니티에 대해 ISACA 이 담당하는 전문적 역할 중 가장 중요한 것은 바로 IS 감사 표준의 개발과 보급입니다. IS 감사 표준의 프레임워크는 다음과 같이 여러 단계의 지침을 제공하고 있습니다.

- **표준(Standards)**은 IS 감사 및 보고에 있어 다음과 같은 필수 요구사항을 정의합니다.
 - ISACA의 직무윤리규정에 정의된 전문적 종사자 책임에 맞는 IS 감사인으로서의 최소 업무 능력
 - 초보자의 작업에 대한 관리 및 다른 전문가의 예상
 - CISA®(Certified Information Systems Auditor®) 지명권자의 요구사항으로서, CISA 보유자의 업무에 대해 조사하여 표준에 부합하지 않으면 ISACA 감독 위원회 또는 상응하는 ISACA 위원회에서 징계하게 됩니다.
- **지침(Guidelines)**은 IS 감사 표준을 적용하는 지침을 정의합니다. IS 감사인은 표준 구현 방법을 결정하는 데 있어 지침을 고려해야 하고, 업무에 있어 전문가로서 판단해야 하며, 어떠한 상황에서도 대처할 수 있도록 준비가 되어 있어야 합니다. IS 감사 지침의 목적은 IS 감사 표준을 준수하는 방법에 대해 더 많은 정보를 제공하는 것입니다.
- **절차(Procedures)**에는 IS 감사인이 감사 업무에서 수행하게 될 절차의 예제가 나와 있습니다. 절차에서는 IS 감사 작업 수행 시에 표준을 준수하는 방법에 대한 정보가 나와 있지만, 요구사항은 정의되어 있지 않습니다. IS 감사 절차의 목적은 IS 감사 표준을 준수하는 방법에 대해 더 많은 정보를 제공하는 것입니다.

CobiT® 리소스는 우수 사례 지침의 자료로서 사용됩니다. CobiT *프레임워크(Framework)*는 "기업의 모든 자산을 보호하는 것은 관리자의 책임이다. 이러한 책임을 완수함과 함께 목표를 달성하기 위해, 관리자는 적절한 내부 통제 시스템을 구축해야만 한다"라고 명시하고 있습니다." CobiT는 정보 시스템 관리 환경에 대해 상세한 통제 항목과 통제 기술을 제공합니다. CobiT에서 특정 감사에 적용할 가장 적절한 자료를 선택할 때는 적합한 CobiT IT 프로세스를 선정하고 CobiT 정보 기준을 고려해야 합니다.

CobiT *프레임워크*에 정의된 것과 같이, 다음 항목은 IT 관리 프로세스에 의해 구성됩니다. CobiT은 비즈니스와 IT 관리자 및 IS 감사인이 사용하도록 개발된 것으로, 비즈니스 목적을 이해하고 우수 사례를 교환하며 국제적으로 이해 및 인정되는 표준 참조가 추천되어 있습니다. CobiT는 다음을 포함하고 있습니다.

- 통제 목적—최소한의 성공적 통제에 대한 높은 수준의 상세하고 포괄적인 설명
- 통제 사례—통제 목적에 대한 실제적 근거 및 "구현 방법" 지침
- 감사 지침—각 통제분야에 대해 이해하고, 통제를 평가하며, 준거성을 판단하고 통제되지 않은 위험을 구체화 하는 방법에 대한 지침.
- 관리 지침—성숙도 모델, 매트릭스 및 필수 성공 요소를 사용한 IT 프로세스 성능 평가 및 개선 방법에 대한 지침. 이들은 다음 사항에 중점을 둔, 지속적이고 예측적인 통제 자가 평가(control self-assessment)를 위한 관리기반구조를 제공합니다.
 - 성과 관리—사업 요구사항을 지원하는 IT 기능이 어느 정도 양호한지 살펴봅니다. 관리 지침은 자가 평가 워크샵을 지원하고 IT 통제관리계획의 일부분인 지속적인 모니터링 관리와 개선 절차를 구현하는 데에도 사용할 수 있습니다.
 - IT 통제 프로파일—어느 IT 프로세스가 중요한가? 통제에 있어 필수 성공 요소는 무엇인가?
 - 인식—목적을 달성하지 못한 경우에는 어떤 위험이 있는가?
 - 벤치마킹—다른 기업은 무엇을 하는가? 결과의 측정 및 비교 방법을 알아봅니다. 관리 지침은 사업 분야에서 IT 성능을 평가할 수 있는 예제 매트릭스를 제공합니다. 핵심목표지표는 IT 프로세스의 성과를 식별 및 측정하며, 핵심성과지표는 프로세스의 책임자를 평가함으로써 프로세스가 얼마나 제대로 수행되고 있는지를 평가합니다. 성숙도 모델과 성숙도 속성은 성능 평가 및 벤치마킹에 제공되어, 관리자가 통제 능력을 측정하고 통제 오차와 전략을 확인하여 개선할 수 있도록 지원합니다.

용어는 ISACA 웹사이트 www.isaca.org/glossary에서 찾아 볼 수 있습니다.

거부권: ISACA는 ISACA의 직무윤리규정에 정의된, 전문적 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 정보 기술 환경에 있는 특수한 제어 환경에 적용해야 합니다.

ISACA 표준 위원회는 IS 감사 표준, 지침 및 절차를 준비하는 데 있어 다양한 자문을 수용합니다. 문서를 발행하기 전에 표준 위원회는 일반인의 의견을 듣기 위해 국제적 초안을 발행합니다. 또한, 표준 위원회는 자문내용과 관련된 항목에서 전문적 지식이나 의견을 가지고 있는 사람들의 견해를 듣고 있습니다. 표준 위원회는 개발 프로그램을 진행하고 있으며, 새로운 표준이 필요한 문제를 가지고 있는 ISACA 구성원 및 관심 있는 단체의 참여를 환영합니다. 모든 제안 내용은 전자우편(standards@isaca.org), 팩스(+1.847. 253.1443) 또는 우편(문서 마지막에 나와 있는 주소)을 통해 ISACA 국제 본사의 리서치 표준 및 연구 관련 담당자에게 보내시면 됩니다. 본 문서는 2005년 7월 1일에 발행되었습니다.

부정 및 불법 행위 S9

개요

- 01 ISACA 표준은 의무 사항인 기본 원칙과 필수 절차를 굵은 글씨로 기술하고 있으며 관련 지침이 함께 제공됩니다.
- 02 본 ISACA 표준은 감사 프로세스가 진행되는 동안 IS 감사인이 고려해야 하는 부정 및 불법 행위에 대한 지침을 수립, 제공하는 것을 목적으로 합니다.

표준

- 03 감사를 계획하고 수행함에 있어 감사 위험을 최소화하기 위해 IS 감사인은 부정 및 불법 행위의 위험성을 고려해야 합니다.
- 04 IS 감사인은 감사가 진행되는 동안 전문가로서의 비판적 태도를 유지해야 하며 감사인의 판단에 상관없이 부정 및 불법 행위로 인한 문서상의 오류가 항상 존재할 수 있음을 인지해야 합니다.
- 05 IS 감사인은 내부적 통제를 포함한 조직과 조직 환경에 대해 이해해야 합니다.
- 06 IS 감사인은 경영진 혹은 조직 내 구성원들이 실제로 발생되었거나 의심이 가는 부정 및 불법 행위에 대해 알고 있는지를 판단하기 위해 충분하고 적절한 감사 증거를 수집해야 합니다.
- 07 감사 절차를 수행할 경우 조직과 환경에 대해 이해하기 위해, IS 감사인은 부정 및 불법 행위로 인한 문서상 오류의 위험을 보여줄 수 있는 특이하거나 예외적인 관계를 고려해야 합니다.
- 08 IS 감사인은 내부적 통제의 적합성과 경영진의 과도한 통제에 따른 위험성을 테스트하는 절차를 계획하고 수행해야 합니다.
- 09 IS 감사인은 오류를 발견했을 때 그러한 오류가 부정 및 불법 행위를 암시하고 있는지 판단해야 합니다. 만약 그러한 암시가 있을 경우 IS 감사인은 관련된 감사의 다른 부분, 특히 경영진의 진술과 관련해 어떤 의미가 내포되어 있는지 고려해야 합니다.
- 010 IS 감사인은 감사 계약에 따라 최소한 일년에 한 번 혹은 그 이상 경영진으로부터 문서로 된 진술을 수집해야 합니다. 진술서는 다음을 포함해야 합니다.
 - 부정 및 불법 행위를 예방하고 발견하기 위한 내부적 통제의 계획과 수행에 대한 책임 인식
 - IS 감사인에게 부정 및 불법 행위로 인한 문서상의 오류가 존재할 수 있다는 위험 평가의 결과 발표
 - IS 감사인에게 다음과 관련해 조직에 영향을 끼치는 부정 및 불법 행위에 대한 정보 발표
 - 경영진
 - 내부적 통제에 있어 중요한 역할을 수행하는 직원
 - 직원, 전(前) 직원, 관리자 혹은 기타 관련자간의 의사소통 과정에서 조직에 영향을 끼치는 부정 및 불법 행위가 있었다고 알려졌거나 의심이 되는 정보를 IS 감사인에게 제공
- 11 만약 IS 감사인이 문서상의 부정 및 불법 행위를 발견했거나 문서상의 부정 및 불법 행위가 존재할 수 있다는 정보를 수집하면 IS 감사인은 조속한 시일 내에 해당 경영진과 이 문제에 관해 논의해야 합니다.
- 12 만약 IS 감사인이 문서상의 부정 및 불법 행위에 경영진 혹은 내부적 통제에 있어서 중요한 역할을 수행하는 직원이 개입되어 있다는 점을 발견했다면 IS 감사인은 조직구조 책임자와 이러한 문제에 대해 조속한 시일 내에 논의해야 합니다.
- 13 감사 기간 동안 IS 감사인의 주의를 끈 부정 및 불법 행위를 예방하고 발견하기 위한 내부적 통제를 계획하고 수행하는 데 있어서 IS 감사인은 적합한 경영진과 문서상의 취약점을 책임지고 있는 책임자에게 조언을 해야 합니다.
- 14 만약 IS 감사인이 문서상의 오류나 불법 행위로 인해 감사 수행 능력에 차질이 생기는 예외적 상황에 처하게 된다면, 해당 상황에 적용해야 할 법적, 전문가적 책임이 있는지, IS 감사인이 계약 당사자 혹은 관리 책임자나 규제 당국에 보고할 의무가 있는지 혹은 계약을 철회해야 하는지를 고려해야 합니다.
- 15 IS 감사인은 경영진, 지배구조 책임자, 단속자 및 기타 관련자들에게 보고된 바 있는 문서상의 부정 및 불법 행위와 관련된 모든 대화내용, 계획, 결과, 평가, 결론을 문서화 하여 제출해야 합니다.

주석

- 16 IS 감사인은 부정 및 불법 행위의 정의에 대해 IS 감사 지침 G19, 부정 및 불법 행위를 참조해야 합니다.
- 17 IS 감사인은 부정 및 불법 행위로 인한 문서상의 오류가 없음을 논리적으로 입증해야 합니다. IS 감사인의 개인적 판단, 제한된 테스트의 범위, 제한된 내부적 통제로 인해 감사 결과를 절대적으로 보장할 수는 없습니다. 감사 기간 동안 IS 감사인이 사용할 수 있는 감사 증거는 본질적으로 최종적이기 보다는 설득적이어야 합니다.
- 18 불법 행위로 인한 문서상의 오류를 발견하지 못할 위험은 부정 및 실수로 인한 문서상의 오류를 발견하지 못할 위험보다 큼니다. 이는 불법 행위는 IS 감사인이 의도적인 오류 및 사건을 발견하지 못하도록 치밀한 계획하에 이루어지기 때문입니다.
- 19 IS 감사인의 감사를 진행하는 동안 자신의 조직에 대한 이전 경험과 지식을 이용하여야 합니다. 조사에 착수하고 감사 절차를 수행함에 있어 IS 감사인은 이전 경험을 소홀히 해서는 안되며 전문가로서의 비판적 태도를 유지해야 합니다. IS 감사인은 경영진과 지배구조 책임자들이 정직하고 결백하다고 믿음으로써 설득력 없는 감사 증거에 만족하여서는 안됩니다. IS 감사인과 계약팀(engagement team)은 감사 프로세스의 계획의 일부로서 감사가 진행되는 전 기간에 걸쳐 부정 및 불법 행위에 대한 조직의 민감성(susceptibility)에 대해 논의해야 합니다.
- 20 문서의 부정 및 불법 행위 존재의 위험성을 평가하기 위해 IS 감사인은 다음 사항을 이용하는 것을 고려해야 합니다.
 - 조직에 관한 이전 경험과 지식(경영진과 지배구조 책임자의 정직성과 결백에 관한 경험 포함)
 - 경영진 조사 과정에서 수집한 정보
 - 경영진 진술과 내부적 통제의 표시(sign-off)
 - 감사 과정에서 수집된 기타 신뢰성 있는 정보
 - 부정 및 불법 행위의 위험성에 관한 경영진의 평가와 위험을 파악하고 대처하는 프로세스
- 21 부정 및 불법 행위에 대한 자세한 정보는 다음 지침을 참조하십시오.
 - IS 감사 지침 G5, 감사 약정
 - CobiT 프레임워크, 통제 목적 DS3, DS5, DS9, DS11 과 PO6
 - 2002년 제정된 사베인 옥슬리 법안(Sarbanes-Oxley Act)
 - 1977년 제정된 해외부패방지법(Foreign Corrupt Practices Act)

적용일

22 본 ISACA 표준은 2005년 9월 1일 이후 모든 정보 시스템 감사에 적용됩니다.

Information Systems Audit and Control Association 2004-2005 표준 위원회

Chair, Sergio Fleginsky, CISA ICI Paints, 우루과이
Svein Aldal Aldal Consulting, 노르웨이
John Beveridge, CISA, CISM, CFE, CGFM, CQA Office of the Massachusetts State Auditor, 미국
Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP Tangerine Consulting, 이탈리아
Christina Ledesma, CISA, CISM Citibank NA Sucursal, 우루과이
Andrew MacLeod, CISA, CIA, FCPA, PCP Brisbane City Council, 호주
V. Meera, CISA, CISM, ACS, CWA Microsoft Corporation, 미국
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA Ikanos Communications., 인도
Peter Niblett, CISA, CISM, CA, CIA, FCPA WHK Day Neilson, 호주
John G. Ott, CISA, CPA AmerisourceBergen, 미국
Thomas Thompson, CISA Ernst & Young, 아랍에미리트 연합

©Copyright 2005

Information Systems Audit and Control Association

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

전화: +1.847.253.1545

팩스: +1.847.253.1443

전자우편: standards@isaca.org

웹사이트: www.isaca.org