Samil PwC Governance Center KSOX series

내부회계관리제도, IT시스템 통제는 왜 필요한가?

삼일회계법인 내부회계자문센터

pwc 삼일회계법인

내부회계관리제도, IT시스템 통제는 왜 필요한가?

정보기술이 고도화됨에 따라 기업의 재무정보는 기존 수작업 기반에서 IT시스템에 의존하는 형태로 진보했습니다. 정보기술일반통제(IT General Controls, ITGCs)는 IT인프라, 보안관리, 정보기술의 취득, 개발 및 유지보수에 대한 통제활동으로, 구체적으로 ▲프로그램 개발(시스템 도입, 테스트, 데이터 이관), ▲프로그램 변경(설정 및 이관권한 관리), ▲프로그램&데이터 접근 보안(DB접근관리, 사용자 권한관리, 보안), ▲운영(백업관리, 장애관리)에 대한 통제를 의미합니다.

본고에서는 IT시스템 통제의 이유와 IT시스템 통제 평가 시 고려할 사항에 대해 살펴보고자 합니다.

1. 정보기술일반통제(ITGCs) 평가 의의

재무정보의 기반이 되는 여러 업무 과정에서 ERP 등 IT시스템을 활용하는 정보시스템 환경에서는 정보가 생성, 저장, 처리되는 과정에 IT시스템에 대한 의존이 필연적입니다. 따라서, IT시스템에 기반한 정보처리의 정확성 등을 담보하기 위해서는 IT시스템의 신뢰성과 안정성이 전제되어야 합니다. 정보기술일반통제(이하 'ITGCs')는 IT시스템의 신뢰성과 안정성을 담보하기 위한 IT시스템에 대한 통제로 IT인프라, 보안관리, 정보기술의 취득, 개발 및 유지보수에 대한 통제활동을 의미합니다.

프로그램 자동설정, 프로그램 자동계산, 프로그램 데이터 보관, 프로그램 권한 제어 등 IT시스템에 의존하는 내부회계관리제도가 유효하기 위해서는 ITGCs에 대한 고려는 선결 사항입니다. ITGCs는 정보시스템에 의존하는 비즈니스 프로세스 상 통제활동의 신뢰성 관련 기반을 제공하며, 이는 관련 통제활동의 적정성을 담보하기 위한 기반일 뿐만 아니라 일부 ITGCs(예, 데이터 직접 변경 통제)의 경우 ITGCs 자체가 재무정보에 직접적인 영향을 미치는 통제활동이기도 합니다.

ITGCs에 통제상 미비점이 존재한다(예, 데이터 직접 변경 통제 부재)는 것은 IT시스템에서 생성, 저장 및 처리되는 정보를 신뢰할 수 없으므로 비즈니스 프로세스 상 IT시스템에 기반하는 제반 통제활동(ITGCs가 잘 이루어진 기반에서 현업부서 비즈니스 프로세스 상 자동화 되어있는 업무에 관한 통제 – 예를 들어, 운반비는 정해진 비용 테이블과 계산 로직에 의해서 자동계산 된다)이

무력화된다는 의미입니다.

반대로 ITGCs에 통제상 미비점이 발견되지 않는다는 것은 IT시스템이 제공하는 기능 및 IT시스템에서 관리되는 정보가 신뢰할 수 있다는 것으로 비즈니스 프로세스 상 IT시스템에 기반하는 제반 통제활동이 유효하다는 의미입니다.

정보기술이 고도화됨에 따라 기업은 정보처리의 많은 부분을 IT시스템에 고도로 의존하기 때문에 IT시스템 관리 구조의 기반에 대한 통제는 선택이 아닌 필수임을 명심해야 합니다.

2. 정보기술일반통제(ITGCs) 구축

내부회계관리제도에서 요구하는 'IT시스템 관리 구조의 기반'에 필수적인 ITGCs 항목의 선정과 구축을 달성하기 위해서는 주요 위험요소에 대한 통제와 중점 고려사항이 충족되어야 합니다.

주요 위험요소로는 ▲데이터를 잘못 처리하거나, 잘못된 데이터를 처리하는 시스템에 의존 ▲데이터에 대한 승인되지 않은 접근으로 데이터가 부적절하게 변경 ▲IT부서 인원의 업무분장이 적절하지 않을 위험 ▲승인되지 않은 마스터 파일의 수정 ▲시스템이나 프로그램의 부적절한 변경 ▲적절하지 않은 수작업 개입 ▲데이터 유실 위험 등으로 ITGCs는 이러한 주요 위험요소를 통제할 수 있도록 다음의 예와 같이 구축 및 운영됩니다.

관리 영역	주요 위험	통제활동 사례
프로그램 개발	• 개발프로세스에 대한 부적절한 적용으로 인해 의도한 대로 프로그램 개발이 이루어지지 않을 위험 • 새롭게 적용된 시스템에 오류 등의 사유로 불완전하고 부정확하게 데이터가 생성될 위험	• 새로운 시스템의 개발 및 도입은 적절한 경영진에 의해 승인된다. • 전산시스템 및 응용프로그램의 개발은 현업부서 및 전산관련 부서의 적절한 테스트과정을 거친다.
프로그램 변경	• 승인되지 않은 시스템 및 프로그램의 수정 • 시스템이나 프로그램에 필요한 변경이 적절히 이루어지지 못할 위험	• 시스템에 대한 변경 요청은 적절한 경영진의 승인을 받는다. • 시스템의 변경을 적절히 테스트하고, 그 결과를 문서화한다.

프로그램과 데이터에 대한 접근보안	• 데이터에 대한 승인되지 않은 접근으로 데이터가 위조, 변조, 훼손 및 파기될 위험 • IT부서 인원이 과도한 권한을 보유하여 업무분장이 적절하지 않을 위험	• 구성원이 수행하는 업무의 내용 및 직무기술서 등을 고려하여 시스템 접근권한의 적정성을 정기적으로 검토한다. • 적시에 사용자 계정을 추가, 수정, 삭제할 수 있는 절차를 수립하고 적용하고 있다.
프로그램 운영	• 데이터 유실 위험 또는 필요한 데이터를 사용하지 못할 위험	• 재무보고에 필요한 데이터, 거래, 프로그램을 복구하기 위해 적절한 백업 및 복구절차가 존재한다. • 시스템과 관련된 장애나 오류 등을 기록하고 분석하여 동일한 문제의 재발을 방지할 수 있는 절차가 존재한다.

3. 정보기술일반통제(ITGCs) 주요 점검 포인트

ITGCs 주요 점검 포인트는 아래와 같습니다.

관리 영역	Question to Ask
일반	• IT정책서가 존재하며 적시에 업데이트되고 있는가? • IT시스템에 의존하는 통제활동과 관련된 시스템이 모두 ITGC 대상 시스템으로 관리되고 있는가?
프로그램 개발	• 신규 시스템의 개발 또는 도입이 적절한 IT관리자에 의해 승인되고 관리되고 있는가? • IT시스템의 개발은 현업부서 및 IT부서의 적절한 테스트 과정을 거치고 있는가?
프로그램 변경	• 프로그램 변경 이력이 관리되고 있는가? • 프로그램 변경 시 적절한 인원에 의해 검토되고 승인되고 있는가? • 프로그램 변경을 적절하게 테스트하고, 그 결과를 문서화하고 있는가?

프로그램과 데이터에 대한 접근보안	• 적시에 사용자 계정을 추가, 수정, 삭제할 수 있는 절차를 수립하고 적용하고 있는가? • 구성원이 수행하는 업무의 내용 및 직무기술서 등을 고려하여 시스템 접근권한의 적절성이 정기적으로 검토되고 있는가? • 데이터 직접 변경 이력이 관리되고 있는가? • 데이터 직접 변경 시 적절한 인원에 의해 검토되고 승인되고 있는가?
프로그램 운영	• 데이터, 거래, 프로그램을 복구하기 위해 적절한 백업 및 복구절차가 존재하는가? • IT시스템과 관련된 장애나 오류 등을 기록하고 분석하여 동일한 문제의 재발을 방지할 수 있는 절차가 존재하는가?

Contacts

삼일회계법인 내부회계자문센터

박승운 Partner

seung-woon.park@pwc.com

김재현 Senior-Manager

jaehyun.j.kim@pwc.com