

S16 전자 상거래(E-COMMERCE)

정보 시스템(IS) 감사를 수행하는 데 필요한 특수한 특성 및 기술에는 특별히 적용할 표준이 필요합니다. ISACA[®]의 목적 중 하나는 세계적으로 적용되는 표준을 비전에 부합하도록 발전시키는 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 필수 요구사항을 정의합니다. 다음과 같은 내용이 있습니다.
 - ISACA의 직무윤리규정에 정의된 전문직 종사자 책임에 맞는 IS 감사인으로서의 최소 업무 능력
 - 초보자의 작업에 대한 관리 및 다른 전문가의 예상
 - CISA[®](Certified Information Systems Auditor[™]) 지명권자의 요구 사항으로서, 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.

정보 및 관련 기술에 대한 통제 목적(CoBIT[®])은 관리자가 통제 요건, 기술 문제 및 사업 위험 간의 격차를 해소시킬 수 있도록 하는 정보 기술(IT) 거버넌스 프레임워크 및 지원 도구입니다. CoBIT는 조직 전반의 IT 통제를 위한 확실한 정책 개발 및 우수 사례를 가능하게 합니다. 이것은 규정 준수를 강조하고, 조직이 IT로부터 얻는 가치를 증대시킬 수 있도록 하고, CoBIT 프레임워크의 개념을 준수하고 구현을 간단하게 만듭니다.

CoBIT는 비즈니스와 IT 관리자 및 IS 감사인이 사용하도록 개발된 것으로, 비즈니스 목적을 이해하고 우수 사례를 교환하며 국제적으로 이해 및 인정되는 프레임워크가 추천되어 있습니다. CoBIT는 ISACA 웹 사이트 www.isaca.org/cobit에서 다운로드 가능합니다. CoBIT 프레임워크에 정의된 것과 같이, 다음 관련 제품 및/또는 구성 요소는 IT 관리 프로세스에 의해 구성됩니다.

- 통제 목적—IT 프로세스와 관련하여 최소한의 좋은 통제에 대한 일반적인 설명.
- 관리 지침—성숙도 모델, RACI (Responsible, Accountable, Consulted and/or Informed) 차트 사용, 목표, 그리고 측정 기준 등을 사용하여 IT 프로세스 성능을 평가하고 개선하는 방법에 대한 지침. 이들은 다음 사항에 중점을 둔, 지속적이고 예측적인 통제 자가 평가(control self-assessment)를 위한 관리기반구조를 제공합니다.
 - 성과 측정
 - IT 통제 프로파일
 - 인식
 - 벤치마킹
- *CoBIT 통제 사례*—통제 목적을 위한 '구현 방법' 지침과 위험 및 가치 설명서.
- *IT 보증 가이드*—각 통제분야에 대해 이해하고, 통제를 평가하며, 준거성을 판단하고 통제되지 않은 위험을 구체화 하는 방법에 대한 지침.

용어는 ISACA 웹사이트 www.isaca.org/glossary에서 찾아 볼 수 있습니다. IS 감사 표준, 지침 및 절차에서는 감사와 검토라는 단어가 교대로 사용됩니다.

거부권: 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 전문가가 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 자료는 2007년 12월 1일에 발행되었습니다.

S16 E-commerce

개요

- 01 ISACA 표준은 의무 사항인 기본 원칙과 필수 절차를 굵은 글씨(검정색)로 기술하고 있으며 관련 지침이 함께 제공됩니다.
- 02 ISACA 표준의 목적은 전자 상거래 환경의 검토와 관련된 표준을 구축하고 지침을 제공하기 위한 것입니다.

표준

- 03 IS 감사인은 전자 상거래 트랜잭션이 적절하게 통제되도록 전자 상거래 환경을 검토할 때 해당 통제와 위험을 평가해야 합니다.

주석

- 04 전자 상거래(E-commerce)란 조직이 인터넷을 기본 기술로 사용하여 그 고객, 공급업체 및 기타 외부 사업 파트너와 사업을 온라인으로 처리하는 프로세스로 정의됩니다. 따라서, 이것은 B2B(Business-to-Business) 및 B2C (Business-to-Consumer) 전자 상거래 모델을 포함합니다.
- 05 IS 감사인은 전반적인 IT 감사 계획을 개발함에 있어서 적절한 위험 평가 기술 또는 방법을 사용해야 하며, 전자 상거래 환경을 고려해야 합니다.
- 06 IS 감사인은 지속적 보증의 사용을 포함하는 데이터 분석 기술의 사용을 고려해야 하는데, 이것은 IS 감사인이 시스템의 신뢰성을 지속적으로 모니터링하고 전자 상거래 활동 검토시 컴퓨터를 통해 선택적 감사 증거를 수집할 수 있도록 합니다.
- 07 전자 상거래에 있어서 통제 및 위험 관리의 의미를 이해하기 위해 필요한 기술 및 지식의 수준은 조직의 전자 상거래 활동의 복잡도에 따라 달라집니다.
- 08 IS 감사인은 적절한 상황을 고려하여 결과를 평가할 수 있도록 감사를 실시하기 전에 전자 상거래 어플리케이션에 의해 지원되는 사업 프로세스의 성격과 중요도를 이해해야 합니다.
- 09 전자 상거래에 관한 자세한 내용은 다음 지침을 참조해야 합니다.
 - 지침 G21 전사적 자원 관리(ERP) 시스템 검토
 - 지침 G22 B2C(Business-to-Consumer) 전자 상거래 검토
 - 지침 G24 인터넷 बैं킹
 - 지침 G25 가상 사설 네트워크(VPN)의 검토
 - 지침 G33 인터넷 사용에 대한 일반적인 고찰
 - 절차 P6 방화벽
 - CoBIT 프레임워크 및 통제 목적

적용일

- 10 본 ISACA 표준은 2008년 2월 1일부터 시작되는 IS 감사에 적용됩니다.

2007-2008 ISACA 표준 위원회

회장, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA Capco IT Services India Private Limited, 인도
Brad David Chin, CISA, CPA Google Inc., 미국
Sergio Fleginsky, CISA ICI Paints, 우루과이
Maria Gonzalez, CISA HomeLand Office, 스페인
John Ho Chi, CISA, CISM, CBCP, CFE Ernst & Young, 싱가포르
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, 호주
John G. Ott, CISA, CPA AmerisourceBergen, 미국
Jason Thompson, CISA, CIA KPMG LLP, 미국
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA Microsoft Corp., 미국

© 2007 ISACA. 판권 본사 소유.

ISACA
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