선진국의 IT감사기준 분석을 통한 IT감사체계 발전방안 연구

2010. 2.

호진원

감 사 연 구 원

발 간 사

지난 10년간 공공부문의 정보화 및 전자정부사업에 대하여 대규모 예산이 투입되었으나 이러한 사업들이 원래의 목적을 달성하였는지의 여부에 대한 체계적인 점검활동이 부족하였고, 감사초점이 일정한 기준에 의하여 결정되기보다는 특정사안의 중요성, 감사증거 확보의 용이성 등 감사결과를 확신할 수 있는 경우에 대부분 맞추어져 있어 감사의 일관성이 부족하였다. 따라서 표준화된 감사기준에 따라 일관성 있고 체계적인 IT감사접근방법으로의 패러다임 전환이 필요한 시점이다.

대규모 예산이 투입되는 정보시스템 구축사업의 경우 상시 모니터링을 통하여 예산의 낭비를 막고 사업결과의 효과성 및 효율성을 주기적으로 관리감독하는 체계가 마련되어야 한다. 그럼에도 불구하고 정보화사업에 대한 감사원 감사가 비정기적·비계획적으로 이루어고 있는 것은 중요도 면에서 사회적 파급효과가 큰 감사에 집중하고, 증거 확보가 비교적 용이한 감사에 중점을 두고 있기 때문에 상대적으로 소홀한 것이라고 예상된다.

따라서 본 연구에서는 체계적인 감사기준을 통한 점검활동과 감사의 일관성을 확보하기 위하여 IT감사의 개념 및 GAO, NAO 등 주요국 감사원의 IT감사 현황을 살펴보고, INTOSAI, 미국 정보시스템감사통제협회(ISACA) 등의 국제적인 IT감사기준을 감사단계별로 비교·분석해보고, IT감사수행 시 공통적으로 고려하여야 할 전략, 12개의 감사중점사항을 제시하였다. 이러한 종

합적인 연구결과가 감사원의 IT감사를 한층 발전시키는 첫 단추가 되기를 희망한다. 끝으로 본 연구를 위하여 열심히 수고해준 호진원 연구관의 노력에 감사를 표하는 바이다.

2010년 2월

감사원 감사연구원

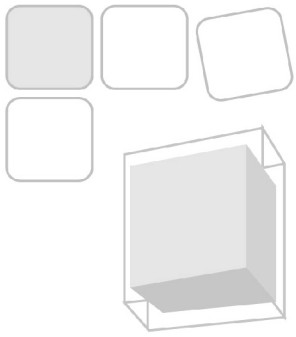
원장 **김용우**

목 차

목 차

표 목차

그림 목차



제1장 서 론

제1장 서 론

제1절 연구목적

1. IT감사기준 마련 필요

우리나라 감사원은 IT감사를 수행하는 데 있어 이에 적용할 표준화된 기준과 절차가 아직 마련되어 있지 않은 상황이다. 감사원에서는 성과감사·특정과제감사 또는 기관운영감사 등 다양한 감사를 통해 각 부처에서 추진 중인 정보화사업에 대한 감사를 실시하여왔다. 그런데 이러한 감사원 감사는 주기적으로 이루어진 것이 아니라 감사원의 연간감사계획에 따라 성과감사나 특정과제감사로 정보화사업을 감사대상으로 한 집중적인 감사가 이루어지는 경우가 있거나 다른 형태의 감사나 기관운영감사에서 개별정보시스템에 대한 감사가 이루어지는 경우가 있다(이미영·이영범, 2009). 또한 감사원이 재무감사, 성과감사 등 다양한 분야의 감사활동을 수행해왔지만, IT분야의 감사활동은 다른 감사활동에 비해 비중이 높지 않았던 것이 사실이다. 대규모 예산이 투입되는 정보시스템 구축사업의 경우 상시 모니터링을 통하여 예산의 낭비를 막고 사업결과의 효과성 및 효율성을 주기적으로 관리·감독하는 체계가 마련되어야 한다. 그럼에도 불구하고 정보화사업에 대한 감사원 감사가 비정기적·비계획적으로 이루어고 있는 것은 중요도 면에서 사회적 파급효과가 큰 감사에 집중하고, 증거 확보가 비교적 용이한 감사에 중점을 두고 있기 때문에 상대적으로 소홀한 것이라고 예상된다. 또한 감사원 내부에 IT감사에 필요한 전문성이나 전문인력이 확보되어 있지 않은 것도 원인이라고 볼 수 있다. 금융감독원이나 정보화진흥원의 경우는 선진국 IT감사기준을 도입하여 운영 중으로 감사원도 IT감사기준 마련이 시급한 실

정이다. IT감사를 하기 위해서 감사인들은 전문적인 IT감사기준에서 정의하고 있는 요구사항을 정확하게 이해하고 있어야 한다. 또한 IT감사를 수행하는 데 영향을 미치는 관련 법규 등에도 지식이 있어야 한다. 최고감사기구에서 수행하는 IT감사는 국제기준이나 그에 상응하는 국가의 IT감사표준을 따라야 한다. 우리나라는 아직 국가 차원의 IT감사기준이 없는 상태라 이에 대한 방안 모색이 시급하다. 국가 차원의 IT감사기준이 없더라도 국제기준에 맞추어 IT감사를 수행하는 것이 IT감사의 효과성 및 효율성을 개선하는 데 도움을 줄 수 있을 것이다.

2. 체계적인 IT감사 실시 필요

정보화진흥원이 주관하여 실시하고 있는 기존의 '정보시스템감리제도'는 자율적으로 감리 수감 여부를 결정할 수 있었기 때문에 국가적으로 중대한 정보시스템 구축사업임에도 불구하고, 감리를 받지 않아 문제점을 사전에 발견해내지 못한 사례들이 발생하였고, 감리의 지적사항은 권고사항이었기 때문에 실질적인 개선을 추진하지 않아 감리의 효과를 반감시키는 사례가 발견되었다. 또한, 감리업무의 특성상 감리현장에 투입되는 감리인력의 전문성이 매우 중요함에도 불구하고, 자격에 대한 기준과 책임 소재 등이 불명확하여 부실감리가 발생하는 경우에도 이를 제재할 근거가 없었다(한국정보사회진흥원, 2007). 또한 1987년부터 17년간의 정보시스템 감리분야는 감리방법론적 지식체계 미흡, 감리 관련 기준/지침/절차의 연계 방안 부족, 국내외 유사 감리체계와의 관계 미정립 등 아직까지 정보시스템 감리는 하나의 통합 프레임워크로 체계화되어 있지 않아 이러한 문제점들을 제기하고 있다(한국전산원, 2003). 또한 정보화진흥원이 지난 2009년 7월에 감리제도의 현황과 문제점과 관련하여 이해관계자들을 대상으로 설문조사한 결과, 감리결과의 품질 편차가 크고, 저가입찰 과당경쟁 등으로 감리품질 확보가 어려운 것으로 나타나 위의 문제들이 현재에도 해결되지 못한 채 진행되어 오고 있음을 알 수 있다.

정보와 정보시스템은 조직의 핵심적인 자원 중의 하나이다. 이러한 자원이 효율적이고 효과적으로 활용되지 못하면 조직의 전략적 목표 달성에 지장을 초래하게 된다. 이러한 중요한 자원을 체계적으로 관리하기 위해서는 정보시스템에 대한 적절한 통제가 수립되어야 하고, 이러한 통제가 적절하게 잘 작동하고 있는지를 점검하고, 여기에 대하여 필요한 조언을 해주는 기능, 즉 정보시스템 감사기능의 수립 및 실행이 필요하다. 우리나라의 경우 민간 및 공공부문은 전반적으로 정보시스템을 도입한 역사가 오래되었고, 무제한적인 기술의 사용을 장려하는 시기는 이미 지난 것으로 판단된다. 따라서 정보시스템의 효율성 및 효과성 등을 평가하여 정보시스템이 조직의 목표 달성을 위해 어느 정도 기여하였는지, 그리고 이러한 목표 달성에 장애가 되는 통제 위험을 적정한 수준으로 관리하기 위해 정보시스템에 대한 감사체계를 도입하여 조직의 전반적인 위험 수준을 최소화하는 것이 필요하다(황경태, 2002). 그러므로 국가최고감사기구인 감사원이 IT감사의 체계를 정립하여 IT감사 관련 문제점들을 관련 기관과 협력하여 개선하는 데 주도적인 역할과 기능을 수행해야 한다.

3. 감사초점 선택의 일관성 노력 필요

IT감사가 실시되는 경우 감사초점이 일정한 기준에 의하여 선택되기보다는 특정사안의 중요성, 감사증거 확보의 용이성 등 감사결과를 확신할 수 있는 경우에 맞추는 경향이 있다. 이는 IT특성상 서류상 존재하지 않는 시스템 내부자료에 접근이 필요하나 적발 위주의 감사형태이다 보니 부처의 협조가 매우 미온적이어서 실효성 있는 증거 확보에 어려움이 있기 때문에 발생하는 문제라고 볼 수 있다. 그러나 감사원의 한정된 자원으로 파급효과가 큰 감사분야에 집중하다 보니 IT감사 수행의 여력이 없어서 발생하는 문제도 있다. 감사를 수행하더라도 아직 표준화된 IT감사기준이 없는 상태라 비교적 증거확보가 용이한 부문에 초점을 맞추어 감사가 진행되다 보니 감사의 사각지대

가 발생할 우려가 높고 감사의 질 제고를 담보하기가 어려운 상황이다.

4. 국가 정보화사업의 지속적인 모니터링 필요

우리나라의 정보화사업은 규모와 내용 면에서 광범위하여 사업 전체를 일시에 감사하기란 불가능하다. 따라서 표준화된 감사기준 및 절차를 기반으로 하는 정기적인 감사만이 가능할 것이다. 그동안 전자정부사업은 8,984명 인력 감축 효과, 약 1조 원의 예산 절감, 사회경제적 효과로 연간 15조 원 이상 비용 절감을 성과로 내세우고 있으나(2007년 9월 행정자치부 '전자정부 추진경과 및 성과' 자체 발표자료) 개인정보 유출 및 사이버테러 우려 증가, 정보격차 해소 문제, 부처 간 시스템 및 데이터의 중복과 상호운용성 미흡, 정보자원 및 서비스의 공동이용 곤란 등 다양한 문제가 아직 상존하고 있다. 따라서 이러한 성과결과가 정확한 것인지, 평가는 객관적이고 투명한 평가지표에 의하여 도출한 결과인지, 이러한 문제점들은 어느 정도 개선되었는지 등에 대한 확인 및 점검이 미흡하였다. 위에서 언급한 바와 같이 체계적인 절차 없이 부분적인 접근방법으로 부분적인 문제점만 지적하고 개선을 요구한 경우가 대부분이었다. 이런 상황에서 행정안전부는 2009년도 총 정보화예산 2729억 원 중 39%에 해당하는 1052억 원의 예산을 투입하여 10여 개의 '전자정부지원사업'을 신규로 추진할 예정이어서 체계적인 IT감사의 도입은 시급한 과제가 아닐 수 없다. IT는 모든 정부행정업무 및 사업에 인프라 역할을 하고 있기 때문에 IT를 어떻게 활용하느냐에 따라 사업의 성공과 실패가 좌우된다. 그러므로 IT감사는 필요한 경우에만 선택적으로 하는 특정감사의 형태가 아닌 일상감사의 형태로 실시되어야 한다는 인식전환이 필요한 시점이다. 또한 향후 '국가정보화 기본계획', '녹색뉴딜 사업계획'에 따라 대규모 IT사업 추진('12년까지)으로 감사원의 IT감사 비중 증가가 예상되므로 상시 모니터링의 기반 구축이 필요하다.

제2절 IT감사 개념

IT(Information Technology)감사는 정보시스템이 조직의 컴퓨터 자산(하드웨어 및 소프트웨어)을 안전하게 보호하는지, 데이터의 무결성(integrity)을 유지하는지, 조직의 목표를 효과적으로 달성하는지, 조직의 자원을 효율적으로 사용하고 있는지 여부를 파악하기 위한 증거를 수집하고 평가하는 절차이다(Weber, 1999; Pathak, 2005)

하드웨어 및 소프트웨어 등의 컴퓨터 자산을 보호한다는 의미는 컴퓨터의 손실 또는 파괴, 권한이 없는 사용자의 도용이나 도난 등으로부터 보호한다는 것을 말한다. 데이터의 무결성 상태는 정보시스템 내부에서 활용되는 데이터가 정확하고, 완결성이 있고, 일관성 있는 것을 의미한다.

컴퓨터를 이용한 정보처리와 인터넷 등과 같은 통신기술에 의해 융합된 형태의 정보통신기술의 발달은 조직의 업무처리 신속화, 생산성 향상 등 순기능적인 효과가 있는 반면, 이에 따른 역기능적인 문제점 역시 매우 심각해지고 있는 상황이다. 예를 들어 증권시장에서의 전산시스템 장애나 최근의 DDoS(Distributed Denial of Service)로 인한 불특정 다수 시스템 장애 등은 어느 한정된 기관의 문제가 아니라 사회 경제적인 문제로 확대될 수 있다. 이외에도 컴퓨터를 이용한 데이터를 조작하여 부정행위나 범죄를 저지르는 등 점차 문제가 복잡해지고 영향력이 커지고 있다. 정보시스템의 도입은 기존의 수작업 처리에서 업무처리가 컴퓨터에 의해 처리됨으로써 업무상 책임문제, 감사에 필요한 증거문제, 전자매체에 기록된 자료를 검토할 수 있는 특별한 기법의 발전 등이 요구되었다. 이처럼 정보시스템의 이용범위가 확대되면서 조직의 정보시스템에 대한 의존도도 증대되고 시스템에 장애가 발생하였을 때 그 파급효과로 인한 불편과 피해도 점점 증가하는 추세이다. 또한 정보시스템에 대한 투자가 계속 증가하면서 투자에 대한 효과가 어느 정도인지 검토해야 할 필요성이 대두되었다. 이러한 요구를 기반으로

정보시스템의 효과성·효율성·경제성 측면을 객관적이고 투명하게 평가할 수 있는 정보시스템 감사가 필요하게 된 것이다(박종태, 2006). 예를 들어, 정보화사업에 대한 감사는 정보화 추진의 장애요인과 그 문제점들을 분석 검토하고 개선방안을 제시함으로써 국가정보화사업의 효율적 추진에 기여해야 한다. 따라서 정보기술의 활용이 급격히 확산·통합되어감에 따라 기존의 회계감사뿐만 아니라 시스템 개발 및 운영과정에서의 내부통제와 보안, 그리고 성과감사 측면에서 감사의 필요성이 대두되고 있다(이재권, 2001).

정보시스템 감사는 정보시스템이 적시에 정확하게 누락되지 아니하고 완전한 정보를 생산하고 있는가를 평가하는 통제의 감사에만 국한되는 것이 아니다. 즉, 응용소프트웨어의 내부통제뿐 아니라 정보시스템을 함께 구성하는 시스템 소프트웨어와 정보 그 자체의 데이터도 감사대상이 된다. 사용자의 입장에서 정보시스템 운영절차와 보안, 그리고 시스템 관리자의 입장에서 정보처리에 필요한 자금, 데이터, 기계설비, 인력, 소모품 등 각종 자원의 관리도 감사대상이 되어야 한다. 그래야 정보시스템에 관련한 모든 구성요소들을 엄밀하게 평가할 수 있다. 그뿐 아니라 '정보시스템이 어떠한 개발주기를 거쳐 개발 혹은 외부로부터 취득되었는가?', '정보시스템의 유지 보수는 어떻게 진행되는가?' 하는 것까지도 감사의 대상이 된다. 심지어는 정보시스템 감사방법론까지도 관리하는 것이 원칙이다. 다시 말해서 감사란 '무엇을, 어떻게, 왜' 등의 질문 등을 던지며 정보시스템의 모든 영역을 평가하는 과정이라고 볼 수 있다(장태범·김문오, 2004).

그러나 이러한 일반적인 IT감사의 개념 정의에도 불구하고 IT감사의 개념에 대하여 혼동하는 경우가 있다. 그 하나는 IT감사가 IT를 이용한 감사인지 아니면 IT를 대상으로 한 감사인지 하는 부분이고, 또 하나는 IT감사와 감리의 차이점에 대한 부분이다.

먼저 일반적인 IT감사의 대상은 IT 자체이다. 이 IT에는 정보시스템이 근간을 이루므로 IT감사의 대상을 정보시스템이라고 볼 수 있다. 조직에서 정보시스템이 제대로 원하는 목적에 맞추어 작동하고 있는지를 시스템 평가로

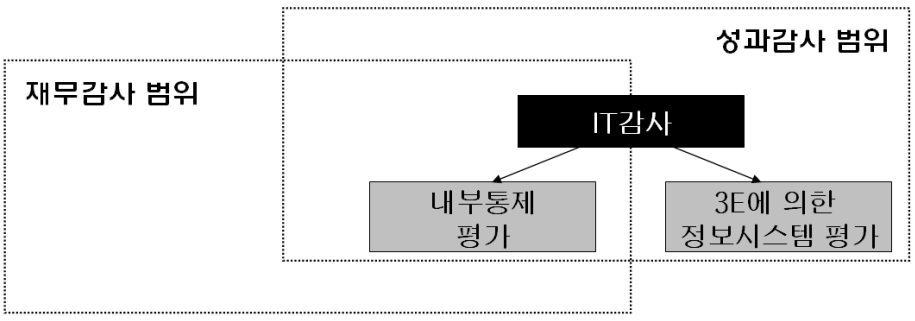
만 알 수 있는 것이 아니라 시스템과 유기적으로 연결된 전략, 인력, 재무, 조직 등 시스템 외적인 환경과의 관계 분석이 필수적이다. 왜냐하면 시스템에서 나오는 모든 결과물이 이러한 시스템 외적인 환경에도 영향을 주기 때문이다. 따라서 이러한 결과물이 정확한 것인지, 믿을 수 있는 것인지 등을 파악하려면 시스템 자체의 복잡성 때문에 이를 일일이 대조하면서 검사하기란 어렵기 때문에 소프트웨어의 도움이 필요하다. 이럴 경우에 사용하는 기법이 '전산감사기법(Computer Assisted Audit Techniques, CAAT)'인 감사의 기능 및 생산성을 향상시킬 수 있는 컴퓨터 기반의 기술/프로그램을 모두 포함하는 광범위한 개념이며, 협의적 개념은 데이터의 추출 및 분석을 위한 모든 감사기법을 의미한다. 현재 전 세계적으로 사용 중인 전산감사기법 전문 소프트웨어로는 ACL, IDEA 등이 있으나 우리가 많이 사용하고 있는 엑셀 등 범용 소프트웨어도 전산감사기법으로 사용할 수 있다. 이 경우 넓은 의미에서는 'IT를 이용한 감사'라고 할 수 있지만 정확히 말하면 '소프트웨어를 이용한 IT감사'라고 표현하는 것이 더 적절하다. 그러므로 IT감사는 IT를 대상으로 한 감사와 소프트웨어를 이용한 IT감사 모두를 포함하는 개념이다.

다음은 IT감사와 감리의 차이점에 대한 부분인데, 한국전산원(2003)에 따르면 "정보시스템의 감리란 위험평가를 통해 통제의 필요성을 판단하고, 통제대책의 설정과 적용 여부를 검토하는 것"이다. 여기서 '위험'이란 정보시스템에 대한 투자 대비 성과가 낮은 경우, 조직 내 정보시스템 활용률이 저조한 경우, 정보시스템의 정보 오류 또는 누출, 시스템 다운으로 인한 정보 손실 등이 해당되며, '통제'란 정보시스템의 구축과 운영에 따른 많은 위험요인에 대하여 정보시스템 자산을 보호하기 위한 대비책을 의미한다. 한편 한국전산원(2003)의 '감리'에 대한 정의는 "성과의 극대화를 위하여 주로 기술적인 측면에서 기획에서 개발, 운용단계에 이르기까지 단계별 또는 종합적으로 합리성·타당성·신뢰성·안정성·효율성 등을 조사하고 감독하는 평가행위"이고, '감사'는 "주로 회계적인 측면에서 예산운영과 집행결과에 대한 합법성·정당성·적정성 등을 조사하고 검증"한다고 주장하고 있다. 그러나 신

동익(2003)은 IT감사는 단순히 기술적 정보시스템에만 국한되는 것이 아니라 업무처리 프로세스의 전반적인 검토와 평가를 의미하며, 이는 업무성과 측면의 평가라고 정의하고 있다. 따라서 한국전산원의 주장처럼 감사가 회계적인 측면에 국한되어 있다는 시각은 감사의 영역을 좁게 해석한 것에 지나지 않는다. 오히려 감리의 경우 실제로 업무 분석부터 평가까지 수행되는 경우보다는 프로젝트가 착수되고 계약이 시작된 이후부터 프로젝트가 종료되는 시점까지 형태를 가지고 있어 개발감리 위주의 제한된 성격이 강하다(신동익, 2003). 정보시스템의 감리와 IT감사라는 용어가 혼용되고 있으며 일부에서는 감리와 감사가 다르다고 주장하고 있으나 정보시스템에 대한 경제성·효율성·효과성 평가에 초점을 맞추고 있다는 측면에서 모두 공통점을 가지고 있어 감리와 감사는 동일한 의미로 해석하는 것이 바람직하다. 해외 사례를 보더라도 어느 국가든 IT감사와 감리를 분리한 경우를 보지 못하였으며, 감리하는 용어 자체가 존재하지 않는다. 따라서 본 연구에서는 IT감사와 감리를 동일한 의미로 사용하도록 한다.

IT감사는 '내부통제 평가'와 경제성(Economy)·효율성(Efficiency)·효과성(Effectiveness)을 바탕으로 한 '정보시스템 평가'의 두 영역으로 구분할 수 있다. 수감기관의 내부통제 평가는 재무와 성과감사의 영역이므로 IT감사는 재무감사와 성과감사의 구성요소라고 볼 수 있다. 3E에 의한 정보시스템 평가는 성과감사 매뉴얼에 의해 수행되는 별도의 정보시스템 성과감사라고 정의할 수 있다(INTOSAI, 2006a).

〈그림 1-1〉 IT감사의 범위



IT감사의 목적은 감사의 성격이나 종류에 따라 달라질 수 있는데 예를 들어 IT감사가 재무감사의 일환으로 수행된다면 재무감사가 재무에 초점이 맞추어져 있으므로 주목적은 재무제표가 기관의 재무상태를 기준으로 정확하고 공정하게 반영되었는지 여부를 파악하는 것이다. 반면 성과감사의 한 부분으로 IT감사가 수행될 경우 IT감사의 목적은 모든 부분에서 IT 시스템이 문제없이 효과적으로 작동되고 있는지 파악하는 것이다(ASOSAI, 2003).

모든 정보시스템은 그 속성상 '취약성(vulnerability)'이 있다. 모든 시스템은 내·외부적으로 '위협(threat)'을 받으며, 여기에는 물리적·인위적·자연적인 것을 모두 포함할 수 있다. 이러한 위협은 정보시스템에 '위험(risk)'을 초래하게 된다. 이 위험이라는 것은 잠재적인 것으로 손실, 손해, 역기능 등의 발생 가능성을 뜻한다. 따라서 이러한 위험을 차단하거나 감소시키기 위해서는 통제 기능이 필요한데, 이러한 통제는 항상 현실적이고 조직 특성을 반영하는 상대적인 것이어야 한다. 완전 통제란 있을 수 없다. 왜냐하면 완전 통제를 위한 무리한 통제는 시스템 기능 자체를 마비시킬 우려가 있기 때문이다. 따라서 이 통제 기능은 언제나 비용 대비 효과에 따라 설정되는 것이며 여기에 감사기능이 등장하게 된다. 즉, 시스템의 개발과정에서 적합한 통제가 구축되고 있는지, 운영 중인 시스템에 설정되어 있는 각종 통제가 적절한 것인지, 효과적이며 효율적인 운영을 하고 있는지를 검토, 확인, 평가하는 것이 IT감사이다(이장형, 1997).

다시 말해 정보시스템의 가치를 극대화하는 것은 잠재적인 위험요소를 최소화하는 것과 연관이 있으며, 이러한 잠재적인 위험요소를 관리하기 위해서 필요한 것이 통제기능이며, 이러한 통제기능이 조직 내에서 제대로 운영되고 있는지를 파악하는 것이 IT감사의 목적이다. 그리고 감사의 목적이 의사결정자에게 유용하고 신뢰성 있는 정보를 제공하고 내부통제와 시스템의 적정성을 향상시키는 것이라 하면 IT통제수단은 전산화된 환경에서 이와 같은 목적을 달성하는 데 있어 기관의 내부통제구조를 이해하는 데 핵심적인 요소라 할 수 있다. 따라서 IT통제수단은 감사계획의 수립, 감사실시, 보고

등 감사의 모든 단계에서 반드시 고려해야 한다. 정보시스템에 대한 감사의 필요성이 증대된다고 하여도 일반적으로 전통적인 회계감사에서 이루어지는 감사절차와 방법론 자체가 근본적으로 바뀌어야 하는 것은 아니다. 다만 전산화된 환경에서 나타나는 특성을 감안하여 이를 반영하여야 하는 것이다. 그러므로 IT감사는 기존의 재무감사나 성과감사를 실시하면서 나타나는 정보시스템과 관련한 IT특성을 반영하여 실시되므로 기존 감사의 한 부분으로 볼 수 있다. 예를 들어 재무정보는 대개 정보시스템에 의하여 처리되어 나오는 결과이므로 정보시스템 통제가 재무감사와 관련이 있기 때문이다. 또한 필요에 따라 IT감사는 정보시스템적인 측면만 고려하여 실시될 경우 별도의 독립된 감사형태로 실시할 수 있다.

제3절 IT감사 유형

〈그림 1-1〉에서 설명한 바와 같이 IT감사는 재무감사나 성과감사의 일부분으로 포함해서 볼 수 있는데 재무감사의 일부분으로 수행하는 경우 재무감사는 IT시스템에서 생산되는 데이터의 정확성 및 신뢰성을 판별하는 것이 주요 목적이 된다(Cascarino, 2007). 따라서 IT감사 측면에서 재무감사를 지원할 때 감사인은 주로 '전산감사기법' 소프트웨어를 사용하여 필요한 데이터를 추출·비교하여 이를 검증하는 임무를 수행하게 된다.

'운영감사(Operational Audit)'는 업무의 효과성과 효율성에 초점을 맞추고 IT 자체를 하나의 업무 기능으로 포함시켜서 보는 것으로 성과평가기준을 토대로 계획 대비 실적이 어느 정도 되는지를 판단하는 것이 목적이다(Cascarino, 2007). 이러한 의미에서 운영감사는 IT감사가 성과감사의 한 부분으로 수행되는 경우 ['정보시스템 성과감사(INTOSAI, 2006b)'라고도 함] 효율성·경제성·효과성과 관련된 이슈들을 평가한다는 점에서 성과감사 유형과 거의 일치한다고 볼 수 있다.

'일반통제 감사(General Controls Audit)'는 정보처리기능 및 설비와 관련한 관리통제(management control)에 초점을 맞추어 실시하는 감사로 운영적(operational)인 측면이나 규정 준수(compliance) 여부를 검토한다(Cascarino, 2007). 다시 말해 조직의 모든 정보시스템을 포함하는 내부통제를 평가하는 것을 말한다(INTOSAI, 2006a). 일반통제는 데이터센터 운영, 시스템 소프트웨어 구매 및 유지보수, 접근보호 및 시스템 개발/보수 등이 포함된다. 여기서 검토되는 주요 내용은 IT정책, IT보안기준 및 가이드라인, 어플리케이션 개발 및 변경 통제, 직무분리, 사업연속성 계획, IT프로젝트 관리 등이다. 따라서 일반통제의 검토사항은 개별 프로그램에 대한 것이 아니라 수감기관의 IT부서 또는 유사한 기능에 초점을 맞추는 것이 특징이다. 예를 들어 IT 정책, 정보보안 기준 및 가이드라인, 소프트웨어 개발, 업무분리, 업무지속계획

(business continuity planning), IT프로젝트 관리 등이 검토사항으로 포함된다(ASOSAI, 2003).

'어플리케이션 통제감사(Application Control Audit)'는 특정 어플리케이션에서의 데이터 입력, 처리, 보호(protection), 결과 획득 등과 관련된 통제를 평가하는 것이고, 정보시스템 개발통제감사(Information Systems Development Controls Audit)는 정보시스템 개발 시작부터 완료까지의 관리와 통제를 평가하는 것이다(INTOSAI, 2006a).

제4절 IT감사 동향

INTOSAI는 정보기술의 중요성 인식이 증가함에 따라 1989년 IT워킹그룹을 통하여 회원국 간의 IT감사 지식과 경험을 공유하고 있다. 현재 미국·영국·캐나다·일본·중국 등 33개국이 참여하고 있으나 우리나라는 아직 비회원국이다. INTOSAI의 IT워킹그룹은 특히, 전자정부 감사 및 IT거버넌스에 대한 관심이 증가함에 따라 이를 위한 감사기법, 기준, 사례 등에 관한 데이터베이스를 운영 중이며, ASOSAI는 지난 2003년 호주·중국·인도·말레이시아 4개국이 공동으로 진행한 연구 프로젝트에서 'IT감사 가이드라인'을 발표한 바 있다.

미국 GAO의 전략계획(2007-2012)에 의하면 핵심 이슈 7개를 주요 주제로 선정하고, 각각의 흐름변화가 정부 주요정책에 미치게 될 영향과 대응방향을 제시하고 있다. 오늘날 정보기술이 전 세계적으로 개인과 조직, 경제를 연계하는 주요 동력으로서 삶의 질, 경제 및 정부의 성과, 정부와 국민 간의 관계 등에 영향을 주고 있는 가운데, 정부는 정보기술 변화의 잠재력을 평가하고 보안, 사생활, 평등 등에 미칠 영향을 평가할 수 있는 능력을 보유할 필요가 있으며, 따라서 데이터 정보의 오·남용 방지, 사이버 보안 및 개인정보 보호, 데이터의 정확성과 신뢰성 확보 등을 주요 주제로 선정하였다. 또한 GAO는 2007년부터 매년 고위험 영역을 선정하여 중점 관리하고 있는데, 2009년 1월에 발표한 '고위험 시리즈(업데이트)' 보고서에 따르면, "연방 정보시스템과 국가 주요 시스템 인프라의 보호"를 29개의 주요 고위험 영역 중의 하나로 선정함으로써 정보보안에 대한 감사의 중요성을 강조하고 있다.

한편, 영국 NAO의 2009년도 연차보고서에 의하면 정부부처 및 공기업의 데이터는 안전하게 보호되어야 하며, 이를 효과적으로 달성하기 위하여 '행정부처 보안정책 체계(Cabinet Office Security Policy Framework)'를 제시함으로써 정보보안 감사의 기반 구축을 위해 노력하고 있다.

제5절 IT감사 관련 법제도 및 체계

IT감사는 용어상 혼용되어 사용하고 있는 정보시스템 감리와 관련된 법제도 및 체계에서 찾아볼 수 있는데 「정보시스템의효율적도입및운영등에관한법률」에서 '정보시스템 감리'에 대한 정의, 대상, 범위 등을 규정해 놓고 있다. 정보시스템 감리점검체계는 1999년 제정된 정보시스템 감리기준에 첨부된 기본점검표를 기반으로 그 체계가 정립되었으며 3차에 걸쳐 신규 정보화 사업유형 및 개발방법론, 국제 IT 가이던스 등을 수용하면서 현재의 감리체계를 구성하게 되었다. 현재의 국내 정보시스템 감리체계는 「정보시스템의효율적도입및운영등에관한법률」을 근거로 '정보시스템 감리기준(행정안전부 고시 2008-18호)'과 한국정보사회진흥원의 정보시스템 감리점검 해설서(2008. 3. 3.), 정보시스템 감리기준 해설서로 구성되어 있다.

「정보시스템의효율적도입및운영등에관한법률」 제2조 3항에 따르면 '정보시스템 감리'는 감리 발주자 및 피감리인의 이해관계로부터 독립된 자가 정보시스템의 효율성을 향상시키고 안전성을 확보하기 위하여 제3자적 관점에서 정보시스템의 구축에 관한 사항을 종합적으로 점검하고 문제점을 개선하도록 하는 것으로 정의하고 있다. 또한 공공기관의 장은 정보시스템의 특성 및 사업 규모 등이 대통령령이 정하는 기준에 해당하는 정보시스템 구축사업에 대하여 정보시스템 감리를 하도록 되어 있다(제11조 1항). 정보시스템 감리를 수행함에 있어 기본이 되는 기준은 「정보시스템의효율적도입및운영등에관한법률」 제11조 제4항에 의거하여 2008년 6월 19일 행정안전부 고시 제2008-18호로 개정 고시된 정보시스템 감리기준(이하 감리기준)이다. 이 조항에는 정보시스템 감리를 하는 감리법인 또는 기관이 정보시스템 관리를 효율적으로 하도록 하기 위하여 필요한 기준(감리기준)을 정하여 고시하여야 한다고 밝히고 있다.

한편, 감사원의 경우 「공공감사기준」 제20조(전산화된 환경에서의 감사)를

보면 “감사대상기관의 업무처리가 전산화되어 있는 경우에는 그 수준과 특성을 충분히 고려하여 감사를 계획하고 그에 적합한 감사절차를 적용한다”라고 규정하고 있다. 그러나 이러한 조항이 구체적인 IT감사계획과 절차 등을 명시한 것은 아니다. 다만, 「공공감사기준」 제2조에 경제성·능률성·효과성에 대한 검토와 평가를 위주로 특정사업이나 정책에 대하여 수행하는 감사를 “성과감사”라고 정의하고 있다. 이는 IT감사가 정보시스템에 대한 경제성·효율성·효과성 평가에 초점을 맞추고 있다는 측면에서 IT감사를 성과감사의 일부로 볼 수 있다는 법적 해석이 가능하다. 한편, 감사원 규칙 「감사원사무처 직제」 제8조 2항에서 기획관리실이 “전산업무와 전산감사 지원업무 등 감사 지식관리업무”를 수행한다고 명시하고 있는 것 외에 다른 IT감사 관련 구체적인 기준이나 내용을 발견할 수 없다.

미국 GAO의 경우, 연방 정보시스템 통제 감사기준이 포함된 주요 법률인 「연방정보보안관리법(Federal Information Security Management Act of 2002)」이 있다. 다음 장에서 설명할 GAO의 ‘연방정보시스템 통제 및 감사 매뉴얼(FISCAM)’은 이 법에 의거하여 연방정부의 정보보안 프로그램의 독립적인 평가에 사용될 수 있다. 이외에도 미국의 경우 「사베인즈-옥슬리법(Sarbanes-Oxley Act of 2002)」[1]에 의거하여 내부통제 강화를 강조하고 있으며, 이는 IT통제가 조직 전반의 내부통제에 중요함을 시사하고 있다(IIA, 2005).

우리나라에는 IT와 관련된 법으로 「국가정보화기본법」, 「전자정부법」 등이 있다. 그러나 이와 같은 법이 IT감사와 직접적으로 관련된 것은 아니지만 IT감사의 목적과 필요성을 이러한 법의 근거로 설명할 수 있고 IT 관련 합법성 여부를 검토할 때 중요한 기준이 된다는 점에서 감사인들이 알아야 할 필요가 있다. 「국가정보화기본법」은 기존의 「정보화촉진기본법」, 「지식정보자원관리법」, 「정보격차해소법」을 통합한 것으로 2009년 8월 시행되었다. 이 법에 따라 모든 중앙행정기관의 장과 지방자치단체의 장은 국가정보

1) 이 법은 엔론과 월드콤 사태로 인하여 공공회계부문과 기업지배구조의 개혁을 위하여 제정한 법으로 기업의 회계감독 규정을 대폭 강화함으로써 회계정보의 투명성을 강조하고 있다.

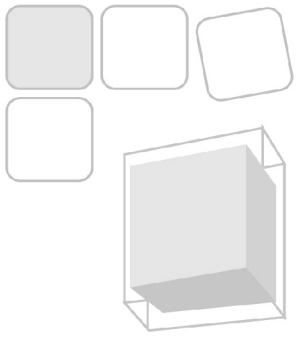
화 시행계획의 전년도 추진실적과 다음 연도의 시행계획, 중요 변경사항을 매년 4월 말까지 국가정보화전략위원회(대통령 직속)에 각각 제출해야 한다. 「전자정부법」은 기존의 「전자정부구현을위한행정업무등의전자화촉진에관한법률」에서 법명을 바꾸어 수정한 법으로 행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성·민주성을 높여 국민의 삶의 질 향상을 목적으로 하고 있다.

제6절 연구방법

본 연구에서는 IT감사기준 미흡 개선 및 체계적인 IT감사 실시를 위하여 GAO와 같은 외국의 감사원과 ISACA(Information Systems Audit and Control Association), INTOSAI(International Organization of Supreme Audit Institutions), IIA(The Institute of Internal Auditors) 등 감사 관련 기관들이 제시하는 IT감사지침과 국내 금융감독원과 정보화진흥원에서 사용하고 있는 IT감사 관련 지침들을 참조하여 IT감사를 실시할 때 감사계획, 감사실시, 감사보고 등의 절차에 따라 어떤 특징들이 있는지를 소개하고, 어떤 공통점과 차이점이 있는지를 비교·분석하였다.

이러한 IT감사기준 비교연구 결과를 바탕으로 주요국 IT감사사례를 비교·분석하여 우리나라 IT감사의 특징 및 문제점을 도출하여 감사원의 IT감사 개선방향에 대한 시사점을 제시하였다.

이를 위한 비교·분석의 틀을 제시하고 일관성 있는 감사초점의 선택을 도모하기 위하여 국내외 감사 관련 기관들의 감사기준의 공통점과 국내 선행 연구결과인 정보화사업 평가를 위한 표준평가항목의 관계 및 특징을 비교하여 공통된 감사초점들을 추출하였다. 이들 요소가 우리 법체계 실정에 맞는지 파악하기 위하여 현재 「국가정보화기본법」, 「전자정부법」, 「정보시스템의효율적도입및운영등에관한법률」의 IT 관련 법조항과 내용들을 비교·검토하였다. 이는 국가정보화사업의 지속적인 모니터링을 위하여 필요한 부분이라고 판단된다. 이 결과를 토대로 공통된 감사초점들을 비교·분석의 틀로 이용하여 국외사례의 경우 GAO, NAO, 캐나다 OAG, 호주 ANAO 등의 2008-2009년도에 실시한 IT 관련 감사보고서를 검토하였다. 국내사례의 경우 감사원의 주요 IT 관련 감사보고서 내용을 비교·분석하여 그 특징을 알아보았다. 본 연구에서 IT감사기준 및 초점 검토, 그리고 선진국 감사원의 IT감사사례를 비교함으로써 우리 원의 현주소와 앞으로 나아가야 할 방향에 대한 디딤돌이 되기를 기대한다.



제2장 IT감사기준 비교·분석

제2장 IT감사기준 비교·분석

IT감사기준은 IT감사를 수행하는 데 필요한 특성, 기술, 절차 등에 대한 기본 원칙과 관련 지침을 제공함으로써 IT감사를 일관성 있고 체계적으로 수행할 수 있도록 도모하는 데 목적이 있다. 이를 위하여 정보시스템 감사 및 보고에서 반드시 따라야 할 의무사항을 정의하고, 어떻게 기준을 반영하여 구현할 것인가에 대한 전문적인 판단방법을 제시하며, 감사완료 시 기준과의 부합성에 대한 구체적인 정보를 제공하고 있다. 이 IT감사기준에 따르면 IT감사계획 수립 시 감사목표, 관련 법령, 감사기준을 고려하여 정보시스템 감사적용범위를 결정해야 하고, 위험기반 감사접근방법을 사용해야 하며, 감사기간, 감사의 성격, 필요한 자원 등을 확인하여 문서화해야 한다.

제1절 GAO의 연방정보시스템 통제 및 감사 매뉴얼

GAO의 '연방정보시스템 통제 및 감사 매뉴얼(FISCAM, Federal Information Systems Control Audit Manual)'은 연방정부 및 다른 정부부처에서 사용하는 전문적인 감사기준과 합치되는 정보시스템 통제감사 수행을 위한 방법론이다. FISCAM은 주로 미국의 '일반적으로 인정되는 정부감사기준(Generally Accepted Government Auditing Standards, GAGAS)'에 근거하여 수행되는 재무감사, 성과감사, 입증감사에 사용될 수 있으며, 정보시스템 통제의 효과성 및 효율성 평가를 위하여 설계되었다. 주요 특징으로는 위험기반의 접근방법을 채택하여 감사목적을 달성할 수 있도록 지원해주고, 감사위험에 대한 통제와 효과, 일반통제(General Control)와 어플리케이션 통제(Application Control)에 대한 영향, 보안관리 등을 평가한다. FISCAM은 정보시스템 통제

의 효과성 평가를 위한 방법론으로 감사기준(standards)이라기보다는 단독으로 정보시스템 감사를 실시하거나 성과감사, 재무감사, 입증감사 등의 일부분으로 실시할 경우 효과적이고 효율적으로 정보시스템 통제감사를 수행할 수 있도록 지침(guidance)을 제공하는 것으로 보는 것이 정확하다.

감사인(auditors)은 정보시스템 통제가 감사목적과 관련이 있는지 여부를 결정해야 한다. 일반적으로 정보시스템 통제는 재무정보가 정보시스템에 의하여 대체적으로 처리되기 때문에 재무감사와 관련이 있다. 재무감사와 관련된 프레임워크는 GAO와 '대통령 직속 무결성 및 효율성 자문위원회(President's Council on Integrity and Efficiency, PCIE)'가 공동으로 개발한 '재무감사 매뉴얼(Financial Audit Manual, FAM)'에 나타나 있다. FAM은 재무감사의 일부분으로 정보시스템 통제를 평가할 수 있는 프레임워크를 제공하며 FISCAM의 감사절차는 FAM의 관련 있는 감사절차에 잘 맞도록 수행해야 한다. 정보시스템 통제감사가 재무감사의 한 부분으로 실시되는 경우 재무제표 감사와 관련된 통제설계를 평가하기 위하여 위험평가절차(risk assessment procedures)를 수행해야 한다. 성과감사의 경우 감사인은 정보시스템 통제와 관련 있는 어떤 감사절차가 적절한 증거를 확보하는 데 필요한 것인지 결정해야 한다. 따라서 감사위험평가 및 감사계획에 필요한 정보시스템 통제에 대한 충분한 이해가 있어야 한다.

1. 감사계획

정보시스템 통제 감사계획을 수립하는 경우, 감사인은 효과적이고 효율적인 감사절차를 계획하기 위하여 감사의 중요도를 고려하여야 한다. 감사의 중요도에 따라 시간이나 절차상의 내용이 달라질 수 있기 때문이다. 따라서 감사인은 상대적으로 중요성이 낮은 정보시스템 통제 감사사항에 대하여 감사를 하지 않을 수 있다. 감사계획은 감사를 진행하는 동안 계획된 접근방법을 수정할 수 있으나 계획단계에서 계획 관련 활동에 집중하는 것이 중요

하다. 이러한 목적을 달성하기 위해서 계획단계에서 점검해야 할 사항은 다음과 같다.

- 정보시스템 통제감사의 전반적인 목적과 범위의 이해
- 수감기관의 운영과 주요 업무 현황 파악
- 수감기관의 일반적인 네트워크 구조 이해
- 주요 감사초점 영역 확인(예: 파일, 어플리케이션, 시스템 등)
- 기초적인 정보시스템 위험 진단
- 중점관리요소(critical control points) 확인
- 기초적인 정보시스템 통제 이해

가. 정보시스템 통제감사의 전반적인 목적과 범위의 이해

전형적인 정보시스템 통제감사 목적으로는 재무보고와 관련한 정보시스템 통제의 효과성 평가, 시스템 보안의 효과성 평가, 데이터의 신뢰성 평가 등을 예로 들 수 있다. 이러한 감사 목적이 확정되면 이에 필요한 적절한 감사범위를 설정해야 하는데 조직 전체를 감사대상으로 할 것인지 아니면 특정한 부서에 초점을 맞출 것인지 등의 감사의 폭(breadth)을 결정해야 하고, 어떤 종류의 정보시스템 통제를 평가할 것인지, 일반통제 또는 어플리케이션 통제 어느 수준을 평가할 것인지, 조직 전체의 정보시스템을 대상으로 할 것인지 아니면 그중에서 몇몇 시스템에 초점을 맞출 것인지 등을 결정해야 한다.

나. 수감기관의 운영과 주요 업무 현황 파악

감사인은 조직 운영에 영향을 미치는, 특히 IT의 중요한 외부 및 내부 요소를 확인해야 한다. 외부요소로는 IT예산, 외부 시스템 사용자, 현재의 정치적인 기류, 관련 법들이 이에 해당되며, 내부요소는 조직 규모, 지점이나 지사 수, 조직 구조(중앙집권형 또는 분산형), 운영의 복잡성, IT관리구조,

사업 운영에 대한 정보시스템의 영향, 주요 IT인력의 자격 및 역량, 주요 IT 인력의 이직률 등이 포함될 수 있다.

다. 수감기관의 일반적인 네트워크 구조 이해

감사인은 수감기관의 일반적인 네트워크 구조에 대한 이해가 있어야 한다. 예를 들어 방화벽, 불법침입 방지시스템, 메일 시스템 등 중요 시스템, 네트워크 관리시스템, 수감기관의 내·외부를 연결하는 네트워크 등의 정보를 입수하여 잠재적인 위험요소들을 파악해야 한다.

라. 주요 감사초점 영역 확인

주요 감사초점은 감사 목적을 달성하기 위하여 매우 중요한 것으로, 감사인은 각 주요 시스템 또는 파일의 위치, 하드웨어 및 소프트웨어의 주요 구성요소(예: 방화벽, 운영체제 등), 과거 감사에서 지적되었던 문제 등과 관련 있는 주요 시스템, 어플리케이션, 파일들을 확인해야 한다.

마. 기초적인 정보시스템 위험 진단

정보시스템 위험을 분석하기 위해서 다음의 3가지 측면에서 정보와 정보시스템 보안이 이루어져야 한다.

첫째가 무결성(integrity)으로 부적정한 정보 수정이나 파괴 등으로부터 정보시스템을 보호하는 것으로 정보의 부인방지[2](nonrepudiation)와 인증[3](authenticity)을 확보하는 것이다.

둘째는 기밀성(confidentiality)으로 개인정보 등을 보호하는 수단으로 정보

2) 부인방지의 일반적인 의미는 보낸 메시지에 첨부된 서명의 확실성을 부정할 수 없도록 보증하는 능력을 말한다. 인터넷상의 전자서명은 메시지나 문서가 당사자에 의해 전자적으로 서명되었다는 것을 보증하는 것은 물론, 후에 그 서명이 제시되었을 때 그가 부인할 수 없도록 보증하기 위해 사용된다.

3) 인증이란 어떤 사람이나 사물이 실제로 그 사람 또는 물건인지를 판단하는 과정이다. 개별 또는 인터넷을 포함한 공공 네트워크에서의 인증은 대개 로그온 시 암호의 사용을 통해 이루어진다.

접근과 정보노출 등에 대한 제한적 승인(authorized restriction)을 유지하는 것을 의미한다.

셋째는 가용성(availability)으로 시의적절하고 믿을 수 있는 정보의 접근과 이용을 확보하는 것이다.

따라서 무결성, 기밀성, 가용성의 손실은 곧 정보시스템의 위험을 말하며, 그러한 위험요소는 조직운영, 자산, 개인 구성원 등의 손실에 큰 영향을 끼칠 수 있다.

바. 중점관리요소(critical control points) 확인

감사인은 조직의 정보시스템 설계의 중점관리요소를 확인하고 증거를 첨부해야 한다. 중점관리요소에는 조직 네트워크에 접근할 수 있는 외부접근 포인트, 내·외부 시스템의 상호연결 포인트, 조직의 네트워크를 통한 정보 흐름을 통제하는 구성요소, 주요 저장 및 처리 장치 등이 해당된다.

사. 기초적인 정보시스템 통제 이해

감사인은 기본적으로 감사대상기관의 정보보안관리를 위한 조직구조, 인력, 권한, 자원 등의 정보시스템 통제의 설계에 대하여 전반적으로 이해를 하고 있어야 한다. 이를 위하여 정보보안관리, 접근통제, 직무분리(segregation of duties), 비상계획(contingency planning) 등의 관련된 조직 전반의 통제와 관련된 서류들을 확보해야 한다.

GAO의 FISCAM의 경우 감사계획단계에서 정보시스템의 위험은 무결성, 기밀성, 또는 가용성 등이 미흡하여 발생하는 위험을 말하며, GAO의 감사뿐만 아니라 연방정부 자체적으로 이를 3가지 위험단계(낮음, 보통, 높음)로 구분하여 평가하고 있다.

▸ **위험단계별 점검사항**

- **낮음:** 무결성, 기밀성, 또는 가용성 손실로 인하여 조직 운영, 자산, 또는 구성원에게 **제한적인 부정적인 효과(limited adverse effect)**를 끼칠 가능성이 있는가?
- **보통:** 무결성, 기밀성, 또는 가용성 손실로 인하여 조직 운영, 자산, 또는 구성원에게 **심각한 부정적인 효과(serious adverse effect)**를 끼칠 가능성이 있는가?
- **높음:** 무결성, 기밀성, 또는 가용성 손실로 인하여 조직 운영, 자산, 또는 구성원에게 **치명적 부정적인 효과(catastrophic adverse effect)**를 끼칠 가능성이 있는가?

2. 감사실시

이 단계에서는 감사 목적과 관련 있는 정보시스템 통제의 효과성을 테스트하는 것으로 일반통제(General Control)와 어플리케이션 통제(Application Control)로 구분한다. 일반통제는 기관의 전산업무처리에 전체적으로 적용되는 정책·절차·구조를 말하며, 다음과 같은 5개 영역으로 구분한다.

- 보안관리(security management): 위험관리, 보안정책 개발, 책임부여, 기관의 컴퓨터와 관련한 통제의 적절성 모니터링 등의 지속적인 활동과 프레임워크를 제공한다.
- 접근통제(access controls): 컴퓨터 하드웨어나 프로그램 등의 접근을 제한하거나 접근 시도를 알아냄으로써 승인되지 않은 프로그램 변경, 손실, 폭로 등으로부터 보호하는 통제수단을 제공한다.
- 구성관리(configuration management): 승인되지 않은 정보시스템 자원의 변경을 막고, 정보시스템이 원래 의도한 목적대로 안전하게 운영되고 있음을 보증하는 통제수단을 제공한다.
- 직무분리(segregation of duties): 어떤 한 개인이 전산 관련 업무의 핵심적인 부분을 혼자서 통제할 수 없도록 정책, 절차, 조직구조 등을 통하여 직원의 업무를 분리하여 통제하는 수단이다.

- 비상계획(contingency planning): 예기치 않은 상황이 발생하였을 때 기관의 중요한 업무 수행이 중단 없이 계속할 수 있게 하거나 즉시 복구가 가능하도록 조치하여 중요하고 민감한 정보를 보호할 수 있는 통제수단을 제공한다.

일반통제의 평가를 하는 경우 감사인들은 기법과 절차와 관련하여 NIST의 정보보안기준, ISO/IEC(International Organization for Standardization and the International Electrotechnical Commission)의 국제보안기준, ISACA의 감사기준 및 절차 등을 참조할 수 있다.

어플리케이션 통제는 개별적인 단위의 응용시스템(예: e-감사시스템, 회계관리시스템 등)과 관련하여 자료의 입력(input), 처리(process), 결과(output)에 대한 통제수단으로서 거래의 유효성, 승인의 적절성, 처리의 완결성과 정확성을 보장하기 위한 것이다. 어플리케이션 통제는 4개의 영역으로 구분하는데, 다음과 같다.

- 어플리케이션 보안(application security): 어플리케이션 통제에서 운영되는 보안관리, 접근통제, 구성관리 등과 같은 일반 통제요소로 구성된다.
- 업무절차 통제(business process control): 어플리케이션 처리 중에 거래와 데이터의 완결성, 정확성, 유효성, 기밀성과 관련한 통제수단을 제공한다.
- 인터페이스 통제(interface control): 어플리케이션 간의 정보처리의 적시성, 정확성, 완결성 및 하나의 운영환경에서 더 나은 운영환경으로 옮기는 과정(migration) 동안 완벽하고 정확한 데이터를 확보하도록 통제하는 수단을 제공한다.
- 데이터관리시스템 통제(data management system control): 정보를 저장하고, 검색하고, 처리하는 데이터베이스 시스템의 특징을 활용하는 통제수단을 제공한다.

3. 감사보고

감사인은 정보시스템 통제 테스트 과정이 끝난 후 감사위험과 관련 있는 정보시스템 통제의 취약점에 대한 개별 또는 통합결과를 평가한다. 감사인은 달성하지 못한 통제활동의 결과에 대하여 평가해야 한다. 다시 말하면, 일반통제의 5가지 영역 또는 어플리케이션 통제의 4가지 영역의 효과성을 방해하는 취약한 부분이 있는지 여부를 파악하는 것이다. 각 요소 중에 어느 하나 또는 그 이상이 비효과적이라면 전체 영역에 대한 통제가 효과적이 아니라고 결론지을 수 있다. 감사인은 이러한 취약점이 감사초점의 주요 부분을 지원하는 시스템 또는 파일에 승인 없이 접근이 가능하도록 만드는지 평가해야 한다.

제2절 ISACA의 정보시스템 감사기준, 지침 및 절차

ISACA의 '정보시스템 감사기준, 지침 및 절차(Information Systems Standards, Guidelines and Procedures)'의 목적은 정보시스템 감사인(IS Auditors)이 전문가로서 전문적인 윤리강령이 요구하는 최소한의 조건을 만족시키기 위한 것이고, 또 하나는 감사업무와 관련하여 경영층과 기타 이해관계자들에게 결과에 대한 기대치를 제시하기 위한 것이다. ISACA의 '감사기준(audit standards)'에는 정보시스템 감사 및 보고에서 반드시 해야 할 의무사항이 무엇인지 정의하고 있으며, '지침(guidelines)'은 이러한 감사기준을 반영할 수 있도록 안내하는 역할을 하는 것으로 정보시스템 감사인은 어떻게 기준들을 반영하여 구현할 것인가와 전문적인 판단방법을 제시해준다. '절차(procedures)'는 정보시스템 감사인이 감사를 수행하는 데 따라야 할 절차의 예를 보여줌으로써 감사가 완료되었을 때 기준과 어떻게 부합되는지에 대한 정보를 제공해준다.

1. 감사계획

ISACA의 감사기준에 따르면 정보시스템 감사인은 감사목표와 적용 가능한 법과 감사기준에 따라 정보시스템 감사적용범위를 수립해야 하고, 위험기반의 감사접근방법을 설정해야 하며, 감사기간, 감사의 성격, 필요한 자원 등을 개발하여 문서화해야 한다. 이는 일반적인 감사계획과 유사한 부분이나 위험기반의 감사접근방법을 제시하고 있다는 점에서 차이가 있다. 감사계획은 크게 5개 사항에 초점을 맞추어야 한다고 지침을 주고 있다.

가. 사업 요구사항(Business Requirements)

감사영역과 관련하여 수감기관의 목표와 기술적인 구조를 고려해야 하며, '정보시스템 전략계획(Information Systems Strategic Plan)'에 대한 정보를

입수해야 한다. 또한 수감기관의 정보구조(information architecture)와 현재 및 향후 기술방향(technical direction)에 대한 이해도 필요하다. 위험평가(risk assessment)와 확인된 위험의 우선사항(prioritization)에 따라 수감기관의 정보시스템 환경이 어떻게 대응할 수 있는지 검토해야 한다.

나. 조직에 대한 지식(Knowledge of the Organization)

수감기관의 일반적인 조직형태와 업무절차에 대한 지식이 필요하다. 이러한 지식을 기반으로 감사내용의 깊이가 결정될 수 있기 때문이다. 또한 조직운영과 이에 따른 정보시스템의 요구사항에 대한 이해도 필요하다.

다. 감사의 중요성 평가(Assessing Materiality)[4]

정보시스템 감사인은 정보의 기밀성, 가용성, 무결성에 의한 정보자산 분류, 권한 관리(privilege management)에 대한 접근통제(access control) 규정, 그리고 임계성(criticality) 및 노출위험 수준을 토대로 한 정보분류의 역할과 책임성 등을 규정해야 한다. 평가는 저장된 정보, 하드웨어, 정보시스템 구조 및 소프트웨어, 네트워크, 정보시스템 운영, 개발 및 테스트 환경의 검증이 포함되어야 한다.

▸ **감사의 중요성을 평가하는 데 고려되어야 할 평가의 예**
- 시스템 운영에 의하여 지원되는 업무 프로세스의 임계성
- 시스템 운영에 의하여 지원되는 데이터베이스의 임계성
- 시스템 운영에 의하여 지원되는 네트워크 통신의 임계성
- 개발된 어플리케이션의 수와 종류
- 정보시스템을 사용하는 이용자 수
- 시스템 비용
- 대응책의 효과성 등

4) 감사에서 중요성은 감사위험이 감사결과에 미칠 영향력의 크기와 민감도를 말한다. 즉, 감사인이 감사업무를 실시하는 과정에서 수감기관 등의 직무상 불법행위·오류 또는 낭비 등을 발견하지 못할 위험이 감사결과에 끼칠 영향력의 크기를 말한다. 이러한 중요성의 원칙은 사전에 설정하고 이를 감사계획에 반영하여야 하며 중요성의 기준에 대한 판단은 감사인의 전문적인 영역에 속하며 감사목적과 감사결과 이용자의 수요에 따라 달라질 수 있다.

라. 위험평가(Risk Assessment)

위험평가는 감사업무 동안 모든 중요한 항목(material items)들이 적절히 포함될 수 있도록 합리적인 보증(reasonable assurance)을 제공해야 한다. 따라서 이러한 위험평가를 통해서 상대적으로 위험도가 높은 항목들이 어떤 것인가 확인하여야 한다.

먼저 위험평가를 하기 위해서는 적절한 위험평가방법론을 선택하여 전체적인 감사계획과 특정감사에 대한 계획을 수립하여야 한다. 이러한 계획은 감사절차의 기간 및 성격, 업무기능 영역, 감사에 투여되는 시간과 자원 등의 내용이 고려되어야 한다. 감사인은 전체적인 위험수준을 결정하기 위하여 위험의 유형을 '고유위험(inherent risk)', '통제위험(control risk)', '적발위험(detection risk)' 등 3가지로 구분하여야 한다.

고유위험은 내부통제(internal control)와는 관련 없이 발생할 수 있는 위험요소로, 예를 들어 보안과 관련되어 컴퓨터 운영체제(operating system)의 경우 일반적으로 고유위험이 높다. 왜냐하면 운영체제를 통한 데이터 또는 프로그램들이 변경될 경우 조직 전체의 파급효과가 크기 때문이다. 반면 네트워크가 연결이 안 된 개인용 컴퓨터(stand-alone PC)는 보안문제에 있어서 일반적인 고유위험은 낮다.

고유위험 증가에 영향을 줄 수 있는 요소
- 많은 사용자 수
- 기술의 급격한 변화
- 외부요인 또는 외부기관에 대한 지나친 의존
- 정보시스템 관리 경험과 지식 부족
- 대규모 프로젝트 과다
- 시스템의 복잡성
- 통합시스템의 부족

통제위험은 조직의 내부통제시스템이 적정한 시기에 중요한 오류를 방지하거나 발견하지 못할 위험요소로, 예를 들면 컴퓨터 로그파일 검토와 관련

된 통제위험은 높다고 볼 수 있다. 왜냐하면 로그파일 자체가 양이 많다 보니 쉽게 검토하지 않고 넘어가는 경우가 흔하기 때문이다. 반면 컴퓨터화된 데이터 유효성(data validation) 검사는 절차가 일관성 있게 적용되기 때문에 통제위험도가 낮다.

적발위험은 실제적인 감사절차를 통해서도 중요한 오류를 발견해내지 못할 위험을 말한다. 예를 들어 시스템 보안 침입 흔적을 발견하려 할 경우 적발위험은 높다고 볼 수 있는데, 그 이유는 감사 전 기간 동안의 로그파일들을 모두 감사 당시에 입수할 수 없기 때문이다. 반면 재난복구계획이 미흡하다는 것을 알아낸 경우 계획의 존재 여부를 파악하는 것은 쉽기 때문에 적발위험은 낮다고 볼 수 있다.

마. 내부통제 평가(Internal Control Evaluation)

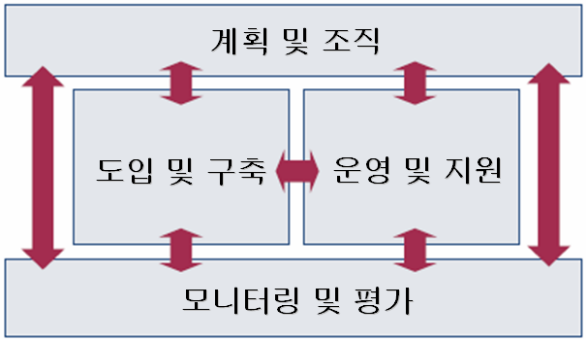
감사에는 직접적으로 감사목표의 일부로 또는 감사의 한 부분으로 수집되는 정보가 신뢰성이 있는가를 내부통제의 요소로 포함하는 것을 고려해야 한다. 일정 기간 동안의 통제의 효과성을 평가하는 것이 감사의 목표라면 감사계획은 감사목표에 맞는 절차가 포함되어야 하며, 이러한 절차에는 통제의 준수성 시험(compliance testing)이 포함되어야 한다.

2. 감사실시

감사실시와 관련된 지침은 'COBIT(Control Objectives for Information and related Technology)'에 잘 나타나 있는데 COBIT은 조직의 IT통제를 위한 정책 및 모범사례 개발을 가능하게 해주는 감사의 통제모델로서 경영층, IT 관리자 및 정보시스템 감사인이 이용할 수 있도록 만들어진 것이다. COBIT의 목표는 ① 사업 요구사항과의 연계, ② 성과의 투명성 확보, ③ 활용할 주요 자원의 확인, ④ 관리통제 목적 정의 등에 있다. COBIT은 4개의 영역과 34개의 프로세스로 구분하는데, 이러한 4개 영역의 활동을 통하여 IT거

버넌스 체계를 구축하여 조직의 전략적인 목적을 달성하는 것이 최종 목적이다.

〈그림 2-1〉 COBIT의 4개 영역



▸ **COBIT의 4개 영역**
- 계획 및 조직(Plan and Organize): 솔루션 및 서비스 방향 설정 단계
- 도입 및 구축(Acquire and Implement): 솔루션을 서비스화하는 단계
- 운영 및 지원(Deliver and Support): 솔루션을 최종사용자에게 제공하는 단계
- 모니터링 및 평가(Monitor and Evaluate): 계획된 방향대로 모든 절차를 밟았는지 점검하는 단계

〈표 2-1〉 COBIT의 영역별 프로세스

영역		프로세스
계획 및 조직	PO1	IT전략계획 정의
	PO2	정보구조 정의
	PO3	기술 방향 결정
	PO4	IT프로세스, 조직, 관계 정의
	PO5	IT투자 관리
	PO6	경영층의 관리목표 및 방향 전파
	PO7	IT인력 관리
	PO8	품질 관리
	PO9	IT위험평가 및 관리
	PO10	프로젝트 관리

영역		프로세스
도입 및 구축	AI1	자동화된 솔루션 도출
	AI2	응용 소프트웨어 도입 및 유지·보수
	AI3	기술구조 도입 및 유지·보수
	AI4	운영 및 이용 준비
	AI5	IT자원 조달
	AI6	변경 관리
	AI7	시스템 설치 및 테스트
운영 및 지원	DS1	서비스 수준 정의 및 관리
	DS2	외부업체 서비스 관리
	DS3	성능 및 용량 관리
	DS4	서비스의 지속성 확보
	DS5	시스템 보안성 확보
	DS6	비용 산정 및 배분
	DS7	사용자 교육 및 훈련
	DS8	고객지원 및 사고 관리
	DS9	구성 관리
	DS10	문제 관리
	DS11	데이터 관리
	DS12	시설 관리
	DS13	운영 관리
모니터링 및 평가	ME1	IT성과 모니터링 및 평가
	ME2	내부통제 모니터링 및 평가
	ME3	외부 요구사항과의 적합성 보증
	ME4	IT거버넌스[5] 제공

5) IT거버넌스는 IT가 조직의 전략과 목표를 유지하고 확장할 수 있게 하는 리더십, 조직구조, 프로세스(기획·구축·운영·관리)로 구성되며, IT조직의 가시성을 확보하고 의사결정에 이를 반영할 수 있는 내부조직체계 및 프로세스를 확보하는 것이다(정보통신산업진흥원, 2006).

COBIT의 초점은 IT를 적절하게 관리하고 통제하는 것이 목적이며 COBIT은 서로 다른 지침서를 통합하여 하나의 프레임워크에 주요 조직목표를 설정하는 역할을 수행한다.

IT통제에는 '일반통제(General Controls)'와 '어플리케이션 통제(Application Controls)'로 구분하는데, 일반통제는 데이터센터 운영, 시스템 소프트웨어 구매 및 유지·보수, 접근보호 및 시스템 개발/보수 등 조직 전반의 IT시스템 기능과 관련한 내용이 포함된다. 여기서 검토되는 주요 내용은 IT정책, IT보안기준 및 가이드라인, 어플리케이션 개발 및 변경 통제, 직무분리, 사업연속성 계획, IT프로젝트 관리 등이다. 따라서 일반통제의 검토사항은 개별 프로그램에 대한 것이 아니라 수감기관의 IT부서 또는 해당 기능에 초점을 맞추는 것이 특징이다. 반면, 어플리케이션 통제는 특정한 컴퓨터 어플리케이션에 관한 것으로 개별적인 처리업무(transaction)와 밀접한 관련이 있다. 일반적으로 입력(input), 처리(processing), 결과(output), 데이터와 마스터 파일에 대한 통제 등 어플리케이션 내의 기능이 포함된다.

3. 감사보고

감사보고서는 주제(subject matter) 또는 감사활동범위(area of activity)와 관련한 자세한 정보를 포함하여야 하는데, 내부통제의 설계 또는 운영과 관련된 내용 및 기준 또는 법이나 규정 준수 여부 등이 이에 해당되고, IT감사인이 직접 특정 주제에 대한 의견을 보고하는 것과 통제절차의 효과성에 대한 임원의 주장(management's assertion)에 대한 의견을 보고하는 내용 등이 포함된다. IT감사인이 특정 주제에 대하여 평가하는 기준은 어떠한 편견도 포함되지 않고 객관적(objective)이어야 하며, 일관성 있는 평가(measurable)를 해야 하며, 결론에 도달하는 데 관련된 모든 요소가 포함되도록 완결성(complete)을 높여야 하며, 주제와 관련성(relevant)이 있어야 한다.

IT감사인의 의견은 적절한 증거(evidence)를 수집하는 데 필요한 절차의

하나로 시행하는데 IT감사인의 의견은 확정적인(conclusive) 증거로 여기기보다는 설득력(persuasive) 있는 증거로 작용한다. 이는 내부통제의 효과성에 대한 보증(assurance)이 내부통제의 성격과 내부통제 운영에 대한 고유의 제한성(inherent limitations)으로 인하여 한정적일 수밖에 없기 때문이다. 예를 들어 임원들은 내부통제 개선에 필요한 소요비용이 예상되는 기대효과를 초과하지 않는 범위 안에서 이루어지도록 요구되기 때문에 제한적인 개선효과만을 기대할 수 있다.

▸ **ISACA의 '정보시스템 감사기준, 지침 및 절차'에 따른 IT감사보고서 주요 내용**
- 감사목적 및 활동 부문 설명
- 결론을 위해 이용하였던 감사기준 및 방법론에 대한 설명
- ISACA 정보시스템 감사기준 또는 다른 전문적인 감사기준에 맞추어 감사를 실시하였다는 내용 포함
- IT감사인의 내부통제의 효과성에 대한 입증검사(attest engagement)에 대한 의견 포함
- 감사부문과 관련한 내부통제 설계 및 운영이 효과적인지에 대한 종합적인 의견 제시

제3절 INTOSAI의 IT감사지침

IT감사를 하기 위해서 감사인은 전문적인 IT감사기준에서 정의하고 있는 요구사항을 잘 이해하고 있어야 한다. 또한 IT감사를 수행하는 데 영향을 끼치는 관련 법규 등에도 지식이 있어야 한다. 예를 들어 국가, 주, 지방의 법과 규정 등은 IT감사를 계획하고 수행하는 데 고려해야 할 사항이다. 컴퓨터와 관련한 통제의 이슈 범위를 결정하는 경우, 데이터의 기밀성·무결성·유효성·신뢰성을 고려해야 한다. 그리고 최고감사기구에서 수행하는 IT감사는 ISACA 등의 국제기준이나 그에 상응하는 국가의 IT감사표준을 따라야 한다.

1. 감사계획

이 단계에서 감사인은 기관의 구조 및 운영에 대한 이해와 지식을 보유하고 있어야 한다. 또한 기관의 컴퓨터와 관련된 운영, 통제, 잠재적인 IT위험요소 등에 대하여 알고 있어야 한다. 이러한 전반적인 기관의 IT환경에 대한 이해를 바탕으로 '예비위험평가(preliminary risk assessment)'를 실시하고 그 결과에 따라서 감사계획을 어떻게 세울 것인가를 결정한다. 예를 들어 보안위험(security risk)은 데이터처리의 유효성을 확인하기 위한 통제 기능이 미흡해서 발생하는 위험으로, 데이터 접근성, 시스템 사용 권한의 분리 여부, 사업 연속성 보장 등을 점검하며, 프로젝트 위험(project risk)은 프로젝트의 비용/편익과 관련한 위험으로 프로젝트 지연, 비용 초과, 프로젝트 성과의 기대효과 미흡 여부 등을 점검해야 한다.

2. 감사실시

정보시스템의 통제는 조직의 목표 달성을 위해 필요한 정책, 절차, 업무, 조직구조 등을 반영하는 것으로, 운영의 효과성과 효율성, 재무보고의 신뢰

성, 법과 규정의 순응 등을 향상시키는 역할을 한다. 따라서 이 단계에서 감사인은 IT통제정책, 절차, 목적, 통제활동 성과와 관련한 상세한 정보를 입수한다. 이렇게 하는 목적은 통제가 효과적으로 잘 운영되고 있는지를 파악하기 위한 것이다.

가. 재무감사의 한 부분으로서의 IT감사

IT감사가 재무감사의 한 부분으로 수행될 경우, 위험기반의 감사접근방법을 선택해야 한다. 즉, 다음과 같은 잠재적인 위험요소를 고려하여 IT감사를 실시하여야 한다.

- 상업용 어플리케이션을 사용하지 않고 감사대상기관 자체적으로 어플리케이션을 개발하여 운영하고 있다.
- 감사대상기관이 속해 있는 산업군이나 내부 환경에 따라 이러한 요소들이 IT통제의 개발과 적용에 영향을 줄 수 있다. 예를 들어 타 기관과의 경쟁에서 이기기 위한 압력 때문에 새로운 어플리케이션을 도입하게 되면, 이것이 적절하게 통제되지 않거나 상세조건에 맞추어 작동되지 않을 수 있다.
- 사용자가 특정한 기능이나 데이터의 접근 권한을 보유하고 있거나 보유할 가능성이 있는 경우가 있다.
- 사용자가 데이터와 보고서를 변경할 수 있는 권한이 있다.
- 최종사용자컴퓨팅(end-user computing) 환경에서 생산되는 재무정보는 조작 가능성이 높다.
- 사용자는 시간, 경험 또는 지식의 부족 등으로 처리 후 결과에 대해 효과적인 모니터링이 어렵다.

나. 성과감사의 한부분으로서의 IT감사

성과감사에서 IT감사는 둘 중 하나의 역할을 수행할 수 있는데, 첫 번째는

IT 자체가 성과감사의 주요 초점이 되는 경우이다. 이런 경우 감사의 목적은 조직의 IT시스템과 IT시스템을 통한 조직의 성과가 어느 정도인지를 파악하는 것이다. 두 번째는 IT가 업무절차나 사업의 효율성과 효과성에 초점을 맞춘 성과감사를 지원하는 것으로 업무절차와 사업 등에 대한 IT의 영향을 평가하게 된다.

다. 정보시스템 개발감사(information systems development audit)

정보시스템 개발감사는 초기 구상이나 제안에서부터 시스템 구현까지의 전 과정이 감사 범위에 포함된다. 정보시스템 개발감사는 다시 두 부분으로 나누어지는데 하나는 시스템 개발단계에 적극적으로 참여하는 감사로 '진행감사(Ongoing Project Audit)'라고 한다. 진행감사는 시스템 개발과정에서 위험평가 및 과정 동안의 산출물을 검토하게 된다. 이러한 감사형태는 시스템 구현단계 전에 잘못된 내용을 미리 개선하거나 원래의 기대 효과를 충족하기 어려워 더 이상의 개발로 인한 손실을 막는 기능을 수행할 수 있다. 다른 하나는 '구현 후 감사(Post Implementation Audit)'로 시스템 구현이 완료된 후 특정한 시스템을 평가하는 것을 말한다. 이 평가에는 전체적인 프로젝트 관리, 자금, 승인절차, 개발과정 동안 중앙부처의 모니터링 역할 등이 포함된다. 구현 후 감사는 또한 시스템의 효과성 및 효율성을 평가하는 데까지 확장할 수 있다.

라. 구매감사(acquisition audit)

구매감사는 감사대상기관의 컴퓨터 관련 장비 구매 결정에 대하여 행정적인 절차와 통제가 적절하였는지를 검토해야 한다. 이러한 목적을 달성하기 위해서 컴퓨터 관련 장비에 대한 요구사항을 적절히 분석할 수 있는 구조가 되어 있는지, 실용적인 정보화정책 및 전략을 지원하는 구매절차가 성립되어 있는지, 평가와 선택의 절차가 조직의 요구사항에 효과적이고 효율적인 방법으로 도움을 주는지를 확인하여야 한다.

마. 운영 및 유지·보수 감사(operation and maintenance audit)

'운영 및 유지·보수 감사(이하 운영감사)'는 일반통제 측면과 어플리케이션 통제 측면으로 구분할 수 있다.

일반통제 측면에서 운영감사는 '직무분리(segregation of duties)', '물리적 접근 통제(physical access control)', '논리적 접근 통제(logical access control)', '운영 및 파일 통제(operation and file control)', '변경관리 통제(change management control)', '네트워크 보안 통제(network communication security control)', '업무지속계획(business continuity planning)' 등을 통하여 안전하고 효과적인 컴퓨터 운영이 될 수 있도록 하는 데 목적이 있다.

- '직무분리'는 컴퓨터 에러나 부정 사용을 근본적으로 줄일 수 있기 때문에 이에 대한 조사가 필요하다. 직무설명서, 조직도, IT인력의 업무 등을 통하여 직무가 적절히 분리되어 있는지 확인할 수 있다. 특히 주요 IT시스템의 경우 IT직무는 시스템 설계 및 프로그래밍, 시스템 지원, 일상적인 IT운영과 관리, 시스템 보안, 데이터베이스 관리 등에 대한 업무가 각각 적절히 분리되어 있어야 한다.
- '물리적 통제'는 전체 IT환경 및 모든 프로그램에까지 적용되는 환경통제로 하드웨어 및 소프트웨어로부터 피해, 도난, 비인가된 접근으로부터 IT자원을 보호하는 데 목적이 있다.
- '논리적 접근 통제'는 일단 컴퓨터에 물리적으로 접근하였다 하더라도 권한이 없는 비인가자(unauthorized person)가 시스템이나 파일 또는 프로그램에 접근하지 못하도록 하거나, 권한이 있는 인가자(authorized person)라 하더라도 그 사람에게 인가된 활동만을 허용하도록 하는 통제를 말한다.
- '운영 및 파일 통제'는 컴퓨터나 컴퓨터 파일을 손실이나 도용 등으로부터 안전하게 보호하는 역할을 수행하는 것으로, 정해진 스케줄에 따라 정기적으로 파일을 구동하는 작업이 이루어지는지, 접근 권한이 있는

인력의 수와 등급에 제한을 두고 있는지 여부를 파악해야 한다.

- '변경관리 통제'는 IT시스템이 접근 권한, 테스트, 승인, 문서화 등의 적절한 통제가 이루어지고 있는지를 파악하는 것으로, 이러한 통제가 적절히 구현되지 않는 경우 소프트웨어와 데이터의 우연이든 악의적이든 데이터의 변경이 이루어질 수 있다.
- '네트워크 보안 통제'는 모든 네트워크상의 민감한 정보들이 적절한 기술에 의하여 보호받고 있는지, 네트워크 장비가 물리적인 피해를 입지 않도록 되어 있는지, 네트워크 구성과 관련된 정보는 문서화가 잘 되어 있는지, 네트워크 진단장비는 보유하고 있는지 등을 점검해야 한다.
- '업무지속계획'은 컴퓨터가 제대로 작동되지 않더라도 업무를 지속적으로 수행할 수 있는 적절한 계획이 있는지 확인해야 한다. 업무지속계획의 정도(degree)는 IT부서의 크기와 컴퓨터 처리에 대한 의존도에 따라 달라질 수 있다. 중요한 시스템의 심각한 IT능력 손실은 재무제표 정보가 잘못 처리될 수 있는 위험을 초래할 수 있다. 따라서 IT장비에 대한 재해복구계획(disaster recovery planning)이 조직의 전반적인 업무지속계획의 하나로 취급되어야 한다. 그러므로 정기적인 테스트와 백업이 일, 주, 월, 분기 단위로 어떻게 이루어지고 있는지 파악해야 한다.

어플리케이션 통제 측면에서는 단위별 어플리케이션이면서 하나의 어플리케이션이 개별적인 트랜잭션 처리에 직접적인 영향을 주는지를 파악하는 데 중점을 두는 것으로 모든 트랜잭션이 유효하고, 승인받은 것인지, 기록되어 있는지를 점검해야 한다. 어플리케이션 통제의 조건들은 '문서기준(documentation standards)', '입력 통제(input control)', '처리 통제(processing control)', '출력 통제(output control)', '마스터 및 대기 데이터 파일 통제(master/standing data file control)' 등으로 구분한다.

- ‘문서기준’은 시스템 관련 문서가 충분히 이해할 수 있도록 써져야 하며, 최근의 시스템 변경사항이 반영되어야 하고, 백업용 복사본을 보유하고 있는지를 점검해야 한다. 따라서 문서내용에는 시스템 개요, 사용자 요구사항, 프로그램 설명 및 리스트, 입력 및 출력 설명, 파일 내용 설명, 사용자 매뉴얼 등이 포함되어야 한다.
- ‘입력통제’는 모든 주요한 입력 행위가 적절하게 승인된 것인지, 데이터의 입력이 적절히 통제되고 제한을 두는지, 원본 문서의 복사를 차단하고 찾아내는 방법이 있는지 등을 평가한다.
- ‘처리통제’는 입력 데이터가 유효한 것인지, 정확한 파일을 처리하고 있는지, 처리하는 동안 에러를 발견해서 다시 원래 데이터를 송부한 사람에게 재처리를 요구할 수 있는 절차가 있는지, 하나의 처리단계에서 다른 단계로의 이동이 적절한지 등을 점검한다.
- ‘출력통제’는 모든 출력 결과물이 적시에 생산되고 배부되는지, 에러와 예외사항을 적절히 파악하고 대응할 수 있는지 여부를 점검한다.
- ‘마스터 및 대기 데이터 파일 통제’는 마스터 파일과 대기 파일의 정확성이 가장 중요한 것으로 대기 데이터의 변경이 적절하게 통제되는지, 입력된 데이터가 변경 또는 파괴되지 않은 상태로 유지되고 검증할 수 있는 방법이 있는지, 데이터 파일에 대한 물리적 및 논리적 접근이 제한되고 통제되는지를 점검한다.

3. 감사보고

이 단계에서는 일반적인 감사보고서 체계와 동일하며, 감사목적, 감사범위, 감사방법론, 감사결과, 결론 및 제안사항 등을 보고서 안에 포함한다.

제4절 IIA의 글로벌 기술 감사지침

미국의 내부감사협회(The Institute of Internal Auditors)의 '글로벌 기술 감사지침(Global Technology Audit Guide, GTAG)'은 감사 관련 업무의 최고 책임자(Chief Audit Executive), 감사위원회, 감사책임자(Audit Supervisors)에게 정보기술 관리, 통제, 보안에 관련한 새로운 IT현안들을 알려주기 위해 작성한 것이다. 지금까지 총 12개의 IT통제와 관련된 지침을 개발하였으나 이 중에서 IT감사기준과 관련된 내용은 포함되어 있지 않은 것으로 파악되었다. 내부감사협회는 1978년 '내부감사기준(The Standards for the Professional Practice of Internal Auditing)'을 제시한 바 있으나 이 감사기준에도 IT감사와 관련된 구체적인 내용은 언급되어 있지 않다. 다만 GTAG의 감사기준에 대한 의견은 감사 관련 업무의 최고책임자들이 IT감사의 수행을 지원하는 데 감사기준의 활용을 추천하며, 그 감사기준에서 현재 나와 있는 여러 감사기준 중 자기 조직과 IT관리에 가장 적합하다고 생각하는 것을 선택하는 것이 중요하다고 주장하고 있다. 업무절차와 업무활동의 내부통제가 점점 더 IT를 기반으로 하고, IT통제가 내부통제의 핵심적인 기능이 되어가고 있기 때문에 내부감사협회의 IT통제와 관련 있는 지침들은 충분히 참고할 만한 가치가 있다고 판단하였다. 따라서 'IT통제(IT Controls)', 'IT감사의 관리(Management of IT Auditing)', 'IT감사계획 개발(Developing the IT Audit Plan)' 등 3개의 지침을 참고로 감사계획, 감사실시, 감사보고의 내용들을 정리하였다.

1. 감사계획

여러 '외부 품질평가(external quality assessment reviews)'에서 드러난 결과는 내부감사활동 중에 가장 취약한 부분이 적절하게 IT감사계획을 수립하지 못한다는 것이다. 대부분의 내부감사는 자신들이 아는 내용을 검토하거나 외부용역을 주고 그들로 하여금 무엇을 감사할 것인지를 결정하게 하고

있는 실정이다.

이러한 문제점을 해결하기 위해 감사계획을 수립할 때는 첫째, 사업을 이해해야 한다. 이를 위하여 기본적으로 조직의 목표, 전략, 사업모델 등을 이해하는 것이 조직의 위험요소들을 파악하는 데 도움을 준다. 또한 어떻게 현재 사업운영과 IT 서비스 기능이 조직을 지원하는지 반드시 이해하여야 한다.

다음으로, 'IT범위(IT universe)'를 정의하는 것이 필요하다. 이는 주요 사업목표 및 절차, 사업절차를 지원하는 주요 어플리케이션 및 인프라, 네트워크 장비 같은 일반적으로 지원하는 기술적인 요소의 역할 등을 '하향식 접근방식(top-down approach)'을 통하여 달성할 수 있다. 그리고 IT범위가 정해진 후 IT위험 발생가능성 및 영향을 평가하기 위하여 등급을 정하고, 이를 점수화하는 'IT위험 등급 모델(IT risk-ranking model)'을 활용한다. 각 위험 발생 가능성(likelihood)을 3단계(낮음, 중간, 높음)로 구분하여 점수별로 평가하고 있으며, 위험영향(impact)에 대한 평가도 위험발생 가능성과 마찬가지로 3단계로 평가하고 있다. 위험항목들은 재정적인 영향(financial impact), 내부통제의 질(quality of internal controls), 감사팀의 변화(changes in the audit unit), 가용성(availability), 무결성(integrity), 기밀성(confidentiality) 등 6개 분야로 구분하고, 위험발생 가능성 및 위험영향 등을 3단계로 점수화하여 평가하고 있다.

▸ **위험발생 가능성(likelihood) 척도:** 위험발생 가능성을 3단계로 구분하여 점수별로 평가

발생 가능성 척도		
높음	3	위험발생 확률이 높음
중간	2	위험발생 확률이 보통
낮음	1	위험발생 확률이 낮음

▸ **위험영향(impact) 척도:** 위험에 대한 영향을 3단계로 구분하여 점수별로 평가

위험영향 척도		
높음	3	위험이 조직과 이해관계자에게 미칠 잠재적인 영향이 높음
중간	2	위험이 감사팀에게는 중요할 수 있으나 전체 조직에게 미칠 잠재적인 영향은 보통
낮음	1	위험이 전체 조직에게 미칠 잠재적인 영향이 매우 미미하거나 범위가 제한적임

▸ **점수범위 및 감사/모니터링 빈도:** 재정적인 영향(financial impact), 내부통제의 질(quality of internal controls), 감사팀의 변화(changes in the audit unit), 가용성(availability), 무결성(integrity), 기밀성(confidentiality) 등 6개 분야로 구분하고, 점수를 종합. 점수범위에 따라 감사 또는 모니터링 순기가 달라짐

등급	종합 점수범위	감사순기
높음	35-54	1~2년마다
중간	20-34	2~3년마다
낮음	6-19	3~5년마다

다시 정리하면 효과적인 IT감사계획 수립을 위해서는 아래 4가지 단계의 절차를 밟는 것을 권장하고 있다.

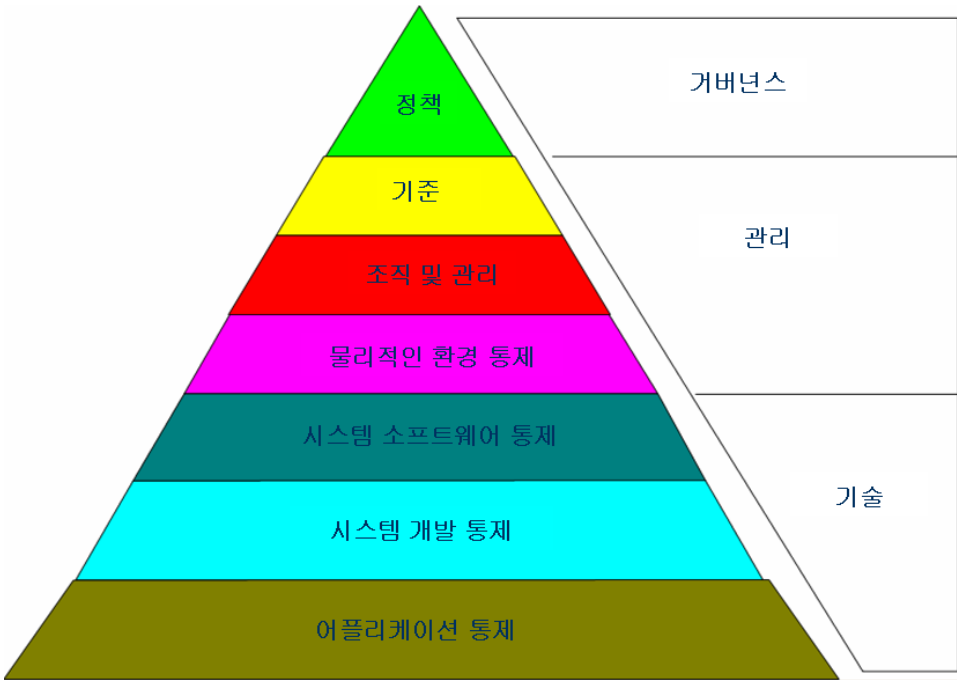
〈표 2-2〉 IT감사계획 수립을 위한 4단계

업무/사업의 이해 ➡	IT범위 설정 ➡	위험평가 실시 ➡	감사계획 수립 ➡
●조직의 전략과 목표 확인 ●조직의 높은 위험수준 이해 ●조직의 업무/사업 운영을 위한 조직구조 이해 ●IT서비스 모델 이해	●근본적인 사업들을 상세히 분석 ●업무/사업운영을 지원하는 중요한 어플리케이션 확인 ●중요 어플리케이션을 위한 인프라 확인 ●기술지원 역할 이해 ●주요 프로젝트 및 계획 확인 ●현실적인 감사과제 결정	●위험발견을 위한 절차 수립 ●위험평가 및 IT위험요인을 이용한 감사과제 우선순위 매김 ●위험평가 및 사업/업무 위험요인을 이용한 과제 우선순위 매김	●감사과제 선정 및 서로 다른 감사업무 통합 ●감사기간 결정 ●경영층의 요구 또는 컨설팅을 위한 기회에 근거하여 적절한 감사업무 추가 ●담당 임원과의 계획 확인 작업

2. 감사실시

내부감사협회에서 제안한 IT통제는 전체 IT운영환경을 거버넌스, 관리, 기술의 3가지 영역으로 구분하고 이를 7개의 세부 통제항목으로 나누고 있다.

〈그림 2-2〉 IT통제구조



가. 정책(Policies)

모든 조직은 전략계획을 통하여 목표와 목적을 정의할 필요가 있다. 명확한 전략과 정책목표가 없는 계획은 추진 방향성을 잃게 되고 성과 면에서도 비효율적이다. 대부분의 조직에서 IT는 필수요소이기 때문에 IT의 모든 측면에 대한 명확한 메시지를 전달해야 한다. 따라서 IT와 관련한 전략계획이 수립되어 있는지, IT개발과 조직의 전략과 어떤 연결고리가 있는지 파악하는 것이 중요하다.

나. 기준(Standards)

전체 IT환경을 보다 효과적으로 유지하기 위해서는, 특히 다음과 같은 부분에 해당 기준이 있어 적용할 수 있어야 한다.

- 시스템 개발 절차(system development process): 조직 내에서 자체적으로 어플리케이션을 개발할 때 시스템 및 프로그램의 설계, 개발, 테스트, 구현 등 일련의 절차에 대해 적용 가능한 기준을 마련해야 한다.
- 시스템 소프트웨어 구성(system software configuration): 운영체제(operating system), 네트워크 소프트웨어, 데이터베이스 관리시스템 등이 구현되면, 구현방법에 따라 보안이 향상되거나 아니면 약점을 노출시킬 수 있다. 이러한 경우를 대비하여 적용기준이 필요하다.
- 또한 어플리케이션 통제(application controls), 데이터 구조(data structures), 문서화(documentation)에도 일정한 기준이 있는지 확인할 필요가 있다.

다. 조직 및 관리(organization and management)

조직 및 관리는 IT통제시스템에서 조직운영에 중요한 역할을 수행한다. 적절한 조직구조는 보고라인 및 책임성 체계를 확립하고 효과적인 통제시스템을 구현할 수 있다.

- 직무 분리(segregation of duties): 조직에서는 한 개인 또는 하나의 부서가 전체 데이터 처리에 대한 책임을 부여해서는 안 된다. 데이터의 권한, 입력, 체크 업무가 각각 분리되어 있어야 위험요소를 줄일 수 있기 때문이다.
- 재무 통제(financial controls): 조직은 IT에 대하여 막대한 양을 투자하기 때문에 예산과 재무 관련 통제는 매우 중요하다. 불충분한 계획으로 인하여 새로운 IT개발이 종종 예산범위를 훨씬 벗어나 원래 기대하였던 비용절감효과 없이 실패하는 경우가 발생한다. 예산 통제가 이러

한 잠재적인 문제점을 이른 시점에서 발견할 수 있게 하여 적절한 대처를 할 수 있도록 도와준다.

- 변경 관리(change management): 변경 관리절차는 시스템 소프트웨어, 어플리케이션 시스템, 데이터 등이 변경되었는지를 확인하게 해준다. 이를 통하여 부정한 목적으로 시스템을 변경하려는 의도를 차단시킬 수 있고, 비효과적인 모니터링과 보고절차에 의해 감추어진 비효율성 및 시스템 정전의 비용을 확인할 수 있다.

라. 물리적인 환경 통제(physical and environmental controls)

물리적인 환경 통제는 대규모 데이터 센터와 관련 있는 것으로 서버 및 워크스테이션 등 모든 컴퓨터 장비는 적절히 보호되어야 한다. 이러한 전형적인 통제방법에는 서버가 위치한 방의 잠금장치를 하여 접근을 차단하고, 특정한 개인에게 서버 접근을 제한하고, 화재경보 및 진압장치를 제공하고, 홍수가 발생할 수 있는 낮은 지역이나 인화성 물질을 판매하는 상점 등의 환경적 위험으로부터 시스템 및 데이터 등을 멀리 위치하게 하는 것 등이 포함된다.

마. 시스템 소프트웨어 통제(system software controls)

윈도, 유닉스, 리눅스 등 운영체제, 네트워크 통신 관련 소프트웨어, 방화벽, 데이터베이스 시스템 등이 시스템 소프트웨어에 포함된다. 시스템 소프트웨어는 매우 복잡하기 때문에 IT감사의 전문성이 특히 요구된다. 이러한 통제를 통하여 데이터 통제 접근권, 직무 분할 강화, 외부 침입 및 보안 취약성 평가, 외부 침입 테스트, 기밀 데이터의 암호화 등을 확인할 수 있다.

바. 시스템 개발 통제(system development and acquisition controls)

모든 시스템 개발 및 구입과 관련된 업무가 효과적으로 수행되었는지 여부를 파악하는 것이 필요한데, 다음과 같은 부분을 점검해야 한다.

- 사용자 요구사항이 문서화되어 있고 그 실적이 측정되어야 한다.
- 시스템 설계는 사용자 요구와 적절한 통제방법을 준수해야 한다.
- 시스템 개발은 요구사항과 설계 등을 충분히 반영하여 구조화된 방법으로 수행되어야 한다.
- 테스팅은 개별시스템이 요구한 사항대로 작동하고, 시스템 인터페이스가 예상하였던 대로 구동하고, 의도하였던 기능들이 제대로 돌아가는지 확인해야 한다.

사. 어플리케이션 통제(application-based controls)

이 통제의 목적은 모든 입력 데이터가 정확하고, 완벽하고, 권한이 부여된 것인지 확인하는 것이며, 모든 데이터가 원래 의도대로 처리되고, 저장된 데이터가 정확하고, 모든 출력 데이터가 정확한지를 검토하는 것이다. 이를 위하여 입력 데이터 무결성을 확인하는 입력 통제, 처리의 완결성 및 정확성을 확인하는 처리 통제, 원래 얻고자 하는 결과가 출력되었는지를 확인하는 출력 통제, 데이터 처리 또는 저장 시 데이터가 일관되고 정확한지를 확인하는 무결성 통제가 제대로 작동하는지를 점검한다.

3. 감사보고

이 단계에서는 일반적인 감사보고서 체계와 동일하며, 감사목적, 감사범위, 감사방법론, 감사결과, 결론 및 제안사항 등을 보고서 내에 포함한다.

제5절 금융감독원 IT경영실태 평가 매뉴얼

금융기관의 핵심업무가 대부분 전산화되어 있고 대다수 거래가 IT에 의해 처리되고 있어, IT부문의 안전성 및 건전성 여부가 금융기관 전체 업무의 안전성 및 건전성에 많은 영향을 미치고 있으므로, 시스템 위험, 전산화 정도, IT조직 및 운영 규모 정도 등에 따라 IT부문에 대한 내부통제제도를 적절히 수립하는 것이 무엇보다 중요하며, 독립적인 위치에 있는 감사조직에서 이러한 내부통제제도가 제대로 준수되고 있는지를 주기적으로 점검하는 것이 매우 중요하다(금융감독원, 2006).

금융감독원에서는 'IT경영실태평가'를 통하여 국내에 금융영업을 하는 조직을 대상으로 IT감사를 시행하고 있다. 한국전산원이 IT개발 중심의 프로젝트 감리를 위한 기준을 제공하고 있다면, 금융감독원의 평가는 전체 IT부문의 내부통제 및 관리체계를 평가한다는 점에 그 특성이 있다. 금융기관 IT부문 경영실태 평가는 각 금융기관 업무의 중추적인 기능을 담당하고 있는 IT분야를 종합적이고 통일적인 방식에 의해 일정한 등급으로 평가하여 금융기관의 안전성 및 건전성을 제고하는 데 의의가 있다. 이에 미국 연방준비은행 등 미국의 5개 금융감독당국이 적용하고 있는 체크리스트를 모델로 국내금융기관 실정에 적합한 'IT부문 경영실태 평가용 체크리스트'를 개발하여 IT부문에 대한 경영실태 평가를 실시하고 있다. IT부문 경영실태 평가는 일반 업무의 성격 및 규모, IT부문에 대한 의존도 등에 비추어 IT부문 위험이 높은 금융기관[6]과 네트워크가 집중된 금융 유관기관[7]을 대상으로 실시한다.

평가분야는 IT부문을 'IT감사', 'IT경영', '시스템 개발 도입 및 유지·보수', 'IT서비스 제공 및 지원' 등 총 4개 분야로 분류하여 평가한 뒤 이를 토대로 종합평가를 실시한다. 'IT감사'는 IT부문에 대한 금융기관 내부의 자체감사 등, 'IT경영'은 IT경영전략, 조직 및 예산, 인적·물적 자원관리 등, '시스템

6) 국내 시중은행, 지방은행, 특수은행, 증권회사, 생명보험, 손해보험, 신용카드사, 종금사를 말한다.
7) 증권선물거래소, 증권예탁원, 증권금융, 보험개발원, 저축은행중앙회, 신협중앙회를 말한다.

개발 도입 및 유지·보수'는 전산시스템 구축 및 업무용 프로그램 개발 등, 'IT서비스 제공 및 지원'은 전산시스템 이용, 통신망 관리 및 운용 등에 중점을 두고 있다.

'IT감사분야'는 금융기관 스스로 IT경영, 시스템 개발, 도입, 유지·보수, IT서비스 제공 및 지원 등 IT부문 전반에 걸친 적절한 내부통제제도 수립 여부, 감사부서 및 IT부서의 내부감사요원이 주기적으로 위의 통제제도의 준수 여부, 그리고 위의 통제제도가 적정한지를 평가함으로써 금융기관 IT부문의 안전성 및 건전성을 확보하도록 한다.

'IT경영분야'는 금융회사의 핵심 업무가 대부분 전산화되어 있어 영업 경쟁력 확보를 위한 IT투자비용이 지속적으로 증가하고 있다. 따라서 전체 경영전략에서 IT부문이 차지하는 비중이 점차 높아지고 있으므로 금융회사의 경영전략을 효율적으로 지원하기 위한 IT조직 및 인력 구성, 재난 및 장애 시를 대비하기 위한 비상대책 수립, 의사결정에 필요한 정보를 제공하는 정보시스템의 구축 및 운영 등 전략적인 측면에서 IT부문에 대한 관리가 필요하다.

'시스템 개발 도입 및 유지·보수 분야'는 금융회사 전산부문에 대한 안전성 및 건전성은 전산시스템의 구축 및 프로그램 개발과 변경과정의 안전성 및 건전성 확보에 달려 있다. 이미 구축된 전산시스템은 근본적인 변경이나 새로운 통제체제를 추가하는 것이 매우 어렵고 지속적인 유지·보수가 필요하므로, 시스템 개발과 유지·보수 과정에 대한 표준화 및 통제절차가 요구된다.

'IT서비스 제공 및 지원 분야'는 금융회사에서 운영 중인 전산시스템의 지속적인 안전성 확보를 위해서는 시스템 개발 및 유지·보수의 중요성과 함께 일상적인 운영활동이 적절하여야 한다. 적정하게 구축된 시스템도 시스템을 운영하는 요원이나 환경에 따라 오류 또는 사고발생 위험이 상존하므로, 오류 등의 최소화를 위하여 표준화된 운영절차 마련 및 준수가 필요하다.

위의 4개 분야에 대하여 총 20개의 평가항목을 설정하되 IT업무의 특성상 모두 비계량지표를 기준으로 평가하고 있다(금융감독원, 2006).

〈표 2-3〉 IT경영실태 평가항목

평가부문	평가항목	세부평가항목
IT감사	IT감사 조직 및 요원	감사위원 및 감사위원회 조직
		IT감사 실무조직
	IT감사 실시내용	정기감사
		일상감사
		수시감사
		IT부서 자체감사
	IT감사 사후관리 및 기타	감사결과 문제점 및 취약사항에 대한 사후관리
		IT감사업무편람
IT경영	IT부서 조직 및 인원	IT부서 조직
		IT부서 요원관리
	IT 관련 내규	IT 관련 내규체계
		IT 관련 내규현황관리
	IT계획 및 방향 제시	IT계획 및 방향 제시
		IT운영회 운영제도
		IT사업 추진
		IT외주용역에 대한 관리
	비상계획	전반적인 비상계획 대응 내용
		백업센터 구축
		하드웨어 백업 및 복구
		소프트웨어/데이터 백업 및 복구
		통신망 백업 및 복구
		테스트
	경영정보시스템 등	경영정보시스템 정책과 지침
		경영정보시스템 개발
		경영정보시스템 운영
		기타 IT경영과 관련된 주요 사항

평가부문	평가항목	세부평가항목
시스템 개발 도입 및 유지·보수	시스템 개발 도입 및 유지·보수 관련 조직 및 요원	직무분리
		인적자원 및 자질
	시스템 개발 도입 및 유지·보수 관련 내규	관련 내규의 적정성
	시스템 개발 도입 및 유지·보수 현황	시스템 개발/도입 프로젝트에 대한 관리 및 통제
		시스템 개발/도입
		응용프로그램 유지·보수
		운영체제 등 시스템 프로그램 유지·보수
		테스트 및 이행
		문서화
	내부통제용 시스템, 시스템 통합 등	내부통제용 시스템
		시스템 통합, 전환, 재개발
		기타 시스템 개발 도입 및 유지·보수와 관련한 주요 사항
IT서비스 제공 및 지원	IT서비스 제공 및 지원 관련 조직 및 요원	직무분리
		인적자원 및 자질
	IT서비스 제공 및 지원 관련 내규	관련 내규의 적정성
	시설 및 장비	물리적인 환경
		장비의 유지·보수
	운영 통제	데이터입력 통제
		처리 통제
		출력자료 분배 통제
		테이프 등 보조기록 매체관리
		시스템 성능관리
	보안	보안감독 및 책임
		물리적 보안
		논리적 보안
		보안성 심의
	통신망	통신망 구축현황 관리
		통신망 통제
		통신망 장애관리

평가부문	평가항목	세부평가항목
	최종사용자 컴퓨팅	최종사용자 컴퓨팅 현황 관리
		최종사용자 컴퓨팅 통제
		재해복구 및 비상대책
	전자금융거래 등	전자금융거래 신청단계의 적정성
		본인확인수단 관리
		현금카드 등 전자금융거래매체 관리
		자동화기기 관리
		입·출금계좌 지정 및 한도 관리
		거래내역 자동통보제도 운영
		전자금융거래 고객 보호
		전자금융거래 관련 계약내용
		전자금융대출 등
		IT서비스 제공 및 지원에 관한 기타 주요 사항

위의 IT감사의 목적에서 보듯이 IT부문의 경영실태 평가를 위해 4개 부문으로 구분하고 있지만, 사실상 IT감사가 나머지 3개 부문을 포함하고 있어 'IT경영', '시스템 개발 도입 및 유지·보수', 'IT서비스 제공 및 지원' 등이 IT감사와 별도의 평가항목이 아닌 IT감사의 일부로 보는 것이 타당하다.

1. 감사계획

내부감사의 효과는 감사기술의 건전성과 적절한 감사계획에 좌우되는데, 감사목적을 명확하게 정의할수록 이에 맞는 감사절차가 보다 더 적절하게 만들어질 수 있고 감사가 효과적으로 수행될 수 있다. 감사계획에는 다음과 같은 내용이 포함되어야 한다.

- 목표 설정, 절차 수립, 예산
- 검사에 필요한 자원
- 수감부서로부터 각종 보고서 명세, 정보, 기타 필요한 자료 수집

- 제한된 예산범위 내에서 목표를 달성하기 위한 업무 할당
- 조건 변경에 따른 목표, 절차, 예산의 재검토

2. 감사실시

감사계획이 확정되면 감사계획을 달성하기 위한 감사요원과 감사방법 및 수단을 선정하여야 한다. 감사계획에 대한 감독은 기설정된 감사목표를 달성하고 감사계획에서 요구된 내용이 부합되도록 감사활동을 지휘, 조정, 통제하는 것을 의미한다. 감사목표를 달성할 수 있도록 IT부문 감사의 범위 및 주기를 결정하여야 하며 수립된 정책, 지침 및 절차의 이행 여부(규정 준수), 관리의 질적 수준과 절차 및 통제의 적절성, 부당행위, 프로그램 및 운영체제의 완전성, 시스템 설계 및 이행, IT자원 접근 권한 등의 완전성을 점검해야 한다. 이러한 범위하에서 조정, 데이터 입력 통제, 컴퓨터 운영, 시스템 개발, 프로그램 변경, 데이터 통신, 출력자료 배포, 사용부서의 데이터 처리 통제 등과 같은 기능에 대한 점검이 이루어져야 한다.

IT부문에 대한 감사절차는 감사부서의 전문적인 지식 보유 여부와 데이터 센터 및 사용자 환경의 복잡성 여부에 따라 다를 수 있으나, 데이터 처리과정에 대한 전문적인 기술감사는 반드시 필요하다. 감사를 진행하는 방법은 서류 검토 등 수작업으로 감사하는 방법과 전산감사기법을 이용하여 감사하는 방법이 있는데, 통상 이 2가지 방법을 병행하여 감사를 실시한다.

3. 감사보고

감사결과 나타난 문제점을 종합하고 경영층에 감사결과를 효과적으로 전달하기 위한 절차가 수립되어야 하는데, 기본적인 지침은 다음과 같다.

- 감사목적 및 범위
- 감사결과 나타난 문제점을 명확하게 종합하여 IT담당 임원과 논의하고,

최고경영층과 이사회 등에 서면으로 보고

- 실무 부서장과 감사결과 적출된 중요한 내부통제 위반사항과 미해결된 상태로 남아 있는 문제점에 대하여 논의
- 감사보고서에 지적사항, 노출된 위험, 시정을 위한 권고안 등을 포함
- 감사내용에 대한 종합적인 의견을 기술(지난번 감사결과보다 개선되었는지 여부와 이유 등)
- 감사보고서에 기술된 평가내용, 문제점 등에 대한 입증자료를 자료에 첨부
- 수감기관 부서담당 경영층이 적시에 감사보고서에 대한 서면 답변을 준비하도록 명문화
- 감사결과 적출된 지적사항이 시정되었고 이사회에서 지적사항을 인정하였는지를 확인하기 위한 사후관리

제6절 정보화진흥원 정보시스템 감리점검 해설서

감리는 감리의 대상이 되는 정보화사업이 초기에 목표한 성과(또는 기대효과)를 만족할 수 있도록 정보시스템의 계획 및 구축 등의 활동이 적정하게 수행될 수 있도록 종합적으로 점검하고 발생할 수 있는 위험요인 및 문제점을 개선할 수 있도록 하는 것이다(한국정보사회진흥원, 2006).

1987년 행정전산망사업에 대한 사업감리를 시작으로 한국전산원이 IT개발감리를 전담하여왔다. 1998년부터 감리를 점진적으로 민간감리전문업체에 위탁하고, IT사업이 양적으로 팽창하면서 개발감리 또한 양적으로 늘어나고 있다. 이에 따라 정보화진흥원은 기존의 전산감리기준(1994년 전산망조정위원회)을 개선, 보완하여 '정보시스템감리기준(1999년 정보통신부)'을 제정하였고 이것이 현재까지 IT개발감리를 수행하는 데 있어 기본적인 기준이 되고 있다(장태범·김문오, 2004). 정보시스템 감리기준 및 점검체계는 4차례의 갱신과정을 거쳐 2003년까지 감리영역, 개발공정, 기술분야 등에 따라 총 24건의 개별 감리지침을 체계화하여 2004년 공공부문의 정보화사업 유형 기반 점검체계를 구성하였다(한국정보사회진흥원, 2008).

현재의 국내 정보시스템 감리체계는 「정보시스템의효율적도입및운영에관한법률」을 근거로 「정보시스템감리기준(행정안전부 고시 제2008-18호)」과 한국정보사회진흥원의 정보시스템 감리점검 해설서(2008.3.3), 정보시스템 감리기준 해설서로 구성되어 있다. 법제도화에 따라 일정 규모 이상의 정보시스템 개발사업에 대한 의무화를 실시하고 정보시스템 감리 지적사항에 대하여 발주기관 및 피감리인의 개선조치 활동을 강화함에 따라 감리의 책임성이 강조되고 있다. 이에 따라 감리점검체계에 기반을 둔 품질 높은 감리가 요구되고 있다. 정보시스템 감리를 수행함에 있어 기본이 되는 기준은 「정보시스템의효율적도입및운영에관한법률」 제11조 제4항에 의거하여 2008년 6월 19일 행정안전부 고시 제2008-18호로 개정·고시된 「정보시스템감리기

준」(이하 감리기준)이다. 감리기준은 감리의 계약, 감리계획 수립, 착수회의, 현장감리, 감리보고서 작성, 감리결과 조치내역 확인 등 감리업무를 효율적으로 수행할 수 있도록 감리의 절차 및 방법을 규정하고 있으며, 정보시스템의 구축·운영에 관한 사항을 종합적으로 점검·평가할 수 있도록 정보시스템 감리 기본점검표(이하 기본점검표)를 제시하고 있다. 기본점검표는 점검프레임워크를 기반으로 사업유형별/감리시점별/감리영역별로 도출된 점검항목을 모아서 표로 나타낸 것이다. 각 감리영역별로 해당 분야에 대한 개요와 점검하여야 할 기본점검항목이 정의되어 있다.

▶ **기본점검표**

- 정보화전략계획 수립사업

감리시점	감리영역	개요	기본점검항목
현황분석 및 전략수립	업무	조직 및 업무의 현황과 문제점을 통하여 정보화 목표 및 업무 개선과제를 적정하게 도출하였는지 점검	1. 업무 관련 사용자 요구사항 도출 및 분석의 충분성, 적정성 2. 조직의 목표와 전략 식별 여부 3. 조직 내·외부 환경분석을 통한 강점, 약점, 기회, 위협요인 파악이 충분한지 여부 4. 정보화 목표 및 조직목표/전략 간의 일관성 및 역할 정립의 적정성 5. 핵심 성공요소 식별의 충분성 및 조직목표/전략에 부합하는지 여부 6. 조직의 업무기능 분석 및 핵심 프로세스 정의의 충분성, 적정성 7. 정보화 관점에서의 개선과제 도출이 적정한지 여부
	기술	……	……

한편, 감리기준에서 정의하지 못한 세부적인 사항에 대해서는 제21조(세부사항)에 근거하여 정보화진흥원장이 세부사항을 정하여 공지할 수 있도록 하고 있다. 이에 기본점검표를 중심으로 기본점검표의 구성 배경 및 기본점검표에서 정의한 점검항목을 점검하기 위한 점검항목별 검토항목을 '사업유형/

감리시점/감리영역별 지침(이하 감리영역별 지침)'으로 제시하고, 기본점검표와 감리영역별 지침에 대한 활용체계를 '감리점검 해설서'로 제공하고 있다. 정보시스템 감리점검체계는 감리수행기관의 관점 위주로 작성되어 있으며 발주기관이나 피감리인(개발업체)의 관점에서는 직접적인 준수 요건으로 활용하기는 어렵다. 발주기관 관점에서는 감리 수행 시 점검항목의 추가를 위한 참조자료로서 활용이 가능하며 피감리인(개발업체)은 자체 점검을 위한 검토항목으로 활용할 수 있다. 현행 정보시스템 감리기준은 기본적으로 '감사지침'의 성격으로 작성되어 있으며 지침내용에는 참조모델, 통제지침 등의 관리지침도 부분적으로 흡수하여 감리수행기관 관점으로 구성되어 있다.

감리관점/점검기준은 대상 사업에 대한 방법론, 사업추진계획, 절차 등 사업에 대한 절차(Process)와 그 결과로 생성되는 산출물(Product)을 점검/평가하고, 결론적으로 대상 사업이 당초에 목적하였던 성과(Performance) 또는 기대효과를 달성할 수 있도록 하는 역할을 구분한 것으로 절차, 산출물, 성과의 3개 관점(〈표 2-4〉 참조)에 13개의 점검기준(〈표 2-5〉 참조)이 설정되어 있다. 각 점검기준은 'COBIT(Control Objectives for Information and related Technology)' 등 각종 해외 표준을 참조하였다.

〈표 2-4〉 감리관점

감리관점	내용
절차 (Process)	사업에 대한 각종 관리활동 및 구축/운영 계획 및 절차의 수립과 준수 여부의 적정성을 검토
산출물 (Product)	적정한 구축/운영 절차를 통하여 생산된 각종 문서, 시스템, 서비스 등에 대한 적정성을 검토
성과 (Performance)	궁극적인 사업의 성과목표 및 기대효과의 달성 가능성 및 달성 여부에 대한 검토

〈표 2-5〉 감리관점에 따른 점검기준 및 특징

감리관점	점검기준	관련 성질
절차	계획 적정성 (Plan Reasonability)	사업수행계획, 인력운용계획 등 각종 계획 수립의 적정성
산출물	절차 적정성 (Process Reasonability)	개발/운영/유지·보수 절차 수립 적정성, 위험/일정/품질/형상/인력/변경관리 절차 등의 수립 적정성
	준수성(Compliance)	각종 계획의 준수 적정성, 위험/일정/품질/형상/인력/변경관리 등 절차 및 활동의 준수 적정성
	기능성(Functionality)	기능의 충분성, 완전성, 정확성, 상호 운용성, 연계성
	무결성(Integrity)	데이터 무결성 및 정확성
	편의성(Usability)	사용/운영 편의성, 학습성
	안정성(Stability)	시스템 안정성, 서비스 연속성, 복구 신속성
	보안성(Security)	시스템 기밀성, 안정성
	효율성(Efficiency)	정보자원(인력, 서버 등) 활용의 효율성, 업무 효율성, 응답시간 신속성, 시스템 확장성, 기술발전 부합성
	준수성(Compliance)	산출물의 관련 기준/절차/표준/방법론 준수성
	일관성(Consistency)	분석성, 변경성, 현행화, 추적성, 유지·보수성
성과	실현성(Realizability)	구체성, 실현가능성, 투자 대비 효과성, 성과목표 달성, 시스템 사용 가능성
	충분성(Sufficiency)	업무/기술적 요건 만족, 사업목표 달성, 과업범위 충분성

사업유형과 진행상태에 따라 감리영역의 구분과 점검항목을 선택하기 위한 체계를 점검모델로 구성하였으며, 현행 감리점검체계에서는 7개의 사업유형, 즉 ① 정보기술 아키텍처 구축사업, ② 정보화전략 계획수립사업, ③ 정보시스템 개발사업, ④ 데이터베이스 구축사업, ⑤ 시스템 운영사업, ⑥ 유지·보수 사업, ⑦ 사업관리 사업으로 분류하고, 이를 기준으로 46개 감리영역으로 세분되어 있다(한국정보사회진흥원, 2008).

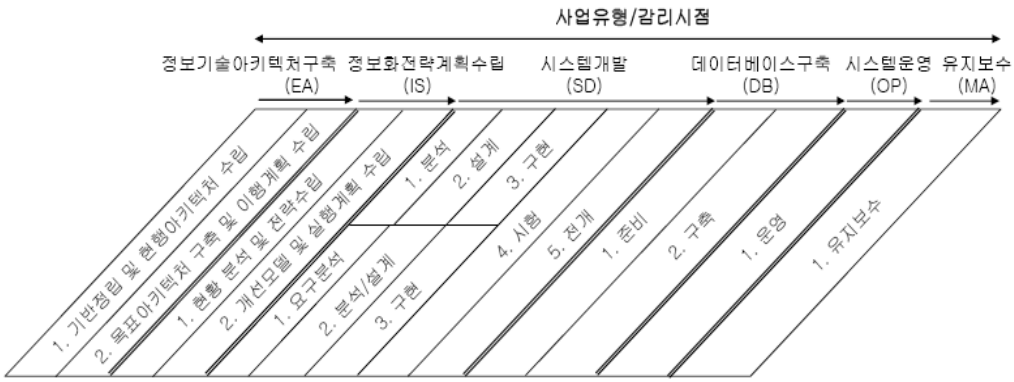
〈표 2-6〉 사업유형별 감리시점 및 감리영역

사업유형	감리시점		감리영역
정보기술 아키텍처 구축	기반정립 및 현행 아키텍처 구축		기반정립
			현행 아키텍처 구축
			품질보증활동
	목표 아키텍처 구축 및 이행계획 수립		이행계획 수립
			목표 아키텍처 구축
			관리체계
			품질보증활동
정보화전략 계획 수립	현황분석 및 전략 수립		업무
			기술
			품질보증
	개선모델 및 실행계획 수립		정보화계획
			품질보증
정보시스템 개발	구조적/정보공학적 모델	분석	시스템 아키텍처
			응용시스템
			데이터베이스
		설계	시스템 아키텍처
			응용시스템
			데이터베이스
		구현	시스템 아키텍처
			응용시스템
			데이터베이스
	객체지향/컴포넌트기반 모델	요구분석	시스템 아키텍처
			응용시스템
			데이터베이스
		분석설계	시스템 아키텍처
			응용시스템
			데이터베이스
		구현	시스템 아키텍처
			응용시스템
			데이터베이스

사업유형	감리시점		감리영역
	공통	분석	품질보증활동
		설계	품질보증활동
		구현	품질보증활동
		시험	시험활동
			품질보증활동
		전개	운영준비
			품질보증활동
데이터베이스 구축	준비		데이터 수집 및 시범 구축
	구축		데이터 구축
			품질검사
시스템 운영	운영		서비스 제공
			서비스 지원
유지·보수	유지·보수		유지·보수 이행
사업관리	착수/계획		사업관리
	실행/통제		사업관리
	종료		사업관리

여기서 사업유형이라고 함은 계획-실행-통제의 생명주기를 기반으로 하여 구분한 것으로, 계획에 해당하는 정보화전략 계획수립사업, 실행에 해당하는 시스템 개발사업, 데이터베이스 구축사업, 통제에 해당하는 시스템 운영과 유지·보수 사업으로 구성된다. 사업유형별 감리시점은, 정기감리체계를 반영하여 각종 방법론, 감리보고서 등을 참조하여 사업유형별로 감리를 시행하기에 적절한 시점을 제시한 것이다.

〈그림 2-3〉 사업유형별 감리시점



1. 감사계획

앞에서도 언급한 바와 같이 정보시스템 감리계획은 감리수행기관의 관점으로 구성되어 있어 감리수행기관이 주체가 되어 발주기관의 IT 관련 사업을 감사하게 된다. 감리대상의 특성, 적용기술, 현재 상태에 대한 정보를 바탕으로 중점검토사항을 정의하는 예비조사활동을 수행한다. 감사계획서 내에는 다음과 같은 사항을 검토하여 작성하게 된다.

가. 관련 근거

감리요청 공문 및 감리계약 공문 등 관련 근거를 기재한다.

▶ 작성 예
- 감리발주기관-20060101(2006.1.1). “XXXX 구축사업에 대한 감리요청”
- 감리법인-20060201(2006.2.1). “XXXX 구축사업에 대한 감리계약”

나. 감리 목적

감리대상사업의 특성을 고려하여 감리의 목적을 기술한다.

다. 감리 적용기준

감리에서 준용하고자 하는 기준, 표준, 지침 등을 명시한다.

▸ 작성 예
- 정보시스템 감리기준(정보통신부 고시 제2006-00호)
- 정보시스템 감리점검 해설서(한국전산원 공지 제2006-00호)
- 정보시스템 구축·운영 기술지침(정보통신부 고시 제2006-37호)
- 국가정보보안기본지침, 국가사이버 안전매뉴얼(국가정보원)
- XXXX 지침, XXXX 표준(KSC-0000)

라. 감리대상범위 및 단계

감리대상사업의 감리단계를 명시(예: 분석설계단계)하고 감리대상이 되는 시스템 또는 업무를 명시(2레벨 이상 상세하게 작성)한다.

▸ 작성 예

가. 대상업무: *[감리대상사업명]*

o *[감리대상사업의 세부 대상 업무 1]*

o *[감리대상사업의 세부 대상 업무 2]*

나. 감리단계: *[감리단계/시점]*

마. 감리영역별 상세 점검항목

정보시스템 감리 기본점검표와 감리대상사업의 특성에 따라 현 감리단계에서 중점적으로 점검할 상세 점검항목을 감리영역별로 제시한다.

▶ 작성 예

감리 영역	점검항목	검토항목	비고
시스템 구조	1. 현행 및 신규 시스템의 운영환경을 충분히 분석하였는지 여부	1. 현행 시스템 및 신규 시스템에 대한 운영환경이 충분히 분석되었는가? - 현행 및 신규 시스템 운영환경 - 현행 시스템의 주요 정보자원 현황 - 신규 시스템 구축 시 정보자원 소요현황	
	.....	.....	
		.....	
	.....	.....	

바. 감리일정

감리일정을 명시하고, 감리보고서 통보 일정, 감리결과 조치내역 확인에 대한 일정 계획을 명시한다.

사. 감리수행기관 편성

참여할 감리수행기관(총괄감리원 및 감리원)의 성명과 감리원증번호를 기재하고, 감리원의 변경은 발주기관의 사전 승인이 필요하다.

아. 감리계획서 및 보고서 통보기관

감리계획서와 감리보고서, 감리결과 조치내역 확인보고서 등을 통보해야 하는 기관을 명시한다.

자. 기타 행정사항

기타 문서보안사항, 감리자료 관련 사항 등 행정적으로 필요하거나 상호 준수해야 할 사항이 있는 경우 이를 기술한다.

2. 감사실시

감사실시에서는 착수회의시점까지 제출된 산출물과 사업 관련 문서 등을 접수하여, 각 감리영역별 감리원들이 상세점검항목을 토대로 점검하여야 한다. 또한, 개발자 또는 공공기관 사업관리 담당자 등 관련자와의 면담을 통하여 발견된 문제점을 상호 검토하고, 감리원은 발견된 문제점에 대한 증거 또는 논거를 충분히 확보하여야 한다. 또한, 수시로 감리영역별 담당 감리원간의 회의 및 협업을 통하여 효율적이고 일관성 있게 수행할 수 있도록 하여야 한다. 감리현장에서의 감리업무 수행과정 및 내용은 통상적으로 다음과 같다.

- 감리원별로 담당 감리영역에 대한 발주기관(공공기관) 및 사업자의 담당자 확인
- 감리원별 담당 감리영역 및 검토부문에 대한 세부적인 필요 문서(산출물, 자료 등) 확보
- 상세 점검항목을 토대로 확보된 문서의 검토를 통한 특이사항 및 문제점 확인, 정리
- 필요시 발주기관 및 사업자에 추가적인 보완자료 요청 및 면담을 통한 확인 실시
- 정리된 문제점 및 개선사항에 대하여 발주기관 및 사업자 담당자와 면담 및 확인
- 산출물 검토 및 면담 등을 통하여 도출한 문제점 및 개선사항에 대한 감리보고서 초안 작성

예를 들어 정보화전략계획 수립사업의 경우 기본적으로 조직 및 업무의 현황과 문제점 분석을 통하여 정보화목표 및 업무 개선과제를 적정하게 도출하였는지에 초점을 맞추어 점검한다. 기본 점검항목은 ① 업무 관련 사용

자 요구사항 도출 및 분석의 충분성·적정성, ② 조직의 목표와 전략 식별 여부, ③ 조직 내·외부 환경분석을 통한 강점, 약점, 기회, 위협요인 파악이 충분한지 여부, ④ 정보화 목표 및 조직목표/전략 간의 일관성 및 역할 정립의 적정성, ⑤ 핵심 성공요소 식별의 충분성 및 조직목표/전략에 부합하는지 여부, ⑥ 조직의 업무기능 분석 및 핵심 프로세스 정의의 충분성·적정성, ⑦ 정보화 관점에서의 개선과제 도출이 적정한지 여부를 검토한다.

3. 감사보고

감리보고서는 감리용역의 최종 산출물이며, 감리원이 감리기간 동안 발견한 문제점과 개선방향을 발주기관/사업자에게 정확하게 통보하여 개선하는데 목적이 있다. 따라서 감리보고서는 이해하기 쉽고, 논리적이며 충분한 증거자료를 토대로 객관적인 관점에서 작성되어야 한다. 또한, 감리보고서는 감리 종료 이후에도 부실감리 여부를 판단하는 주요한 자료로 활용할 수 있으므로 개선이 필요한 문제점은 반드시 보고서에 모두 명시하여야 하며, 명확하고 구체적으로 작성해야 한다.

보고서에는 감리법인의 직인, 총괄감리원의 서명날인, 참여감리원 명단이

감리영역별 평가

평가단계	작성기준
적정	사업의 성공적인 완수에 영향을 미칠 수 있는 문제점이 발견되지 않았으며, 사업목표 달성이 충분한 상태
보통	사업의 성공적인 완수에 영향을 미칠 수 있는 문제점이 발견되었으나 사업 추진전략이나 계획된 자원 내에서 개선할 수 있어 사업목표 달성이 가능한 상태
미흡	사업의 성공적인 완수에 영향을 미칠 수 있는 중대한 문제점이 발견되었고, 사업 추진전략이나 계획된 자원의 정비가 선행되어야만 사업목표 달성이 가능한 상태
부적정	사업의 성공적인 완수에 영향을 미칠 수 있는 중대한 문제점이 발견되었고, 사업 추진전략이나 계획된 자원 내에서 개선할 수 없어 사업목표 달성이 불가능한 상태

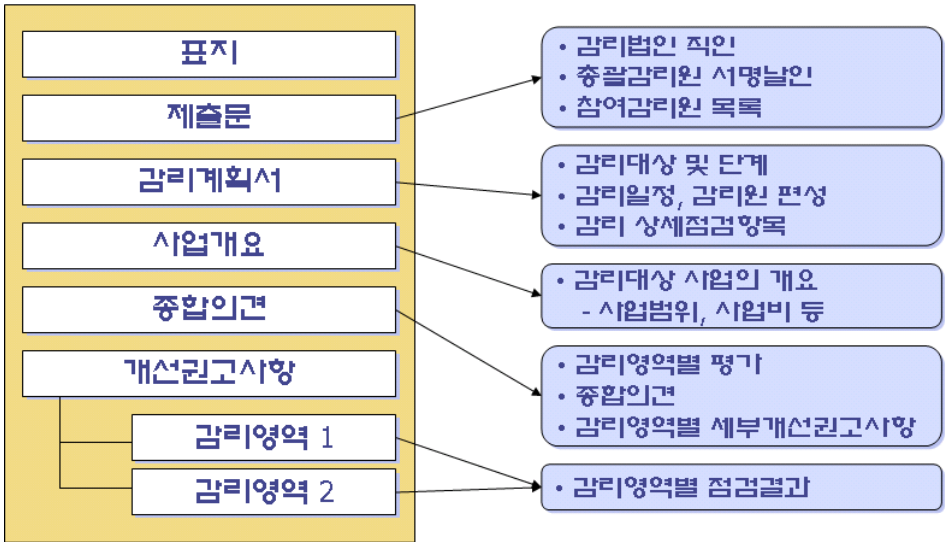
표시된다. 감리보고서상의 감리계획서는 착수회의 등을 통해 변경사항이 발생하였을 경우, 반드시 변경된 최종 버전을 첨부하여야 한다. 감리보고서의 실질적인 부분은 종합의견부터 시작한다. 종합의견 부분에는 감리영역별 평가는 감리원이 발견한 문제점이 사업에 미치는 영향도, 사업목표의 달성 정도 등을 토대로 4단계(적정/보통/미흡/부적정)로 구분하여 작성한다.

그리고 전체적으로 주요한 사항을 요약 정리한 종합의견, 감리영역별 세부 개선권고사항 목록(개선권고유형, 개선시점, 중요도, 발주기관 협조 필요 여부 표시 포함)을 작성한다.

▸ **개선권고유형**

개선권고 유형	작성기준
필수	발견된 문제점 중 사업목표를 달성하기 위하여 반드시 개선해야 할 사항
협의	발견된 문제점 또는 발생 가능성이 큰 문제점 중 발주기관과 피감리인이 상호 협의를 거쳐 반영 여부를 결정할 수 있는 사항
권고	감리의 대상범위를 벗어나지만 사업목표 달성에 도움이 되는 사항

〈그림 2-4〉 감리보고서 양식



제7절 비교·분석결과

감사기준을 보면 대부분의 기관들이 여러 국제기준을 혼용하여 개발하였고, 특히 그중에서도 COBIT 기준을 공통적으로 참고한 것이 특징이다(〈표 2-7〉 참조). ISACA가 개발한 통제기준인 COBIT은 민간기업에서 많이 사용하는 기준이기도 하지만 공공부문에도 응용하여 사용할 수 있다는 것은 정보시스템에 있어서 공공부문과 민간부문의 영역 차이 없이 범용으로 사용할 수 있다는 것이다. GAO도 자체적인 IT감사 매뉴얼을 개발하면서 COBIT 모델을 참조한 것은 COBIT의 활용 범위가 폭넓음을 알 수 있다.

1. 감사계획

감사인은 감사를 계획하고 효과적인 감사접근방법을 개발하기 위하여 수감기관의 내부통제제도를 충분히 이해하여야 한다. 특히 수감기관의 정보시스템 활동의 중요성과 복잡성 및 감사에 이용될 자료의 가능성에 대한 이해도 필요하다. 이것이 고유위험과 통제위험의 평가에 어떤 영향을 미칠 것인가도 고려해야 한다. 대부분의 감사에서 수감기관의 이해를 높이기 위하여 기초자료들을 감사 초기에 기본적으로 검토하지만 그 자료들을 통해서 위험요소에는 어떤 것들이 있고 어떤 위험요소가 가장 중요한지, 또한 이런 요소들이 기관업무에 어떤 영향을 끼치는가에 대해서 자세히 검토하지는 않는다. 특히 정보시스템의 운영과 관리에 대해 깊은 지식이 없는 경우 기술적인 문제를 찾기란 쉽지 않은 것이 현실이다. 그런 점에서 GAO, ISACA, INTOSAI, IIA 등 외국의 기관들은 모두 위험기반의 감사를 시행하고 있으며, 감사계획 시 위험평가를 통하여 정보시스템의 취약점을 찾아 그 원인과 문제점들을 찾아 해결하려 하고 있다는 것에 주목할 필요가 있다.

감사계획단계에서는 수감기관의 업무/사업계획, 예산, 인력, 인터넷 자료 등 기본적인 서류들을 검토한다. 일반적인 수감기관의 업무나 사업에 대한

이해를 해야 하기 때문에 반드시 필요한 부분이다. GAO의 경우 정보시스템의 잠재적인 위험요소를 미리 파악하여 감사계획단계에서 진단을 한다. ISACA는 고유위험, 통제위험, 적발위험 등 3가지로 구분하여 위험평가를 하고, INTOSAI는 기초적인 위험평가를 실시하고 그 결과에 따라 감사계획을 어떻게 세울 것인지를 결정한다. 그만큼 잠재적인 IT위험요소가 무엇인지 파악하는 것이 성공적인 감사를 수행하는 데 얼마만큼 중요한지를 알 수 있는 부분이다.

2. 감사실시

감사실시 부분에서 공통적인 특징은 대부분의 기관들이 IT감사를 조직의 내부통제 중에서 IT통제에 초점을 두고 있으며 일반통제부문과 어플리케이션 통제부문으로 분류하고 있다는 것이다. 앞에서도 설명한 바와 같이 일반통제는 조직의 전산업무에 적용되는 정책·절차·구조 등 IT시스템과 관련된 외부의 환경적인 요소를 대상으로 볼 수 있고, 어플리케이션 통제는 개별단위의 IT시스템의 입력·처리·출력 등 IT시스템 자체의 기능을 대상으로 초점을 맞추어 실시한다. INTOSAI의 경우 감사유형을 IT감사를 일반 감사의 일부분으로 분류하거나, 독립적인 IT감사, IT 관련 감사의 3가지 유형으로 구분하였다. IT감사를 성과감사나 재무감사의 일부분으로 분류하기도 하고, 정보시스템 개발감사나 운영 및 유지·보수 감사처럼 독립적인 IT감사로 구분하기도 하고, 구매감사처럼 IT가 감사대상은 아니나 IT와 직접적인 관련이 있는 IT구매에 관한 감사로 분류하였다. 다시 운영 및 유지·보수 감사에 일반통제와 어플리케이션 통제로 구분하였다. 그러나 여기서의 일반통제 측면은 컴퓨터 운영과 관련된 통제요소로 대부분이 보안과 관련한 내용이고, 어플리케이션 통제는 개별 어플리케이션의 트랜잭션 처리에 중점을 두는 것으로 좀 더 협의적인 의미의 통제 형태라는 것이 다른 기관의 일반적인 일반통제와 어플리케이션 통제의 해석과는 다르다는 것이 특징적이다.

3. 감사보고

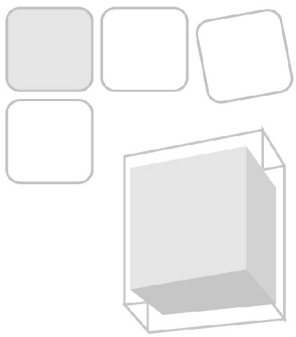
일반 감사보고서와 IT감사보고서의 형식에 있어서 뚜렷한 차이는 없으나, 지침이나 법, 기준, 전산감사기법(CAAT[8]) 활용 등 감사방법에 대한 구체적인 내용을 제시함으로써 감사의 객관성 및 신뢰성을 확보하고자 노력하고 있는 것이 특징적이다.

〈표 2-7〉 IT감사기준 비교·분석

감사절차 / 기관	감사계획	감사실시	감사보고
GAO	- 위험기반의 접근방법	- 정보시스템 통제의 효과성 및 효율성 평가 - 일반통제와 어플리케이션 통제로 구분	- 정보시스템 통제의 취약점 평가결과
ISACA	- 위험기반의 접근방법	- 적절한 IT관리 및 통제 - 일반통제와 어플리케이션 통제로 구분	- 내부통제의 설계 및 운영 - 기준/법/규정 준수 여부
INTOSAI	- 위험기반의 접근방법	- 재무감사, 성과감사, 정보시스템 개발감사, 구매감사, 운영 및 유지·보수 감사(일반통제, 어플리케이션 통제)로 구분	- 감사목적 - 감사범위 - 감사방법론 - 감사결과 - 결론 및 제안사항
IIA	- 업무/사업의 이해 - IT범위 설정 - 위험평가실시	- 거버넌스(정책) - 관리(기준, 조직 및 관리, 물리적인 환경 통제) - 기술(시스템소프트웨어 통제, 시스템개발 통제, 어플리케이션 통제)	- 감사목적 - 감사범위 - 감사방법론 - 감사결과 - 결론 및 제안사항

8) Computer Aided Audit Techniques.

감사절차 / 기관	감사계획	감사실시	감사보고
금융감독원	- 목표 설정, 절차 수립, 예산 - 검사에 필요한 자원 - 수감부서로 부터의 자료 수집 - 업무 할당	- 감사의 범위 및 주기 결정 - 규정 준수 여부 - 내부통제기능의 적절성	- 감사목적 - 감사범위 - 감사결과 - 결론 및 제안사항
정보화진흥원	- 목적 및 기준 - 대상범위 및 단계 - 점검항목 및 일정	- 정보화 사업유형별로 구분하여 감리시점, 감리영역, 점검항목 검토	- 감리계획서 - 감리대상의 사업 개요 - 감리영역별 평가결과



제3장 IT감사 중점사항

제3장 IT감사 중점사항

제1절 비교·분석의 틀

주요국 감사원의 IT감사사례를 비교하기 위해서는 비교기준이 있어야 하는데, 현재 우리나라에는 범정부적인 차원에서 IT감사의 기준을 제공하거나 IT감사를 실시하는 데 필요한 원칙을 제시한 것은 아직 없는 실정이다. 앞에서 언급한 바와 같이 정보화진흥원이나 금융감독원에서 제시한 IT감리 또는 IT검사의 지침서나 매뉴얼이 전부이다. 물론 이들 기관이 제시한 기준이나 원칙을 사용할 수는 있으나 IT감리의 복잡성과 IT검사의 대상기관이 금융부문에 초점이 맞추어져 있다는 점에서 IT감사를 수행할 때 참조할 범용적인 기준으로서 아직 부족한 부분이 있다. 예를 들어 COBIT을 기반으로 한 정보시스템 감리기준의 경우, 기본 점검항목의 개수는 239개이며 감리점검 해설서에서 기본 점검항목을 한 단계 구체화한 검토항목은 299개에 달한다(한국정보사회진흥원, 2008). 상세한 수준까지 세분화되어 있는 평가항목은 보다 정확한 결과를 기대할 수 있으나 평가의 실효성에 대해서는 의문이 든다. 이런 점에서 감리영역의 구분에 있어 사업유형별로 과도하게 세분화되어 있음을 인정하고 재검토가 필요하다고 주장한 바 있다(한국정보사회진흥원, 2008).

그러므로 이러한 범용적인 기준을 적용하기 위해서는 먼저 IT감사의 대상과 초점이 무엇인가를 확인하는 것이 필요하다. 대부분 IT감사의 주요 감사대상은 정부부처나 지방자치단체의 정보화사업 또는 전자정부사업이라고 볼 수 있는데, 이는 정보화사업이나 전자정부사업에 매년 대규모의 예산이 투입되고 있어 성과 측면에서 점검이 필요하기 때문이다. 외국의 경우도 IT감사 대상이 부처의 정보화 관련 사업들이므로 우리와 유사하다고 볼 수 있

다. 따라서 IT감사사례 비교·분석을 위한 감사 대상은 정보화사업 또는 전자정부사업으로 범위를 정하는데 무리가 없을 것으로 판단된다.

한편 감사초점과 관련된 부분은 본 연구에서 소개한 국내외 6개 기관의 IT감사체계를 참고하여 감사중점사항들을 검토하였는데 이를 정리하면 〈표 3-1〉과 같다. 〈표 3-1〉에서 보는 바와 같이 각 기관에서 제시한 구분 형태는 다르지만 감사초점이 될 만한 내용부분에서는 많은 공통점이 있음을 확인할 수 있다. 이는 대부분 기관의 IT감사체계가 COBIT의 기준을 따르고 있는 것이 주요 원인이라고 파악된다. 그러나 감사초점 내용이 다양해서 직접적으로 감사사례를 비교하기에는 너무 복잡하고 이러한 공통된 부분을 보다 효과적으로 분류하기 위하여 감사초점 내용을 유형화하는 것이 필요하였다.

〈표 3-1〉 감사초점에 따른 국내외 IT감사체계 비교

기관	구분	내용
GAO	일반통제	기관의 전산업무 처리에 전체적으로 적용되는 정책, 절차, 구조(보안관리, 접근통제, 구성관리, 직무분리, 비상계획)
	어플리케이션 통제	개별적인 단위의 응용시스템과 관련된 자료의 입력, 처리, 결과에 대한 유효성, 적절성, 완결성, 정확성(어플리케이션 보안, 업무절차 통제, 인터페이스 통제, 데이터 관리 시스템 통제)
ISACA	계획 및 조직	IT전략계획, 정보구조, IT투자관리, IT인력관리, IT위험평가, 프로젝트 관리 등
	도입 및 구축	응용소프트웨어, 기술구조 도입 및 유지·보수, IT자원 조달 등
	운영 및 지원	서비스 수준 정의 및 관리, 시스템 보안성 확보, 비용 산정 및 배분, 사용자 교육 및 훈련, 시설 및 운영 관리 등
	모니터링 및 평가	IT성과, 내부통제 모니터링 및 평가, 외부요구사항과의 적합성 보증 등
INTOSAI	일반통제	직무분리, 물리적 접근통제, 논리적 접근통제, 운영 및 파일 통제, 변경관리 통제, 네트워크보안 통제, 업무지속계획 등
	어플리케이션 통제	문서기준, 입력통제, 처리통제, 출력통제, 마스터 및 대기데이터 파일 통제

기관	구분	내용
IIA	거버넌스	정책
	관리	기준, 조직 및 관리, 물리적인 환경통제
	기술	시스템 소프트웨어 통제, 시스템 개발 통제, 어플리케이션 통제
금융감독원	IT경영	IT부서 조직 및 인원, IT 관련 내규, IT계획 및 방향 제시, 비상계획, 경영정보시스템 등
	시스템개발 도입 및 유지·보수	인력, 내규, 현황, 내부통제용 시스템, 시스템 통합
	IT서비스 제공 및 지원	인력, 내규, 시설 및 장비, 보안, 통신망, 최종사용자 컴퓨팅, 전자금융거래 등
정보화진흥원	정보기술 아키텍처 수립사업	기반 정립, 아키텍처 구축, 품질보증활동, 이행계획 수립, 관리체계
	정보화전략 계획 수립사업	정보화계획, 업무, 기술, 품질보증활동
	시스템 개발사업	시스템구조, 응용시스템, 데이터베이스, 시험활동, 운영준비, 품질보증활동
	데이터베이스 구축사업	데이터 수집 및 시범구축, 데이터 구축, 품질검사
	시스템 운영사업	서비스 제공, 서비스 지원
	유지·보수	유지·보수
	사업관리	사업관리

감사초점의 유형화를 위한 기준 마련을 위하여 2가지 접근방법을 사용하였다. 먼저 정보화사업이나 전자정부사업을 대상으로 한 성과평가항목들을 참고하였다. IT감사의 대상이 정보화사업이고 감사초점 또한 정보화사업의 평가와 관련성이 높으므로 정보화사업에 대한 성과평가지표들을 검토하는 것은 IT감사사례 비교·분석을 위하여 타당성이 있다고 판단되었다. 이를 위하여 호진원·이미영(2008) 연구에서 제시한 표준평가항목들을 참고하였다. 그 이유는 성과평가지표와 관련하여 과거 정부업무평가위원회의 정보화성과지표(2006)와 정보화진흥원이 전자정부 로드맵 과제 표준성과지표(2005)를 통해 평가방법, 평가기준, 평가항목 등을 제시한 적이 있으나 이 연구에서

이러한 지표들의 문제점을 개선하여 대안으로 표준평가항목들을 제시하였고 설문조사를 통하여 이러한 항목들의 타당성을 검증한 바 있기 때문이다.

두 번째는 COBIT이 제시하는 감사초점내용들을 참고한 것인데, 앞에서 언급한 바와 같이 대부분 기관의 IT감사체계가 공통적으로 COBIT 기준을 참고하고 있으므로 COBIT에서 제시하고 있는 감사초점들과의 공통된 부분을 검토하였다.

이러한 2가지 접근방법을 통해서 얻은 공통된 감사초점을 본 연구의 IT감사사례 비교·분석을 위한 틀로서 사용하였다.

1. 표준성과평가항목의 개념 및 정의

먼저 호진원·이미영(2008)의 연구에서 제시한 표준성과평가항목들의 개념 및 정의를 알아보고, 이러한 평가항목들이 현행 IT 관련 국내법 체제하에서도 적용 가능한지를 검토하였다. 새 정부 들어서 정부조직이 개편되면서 추진체계 및 이를 지원하는 법이 변경되면서 개정된 법제도하에서 표준성과평가항목의 유효성을 재확인하는 것이 필요하다고 판단되었기 때문이다. 이 연구에서 제시한 표준평가항목은 총 12개로 기본적인 개념은 다음과 같다.

- **전략**: 전략은 기관의 전략 목표와 미션을 달성하기 위해 정보화사업에서 반드시 필요한 요소이다. 정보화사업을 시작하기 전에 반드시 점검해야 할 사항은 조직의 목표와 미션을 바탕으로 구체적인 필요성과 목적을 명확히 해야 한다는 것이다. 따라서 정부기관의 전자정부사업 전략은 '정보시스템 전략(Information System Planning)'과 반드시 연계되어야 한다. 또한 새로운 서비스 도입으로 인하여 발생하는 제반 문제를 관리적인 관점에서 다룰 필요가 있는데 리더십, 변화관리, 위험평가, 수요평가 등의 요소가 포함된다.

- **조직**: 조직은 보다 효율적인 전자정부 서비스를 제공하기 위하여 유연하게 대응할 수 있도록 조직 재설계가 필요하다. 일반적으로 전자정부 서비스는 서비스 내용이 하나의 정부 부처에만 국한된 것이 아니라 다수의 부처가 함께 공동 작업이 필요한 경우가 많으므로 다른 부처와의 협업체제를 잘 구축하여 원활한 공조체제를 이루는 것이 필요할 것이다. 따라서 조직 재설계와 타 기관 간의 협업체계 구축이 중요한 요소이다.
- **업무절차**: 업무절차는 전자정부 서비스 도입에 맞추어 업무절차를 재설계할 필요가 있다. 예를 들면 유사한 업무절차들을 통합하고 중복되거나 불필요한 업무절차들을 제거하며 새로이 필요한 프로세스를 정의하는 등 조직의 업무절차 재설계를 통해 새로운 시스템 기반으로 전환하여야 한다. 이러한 프로세스 재설계는 새롭게 도입되는 시스템의 활용을 활성화함으로써 업무생산성을 개선하는 데 기여하게 된다. 업무의 표준화, 업무처리 재설계, 기관 내 통합업무처리 등이 포함된다.
- **인력**: 정보화사업의 성공적인 구현을 위해서는 우수한 IT인력의 지식과 경험이 필요하다. 교육은 정보화사업의 근간을 이루는 시스템 관련 정보화 교육뿐만 아니라 시스템 활용의 적절성 및 보완의 필요성 등을 판단할 수 있는 전문적인 지식교육도 포함하여야 한다. 궁극적으로 조직의 IT역량을 키워나가는 데 초점을 맞추어야 할 것이며 업무역량, 정보화교육, 전문성 및 보상체계 등의 평가요소가 포함된다.
- **비용**: 비용은 정보화사업을 수행하는데 소요되는 사업 주관부처의 자본 지출, 운영비, 예산 등 정량적 부분을 측정하기 위한 것으로 일반기업과 달리 공공부문에서는 이윤 추구를 목표로 하는 것이 아니기 때문에 상대적으로 중요도가 떨어진다고 할 수 있다. 그러나 적정한 수준의 예산 수립과 비용통제는 정보화사업의 성공적인 수행에 필수적인 요인이기 때문에 평가요소로 포함되어야 한다.
- **편익**: 편익은 정보화사업을 진행해나가면서 주관부처에서 얻게 되는

비용절감 및 효율성 개선효과 등을 평가하기 위한 요소로서 정량적 지표와 정성적 지표가 모두 포함된다.

- **사용자 만족**: 사용자 만족은 정보화사업이 원래의 의도대로 잘 구현되었는지를 파악하기 위하여 우선적으로 사용자 만족도를 평가하는 평가요소이다. 사용자의 범위는 정보화사업의 수혜자를 모두 포함하는 것으로 일반 주민, 정부부처 내의 실제 사용자, 이해관계자 등 다양한 사용자 시각이 고려되어야 한다. 주로 정성적 평가로 구성되며 고객만족도, 맞춤서비스 제공 여부, 사용편리성 등이 평가요소에 포함된다.
- **사용자 참여**: 사용자 참여는 정부부처가 의도하는 여러 가지 정부활동에 대하여 사용자들이 참여하는 정도를 평가하는 것으로서 전자정부 서비스의 기능적 역할에 대한 평가기준이라 할 수 있다. 여기에는 정책 참여를 유도한다든지 정보의 접근성을 높이는 것 등이 평가요소가 된다.
- **표준화**: 전자정부 서비스를 통한 정보사용의 극대화를 위해서는 조직 내부를 비롯하여 외부와의 정보 공유 활동이 활발해야 하는데 이를 뒷받침할 수 있는 것은 시스템의 표준화를 통해서만이 가능하다. 따라서 표준화는 시스템 간의 중복된 기능을 최소화하고 시스템 간의 연동이 필요한 경우 보다 유연하게 시스템 연계가 가능하도록 해준다. 표준화된 시스템 구조와 모형을 채택하여 시스템 간의 연계성을 높이는 것은 부처 간의 협업체계를 보다 견고히 할 수 있는 기회를 제공하여 궁극적으로 시간 및 비용을 절감할 수 있도록 해준다.
- **보안**: 전자정부 서비스를 이용하는 사용자의 인적사항 등과 관련된 개인 사생활 정보를 보호해야 하며 이 서비스에서 제공되는 정보를 외부 침입자로부터 보호할 수 있어야 한다. 또한 외부로부터 정보시스템에 대한 해킹뿐 아니라 내부구성원에 의한 불법적인 정보유출 등에도 대비할 수 있어야 한다.
- **정보기술품질**: 정보기술품질은 전자정부 서비스를 제공하는 시스템의

질을 평가하는 것이다. 이는 전통적으로 경영정보시스템(Management Information System) 분야에서 주로 다루고 있는 것으로, 예를 들어 제공되는 정보의 시의성 및 정확성 등의 정보품질(information quality)을 평가하고 시스템 속도와 시스템 다운의 빈도 등 시스템 품질(system quality)을 평가한다. 또한 시스템의 관리를 담당하고 있는 전산부서가 제공하는 서비스의 품질(service quality)에 대한 평가도 포함된다.

- **인프라**: 인프라는 성공적인 전자정부 서비스 제공을 위해 필요한 시스템 기반의 구축 여부와 관련된 것으로 사용자가 웹사이트 한곳을 통하여 원하는 서비스를 받도록 하는 포털을 구축하였는지 여부, 시스템 통합 및 연계 정도, 재해복구계획의 수립 여부, 그리고 정보자원 관리의 수준 등을 평가할 수 있어야 한다.

2. 표준성과평가항목과 관련법 비교

이 12개의 표준성과평가항목을 주요 IT 관련 법인 「국가정보화기본법」, 「전자정부법」, 「정보시스템의효율적도입및운영등에관한법률」의 관련 법조항 및 내용과 비교하여 표준성과평가항목이 관련 법조항들을 충분히 반영하고 있는지를 확인하였다. 〈표 3-2〉에서 보는 바와 같이 주요 감사초점들이 관련 법 내용을 골고루 반영하고 있음을 확인할 수 있었다. 그러므로 12개의 표준성과평가항목은 현행 주요 IT 관련 법의 법적인 근거에 의해 검토할 중요한 감사초점으로 활용될 수 있을 것으로 판단된다.

〈표 3-2〉 표준성과평가항목과 관련 법조항과의 비교

표준성과 평가항목	관련 법조항	관련 법조항 내용
전략	● 「국가정보화기본법」[9] 제6조(국가정보화 기본계획의 수립)	○ "기본계획에는……국가정보화정책의 기본 방향 및 중장기 발전방향이 포함되어야 한다"
	● 「국가정보화기본법」 제7조(국가정보화 시행계획의 수립)	○ "중앙행정기관의 장과 지방자치단체의 장은 기본계획에 따라 매년 국가정보화 시행계획을 수립·시행하여야 한다"
	● 「국가정보화기본법」 제13조(정보화계획의 반영 등)	○ "사회간접자본시설사업 및 지역개발사업 등 대통령령으로 정하는 대규모 투자사업을 시행하려는 중앙행정기관의 장과 지방자치단체의 장은 해당 사업계획을 수립·시행할 때에는……정보화계획을 수립하여 최대한 반영하여야 한다"
	● 「전자정부법」 제45조(중장기 전자정부사업계획의 수립)	○ "중앙사무관장기관의 장은 전자정부의 구현을 위한 중장기 전자정부 사업계획을 정보화전략위원회의 심의를 거쳐 수립할 수 있다"
조직	● 「국가정보화기본법 시행령」[10] 제18조(국가기관 등 간의 정보 공동활용)	○ "국가기관 등의 장은……행정업무 처리 및 대국민서비스 제공에 활용도가 높은 데이터베이스를……국가기본 데이터베이스로 지정하고 다른 국가기관 등에 대하여 우선적으로 공동활용하게 할 수 있다"
	● 「전자정부법」 제8조(전자적 처리의 원칙)	○ "행정기관은 업무를 전자화하고자 하는 경우에는……처리과정 전반을 전자적 처리에 적합하도록 혁신하여야 한다"
	● 「전자정부법」 제24조(행정기관의 업무재설계)	○ "행정기관의 장은……정보통신기술을 도입하는 경우에는 기존의 조직 및 업무절차를 정보통신기술의 도입에 적합하도록 사전에 재설계하고 이를 시행하여야 한다"

9) 「국가정보화기본법」(시행 2009. 8. 23).
10) 「국가정보화기본법 시행령」(시행 2009. 8. 23).

표준성과 평가항목	관련 법조항	관련 법조항 내용
업무 절차	● 「국가정보화기본법」 제15조(공공정보화의 추진)	○ “국가기관 등은 행정업무의 효율성 향상……등을 위하여……정보화를 추진하여야 한다”
	● 「국가정보화기본법」 제22조(정보통신망의 상호 연동 등)	○ “국가기관과 지방자치단체가 정보통신망을 구축·운영하려는 경우에는 다른 기관의 정보통신망을 공동 활용하는 방안을 우선적으로 마련하여야 한다”
인력	● 「전자정부법」[11] 제4조(행정기관의 책무)	○ “소속 공무원에 대한 정보통신기술 활용능력의 제고 및 검정”
비용	● 「국가정보화기본법」 제4조(국가정보화 추진의 기본원칙)	○ “국가와 지방자치단체는 시책추진에 필요한 재원을 마련하기 위하여 노력하여야 한다”
	● 「전자정부법」 제13조(중복투자방지의 원칙)	○ “행정기관은 전자정부사업을 추진함에 있어서 다른 행정기관이 보유한 행정정보자원과의 상호연계 및 공동 이용 등을 통하여 중복투자가 되지 아니하도록 필요한 조치를 하여야 한다”
편익	● 「국가정보화기본법」 제15조(공공정보화의 추진)	○ “국가기관 등은……국민편익증진 등을 위하여……정보화를 추진하여야 한다”
	● 「국가정보화기본법」 제16조(지역 정보화의 추진)	○ “국가기관과 지방자치단체는 지역주민의 삶의 질 향상과 지역간 균형발전을 위하여……정보화를 추진할 수 있다”
	● 「전자정부법」 제6조(국민편익 중심의 원칙)	○ “행정기관의 업무처리과정은……민원인이 부담하여야 하는 시간과 노력이 최소화되도록 설계되어야 한다”
	● 「전자정부법」 제10조(행정기관 확인의 원칙)	○ “행정기관은 특별한 사유가 있는 경우를 제외하고……전자적으로 확인할 수 있는 사항을 민원인에게 확인하여 제출하도록 요구하여서는 아니된다”

11) 「전자정부법」(시행 2009. 8. 23).

표준성과 평가항목	관련 법조항	관련 법조항 내용
	● 「전자정부법」 제40조(문서업무의 감축)	○ "행정기관은……종이문서 등을 최대한 감축하여야 한다"
	● 「전자정부법」 제43조(감축실적의 공표)	○ "행정기관의 장은……감축대상문서의 감축실적을 반기별로 파악하여 이를 감축목표와 대비하여 인터넷에 공표하여야 한다"
사용자 만족	● 「국가정보화기본법」 제4조(국가정보화 추진의 기본원칙)	○ "국가와 지방자치단체는 국가정보화 추진과정에서……사회 각 계층의 다양한 의견을 수렴하도록 노력하여야 한다"
	● 「국가정보화기본법」 제41조(이용자의 권익보호 등)	○ "국가기관과 지방자치단체는 국가정보화를 추진할 때 이용자의 권익보호를 위한 시책을 마련하여야 한다"
	● 「전자정부법」 제4조(행정기관의 책무)	○ "전자정부의 운영과 관련한 국민 불만사항에 대한 확인 및 신속한 개선"
	● 「전자정부법」 제9조(행정정보 공개의 원칙)	○ "……행정정보로서 국민생활에 이익이 되는 행정정보는……인터넷을 통하여 적극적으로 공개되어야 한다"
사용자 참여	● 「국가정보화기본법」 제29조(정보문화의 창달)	○ "국가기관과 지방자치단체는 모든 국민이 국가정보화의 편익을 누릴 수 있도록 정보문화교육과 관련 인력의 양성, 콘텐츠 개발·보급 등의 시책을 마련하여야 한다"
	● 「국가정보화기본법」 제31조(정보격차 해소 시책의 마련)	○ "국가기관과 지방자치단체는 모든 국민이 정보통신서비스에 원활하게 접근하고 정보를 유익하게 활용할 수 있도록 필요한 시책을 마련하여야 한다"
	● 「국가정보화기본법」 제35조(정보격차 해소의 시행 등)	○ "국가기관과 지방자치단체는 정보격차의 해소를 위하여 필요한 교육을 시행하여야 한다"
	● 「전자정부법」 제28조(정보통신망을 통한 의견 수렴)	○ "행정기관은……행정예고를 하여야 하는 사항……공청회, 여론조사 등을 실시하도록 한 사항에 관하여는 정보통신망을 통한 의견수렴절차를 병행하여야 한다"

표준성과 평가항목	관련 법조항	관련 법조항 내용
표준화	● 「국가정보화기본법」 제21조(표준화의 추진)	○ "정부는 국가정보화를 효율적으로 추진하고 정보의 공동 활용을 촉진하며……호환성 확보 등을 위하여 표준화를 추진하여야 한다"
	● 「국가정보화기본법」 제26조(지식정보자원의 표준화)	○ "행정안전부 장관은 지식정보자원의 개발·활용 및 효율적인 관리를 위하여……표준화를 추진하여야 한다"
보안	● 「국가정보화기본법」 제37조(정보보호 시책의 마련)	○ "국가기관과 지방자치단체는 정보를 처리하는 모든 과정에서 정보의 안전한 유통을 위하여 정보보호를 위한 시책을 마련하여야 한다"
	● 「국가정보화기본법」 제39조(개인정보 보호 시책의 마련)	○ "국가기관과 지방자치단체는 국가정보화를 추진할 때……개인정보 보호를 위한 시책을 마련하여야 한다"
	● 「전자정부법」 제12조(개인정보 보호의 원칙)	○ "행정기관이 보유 관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다"
	● 「전자정부법」 제27조(정보통신망 등의 보안대책 수립·시행)	○ "행정기관의 장은……정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다"
정보기술 품질	● 「전자정부법」 제48조(정보화시스템의 보급·확산)	○ "중앙사무관장기관의 장은……정보화시스템 중 우수한 시스템을 다른 행정기관에 보급·확산시키기 위한 방안을 마련하여야 한다"
	● 「정보시스템의효율적도입및운영등에관한법률」[12] 제10조(상호운영성 확보 등을 위한 기술평가)	○ "공공기관의 장은……정보시스템의 상호운용 및 정보의 공동 활용, 정보시스템의 효율성, 정보접근을 위한 기술적 편의성에 관하여 사업계획 수립 시에 기술평가를 실시하여야 한다"
	● 「정보시스템의효율적도입및운영등에관한법률」 제11조(공공기관의 정보시스템 감리)	○ "공공기관의 장은……정보시스템 구축사업에 대하여 정보시스템 감리를 하게 하여야 한다"

12) 「정보시스템의효율적도입및운영등에관한법률」(시행 2008. 12. 26).

표준성과 평가항목	관련 법조항	관련 법조항 내용
인프라	● 「국가정보화기본법」 제18조(지식·정보의 공유·유통)	○ “국가기관 등은 국가정보화의 추진을 통하여 창출되는 각종 지식과 정보가 사회 각 분야에 공유·유통될 수 있도록 필요한 기반을 마련하여야 한다”
	● 「국가정보화기본법」 제25조(지식정보자원의 관리 등)	○ “국가기관과 지방자치단체는 지식정보자원을 효율적으로 관리하여야 한다”
	● 「국가정보화기본법」 제49조(초고속국가망의 관리 등)	○ “방송통신위원회는 비영리기관 등이 초고속국가망을 최소의 비용으로 이용할 수 있도록 필요한 시책을 강구하여야 한다”
	● 「국가정보화기본법」 제50조(광대역통합연구개발망의 구축·관리 등)	○ “방송통신위원회는 광대역통합정보통신망의 품질관리를 위하여 필요한 시책을 강구하여야 한다”
	● 「전자정부법」 제26조(정보통신망의 구축)	○ “행정기관은 정보통신망을 구축 운영하는 경우에……다른 행정기관의 정보통신망과 연계될 수 있도록 설계·운영하여야 한다”

3. 표준평가항목과 COBIT과의 비교·분석

대부분의 국내외 IT감사체계는 COBIT 모델을 참조하여 개발된 것이라고 설명하였다. COBIT의 기본 개념은 경영목적이나 요구사항을 지원하기 위하여 필요한 정보를 검토하는 데 목적을 두고 있다. COBIT 모델에서 제시하고 있는 4가지 업무영역은 ‘계획 및 조직’, ‘도입 및 구축’, ‘운영 및 지원’, ‘모니터링 및 평가’로 구분한다. 각각의 정의를 간단히 살펴보면, ‘계획 및 조직’은 IT가 조직의 목적 달성에 기여할 수 있는 방법을 제시하여 이를 관리하는 것이고, ‘도입 및 구축’은 IT전략을 실현하기 위해서 IT솔루션을 자체 개발하거나 도입해야 하고, 시스템의 변경 및 유지·보수가 포함된다. ‘운영 및 지원’은 운영, 보안, 교육훈련 등 필요한 서비스를 실질적으로 제공하는

것이고, '모니터링 및 평가'는 모든 IT프로세스를 시간이 흐름에 따라 품질과 통제요구사항의 준수성 측면에서 정기적으로 모니터링하고 평가하는 것이다. 이 4가지 업무영역은 총 34개의 업무 프로세스로 분류하며 이러한 각각의 프로세스 목적을 충족시키기 위해서는 정보에 대한 경영상의 요구사항이라고 부르는 특정한 기준을 만족시켜야 한다. 이를 정보기준(information criteria)라고 하는데 총 7개로 구분하고 있으며 각 정보기준의 정의는 아래와 같다.

'효과성(effectiveness)'은 정보가 업무 프로세스와 관련된 정도와 정보가 필요한 시기에 정확하고 일관성 있고 사용 가능한 형태로 제공되는 정도를 나타낸다. '효율성(efficiency)'은 정보를 제공하기 위해서 자원을 최적으로 (가장 생산적이고 경제적으로) 사용하는 정도를 의미한다. '기밀성'은 기밀을 요하는 정보를 불법 접근으로부터 보호하는 정도를 나타낸다. '무결성'은 정보의 정확성 및 완전성, 기업의 가치 및 기대를 충족시키는 정보의 타당성을 나타낸다. '가용성'은 현재 또는 미래에 업무 프로세스를 수행하면서 필요한 때에 정보가 가용한 정도를 의미하며, 필요한 자원과 관련된 기능을 보호하는 정도를 의미한다. '순응성(compliance)'은 업무 프로세스를 수행하는 과정에서 준수해야 할 법률, 규정 및 계약 등과 같은 외부 요건을 준수하는 정도를 나타낸다. 마지막으로 '신뢰성(reliability)'은 경영자들이 기업을 운영하고 재무 및 준수 보고 의무를 수행하는 데 필요한 적절한 정보를 제공하는 정도를 의미한다(나종필, 2005).

〈표 3-3〉은 프로세스와 정보기준의 관계를 파악하기 위하여 COBIT 개념모델 중의 일부를 수정하여 재작성한 것이다. 34개의 프로세스 중에 효과성과 효율성에 직접적인 영향을 주는 프로세스를 선택하였다. IT감사의 목적이 정보시스템의 효율성·효과성·경제성을 평가하는 것이기 때문에 7개의 요건 중 효과성과 효율성이 이를 만족시키는 관련성이 높은 요건으로 판단하였기 때문이다. 효과성과 효율성에 직접적인 영향을 주는 프로세스의 개수는 총 30개로 나머지 4개의 프로세스는 해당 프로세스와 관련이 없어 제

외하였다. 4개의 제외된 프로세스 중에서 '시스템 보안성 확보'는 COBIT이 정하는 효과성과 효율성과는 직접적인 연관이 없으나, 효과적인 보안관리가 보안의 취약성 및 사고를 최소화하고, 정보자원을 보호하여 궁극적으로 시스템의 효율화를 향상시킨다는 점에서 포함하였다. 따라서 표준성과평가항목과의 비교를 위하여 총 31개의 COBIT 프로세스를 추출하였다.

〈표 3-3〉 COBIT 4.0 모델(Tuttle & Vandervelde, 2007)

COBIT 프로세스	COBIT 정보기준						
	효과성	효율성	기밀성	무결성	가용성	순응성	신뢰성
계획 및 조직							
1. IT 전략계획 정의	●	●					
2. 정보구조 정의	●	●	●	●			
3. 기술 방향 결정	●	●					
4. IT 프로세스·조직·관계 정의	●	●					
5. IT투자 관리	●	●					●
6. 경영층의 관리 목표 및 방향 전파	●					●	
7. IT인력 관리	●	●					
8. 품질 관리	●	●		●			●
9. IT위험평가 및 관리	●	●	●	●	●	●	●
10. 프로젝트 관리	●	●					
도입 및 구축							
11. 자동화된 솔루션 도출	●	●					
12. 응용 소프트웨어 도입 및 유지·보수	●	●		●			●
13. 기술구조 도입 및 유지·보수	●	●		●	●		
14. 운영 및 이용 준비	●	●		●	●	●	●
15. IT자원 조달	●	●				●	
16. 변경 관리	●	●		●	●		●
17. 시스템 설치 및 테스트	●	●		●	●		
운영 및 지원							
18. 서비스 수준 정의 및 관리	●	●	●	●	●	●	●
19. 외부업체 서비스 관리	●	●	●	●	●	●	●
20. 성능 및 용량 관리	●	●			●		

COBIT 프로세스	COBIT 정보기준						
	효과성	효율성	기밀성	무결성	가용성	순응성	신뢰성
21. 서비스의 지속성 확보	●	●			●		
22. 시스템 보안성 확보			●	●	●	●	●
23. 비용 산정 및 배분	●						●
24. 사용자 교육 및 훈련	●	●					
25. 고객지원 및 사고 관리	●	●					
26. 구성 관리	●	●			●		●
27. 문제 관리	●	●			●		
데이터 관리				●			●
시설 관리				●	●		
28. 운영 관리	●	●		●	●		
모니터링 및 평가							
29. IT성과 모니터링 및 평가	●	●	●	●	●	●	●
30. 내부통제 모니터링 및 평가	●	●	●	●	●	●	●
외부 요구사항과의 적합성 보증							
31. IT 거버넌스 제공	●	●	●	●	●	●	●

〈표 3-4〉에서 보는 바와 같이 전반적으로 COBIT 프로세스는 정보기술품질이 총 13개로 가장 많았고, 그 다음이 전략으로 6개, 조직·비용·사용자 만족·인프라 등이 각각 2개의 프로세스와 관련이 있는 것으로 나타났다. 그리고 'IT 프로세스·조직·관계 정의'는 조직과 프로세스 모두에 해당하므로 2개 부문에 중복하여 분류하였고, 마찬가지로 'IT투자관리'도 각각 비용과 편익부문에 해당하므로 중복하여 분류하였다. 정보기술품질에서 '응용소프트웨어 도입 및 유지·보수', '외부업체 서비스 관리', '서비스의 지속성 확보' 등은 계약이나 구매와 관련된 부분이라고 할 수 있다. 우리나라 정부부처의 경우 부서 내에서 자체적으로 시스템을 개발하는 경우는 거의 없고 대부분 외주용역을 주는 것이 일반화되어 있어 외주용역계약에서 특히 위에 언급한 항목들은 궁극적으로 시스템의 품질 제고에 중대한 영향을 미치기 때문에 정보기술품질항목에 포함시켰다.

12개의 표준성과평가항목과 COBIT 프로세스를 비교한 결과 COBIT 프로세스는 12개의 표준성과평가항목을 골고루 반영하고 있는 것으로 확인되었다. 이중에서 전략, 조직, 업무절차, 인력, 비용, 편익, 사용자 만족, 사용자 참여 등 8개 항목은 일반통제에 해당된다고 볼 수 있으며, 표준화, 보안, 정보기술품질, 인프라 등 4개 항목은 어플리케이션 통제에 포함된다.

〈표 3-4〉 표준성과평가항목과 COBIT 프로세스 비교

표준성과 평가항목	COBIT 프로세스	개수
전략	IT전략계획 정의, 기술방향 결정, 경영층의 관리 목표 및 방향 전파, IT위험평가 및 관리, 프로젝트 관리, IT거버넌스 제공	6
조직	IT프로세스·조직·관계 정의, 내부 모니터링 및 평가	2
프로세스	IT프로세스·조직·관계 정의	1
인력	IT인력 관리	1
비용	IT투자 관리, 비용산정 및 배분	2
편익	IT투자 관리	1
사용자 만족	고객지원 및 사고 관리, 문제 관리	2
사용자 참여	사용자 교육 및 훈련	1
표준화	정보구조 정의	1
보안	시스템 보안성 확보	1
정보기술품질	품질관리, 자동화된 솔루션 도출, 응용소프트웨어 도입 및 유지·보수, 기술구조 도입 및 유지·보수, 운영 및 이용 준비, 변경관리, 시스템 설치 및 테스트, 서비스 수준 정의 및 관리, 외부업체 서비스 관리, 성능 및 용량 관리, 서비스의 지속성 확보, 운영 관리, IT성과 모니터링 및 평가	13
인프라	IT자원 조달, 구성 관리	2

다음 절에서는 GAO의 FISCAM 등 6개 기관의 IT감사기준과 정보화사업 및 전자정부사업 평가와 관련한 문헌연구로부터 일반통제 8개와 어플리케이션 통제 4개 등 총 12개의 IT감사의 공통적인 감사중점사항을 비교·분석의

틀로 사용하여 국내외 최고감사기구의 IT감사보고서를 토대로 IT감사 사례를 검토하여 12개의 주요 IT감사초점과 어느 정도 연관성을 갖고 있는지 비교·분석하고자 한다.

- **일반통제**
  - 전략, 조직, 업무절차, 인력, 비용, 편익, 사용자 만족, 사용자 참여
- **어플리케이션 통제**
  - 표준화, 보안, 정보기술품질, 인프라

이를 위하여 감사원, GAO, NAO, ANAO, OAG 등 총 5개 최고감사기구의 최근 IT감사보고서의 내용을 검토하였다. 또한 각 감사사례별 감사방법과 관련된 특징을 파악하고, 아울러 각 최고감사기구가 전체 감사에서 IT감사가 차지하는 비중을 연도별로 비교하였다. 국내외 최고감사기구의 IT감사사례를 분석하기 위하여 2008년에서 2009년 IT 관련 감사보고서를 각 기관별 웹사이트에서 검색하여 추출하였다. 우리 감사원의 경우 전체적으로 2003년부터 7건의 IT감사사례가 있었으나 2008년과 2009년의 5건만 비교를 위해 포함하였다. GAO의 경우는 2008년만 39건의 IT감사사례가 있었으나 2009년 9건만 포함시키고 2008년 자료는 제외하였다.

제2절 감사원

감사원의 IT감사는 전산감사라는 용어를 사용하고 있는데 전산감사의 정의를 살펴보면 전산감사란 감사대상에서 독립된 객관적인 입장에서 컴퓨터를 중심으로 하는 정보처리시스템을 종합적으로 점검·평가하여 관계자에게 조언·권고하는 것을 말하며, 그 시스템의 유효 이용을 촉진하는 한편 그 폐해의 제거도 동시에 추구하여 시스템의 건전화를 도모하는 것이다. 따라서 전산감사는 전통적인 감사목적인 자산보호 목적과 자료보존 목적인 입증목적뿐만 아니라 관리목적을 효율적·효과적으로 달성할 수 있도록 지원하는 것을 말한다(장태범·김문오, 2004). 감사원의 경우 2003년 이후 2009년까지 주요 IT 관련 감사보고서는 총 7건으로 확인되었다. 아래 〈표 3-5〉에서 보는 바와 같이 각 감사보고서별 감사초점을 비교·분석 틀과 비교하였다. 그 결과 대체로 전략과 정보기술품질 등에 감사초점을 두고 있는 것으로 나타났다. 감사방법에 있어서는 감사보고서에 어떤 감사접근방법을 사용하였는지 뚜렷하게 언급한 부분이 없다는 것이 공통된 특징이다. 다만, 2003년 보고서에는 자료의 출처 등이 불분명하였으나, 2005년 보고서에서는 자료의 출처를 파악할 수 있었고, 2008년 보고서부터는 관련 법이나 지침 등을 분명히 밝히고 이를 근거로 감사가 실시되었음을 알도록 작성한 것이 특징이다.

〈표 3-5〉 감사원의 IT감사사례

감사보고서	감사초점	감사방법
전자정부 구현사업 추진 실태(2003)	사업추진체계 평가**(조직)**	명시적으로 감사방법에 대한 설명은 없으나 판단기준으로 관련 법을 제시
	예산 지원의 적정성**(비용)**	
	사업간 연계성 확보**(인프라)**	
	중복투자 방지**(비용)**	
	정보보안의 적정성**(보안)**	
	시스템 구성의 안정성**(표준화)**	

감사보고서	감사초점	감사방법
전자정부사업 추진 실태(2005)	정보시스템의 효율적 통합·운용 여부**(인프라)**	명시적으로 감사방법에 대한 설명은 없으나 검토자료의 출처 제시
	행정정보의 기관간 원활한 공동 활용 여부**(표준화)**	
	전자정부 구현을 위한 인프라 구축의 적정성**(인프라)**	
통합지휘 무선통신망 구축 실태(2008)	사업추진방식의 적정성**(전략)**	명시적으로 감사방법에 대한 설명은 없으나 검토자료의 출처, 판단기준으로 해당기관의 사업계획서, 관련 법, 규정, 지침 등을 구체적으로 제시
	사업의 경제성**(비용, 편익)**	
	사업의 당초 목적 달성 가능성 여부**(전략)**	
	계약체결과정의 적법성 및 공정성**(정보기술품질)**	
	계약이행 및 감독의 적정성**(정보기술품질)**	
행정정보 공유 및 관리 실태(2008)	행정정보의 공동이용 기반 정비**(인프라)**	명시적으로 감사방법에 대한 설명은 없으나 검토자료의 출처, 판단기준으로 해당기관의 사업계획서, 관련 법, 규정, 지침 등을 구체적으로 제시
	개인정보 보호체계 강화**(보안)**	
	개인정보 관리에 대한 확고한 신뢰 확보**(사용자 만족)**	
	행정정보 공동이용 확대**(표준화)**	
	행정정보시스템 개선**(정보기술품질)**	
e-호조(지방재정관리시스템) 구축사업 추진 실태(2009)	e-호조 사업계획 수립 점검**(전략)**	명시적으로 감사방법에 대한 설명은 없으나 검토자료의 출처, 판단기준으로 해당기관의 사업계획서, 관련 법, 규정, 지침 등을 구체적으로 제시
	e-호조 사업계약 체결 점검**(정보기술품질)**	
국가정보화 및 전산화사업 추진 실태(2009)	사업계획의 적정성**(전략)**	명시적으로 감사방법에 대한 설명은 없으나 검토자료의 출처, 판단기준으로 해당기관의 사업계획서, 관련 법, 규정, 지침 등을 구체적으로 제시
	계약 체결의 적정성**(정보기술품질)**	
	중복투자 여부 점검**(비용, 편익)**	
	통합·연계 미흡**(표준화)**	
	정보시스템 부실 개발**(정보기술품질)**	
	활용이 저조한 시스템의 활용률 제고 방안 강구**(정보기술품질)**	

감사보고서	감사초점	감사방법
국가전자조달시스템 운영 실태(2009)	전자조달시스템이 입찰의 공정성을 담보하였는지 여부**(전략)**	명시적으로 감사방법에 대한 설명은 없으나 검토자료의 출처, 판단기준으로 해당기관의 사업계획서, 관련 법, 규정, 지침 등을 구체적으로 제시
	전자조달시스템 구축 시 입찰의 공정성을 확보할 수 있도록 하였는지 여부**(전략)**	
	공정성 확보를 위한 제도 운영의 적정성**(전략)**	
	전자조달시스템을 이용한 입찰에서 불법행위 여부**(전략)**	

감사원의 IT감사비율은 감사원 홈페이지에 등록되어 있는 연도별 감사결과 처분요구서 중 감사분야에서 '정보통신'을 조건으로 검색하여 나온 결과를 바탕으로 작성한 것이다. 다만, 2008년도에는 검색결과 전체 9건 중에 한국정보보호진흥원, 한국정보사회진흥원, 한국방송공사 등 총 7건의 기관운영감사는 직접적으로 IT를 대상으로 한 감사유형이 아니므로 제외하였다.

전체적으로 감사원의 IT감사비율은 6년간 평균 1.1%에 그치고 있다. 그만큼 IT감사 비중이 다른 감사유형보다 높지 않다는 것이 확인되었고, 또한 다른 해외 최고감사기구와 비교하였을 때 가장 낮은 비율인 것으로 나타났다.

〈표 3-6〉 감사원의 IT감사비율

연도	2003	2004	2005	2006	2007	2008
감사보고서 수	49	91	52	47	74	199
정보 또는 IT 관련 감사보고서 수	0	2	0	1	0	2
비율 (평균: 1.1%)	**0%**	**2.2%**	**0%**	**2.1%**	**0%**	**1.0%**

제3절 미국 GAO

미국 GAO는 다양한 형태의 IT감사를 실시하고 있는데 대표적으로 재무시스템(financial system), 전자정부와 IT시스템의 현대화 정책, IT구매 및 개발, 시스템 및 소프트웨어 개발 절차 등을 대상으로 감사를 실시하고 있다(IntoIT, 2006b). GAO의 IT감사사례를 보면 사용자 만족과 사용자 참여를 제외한 나머지 10개 감사초점을 고르게 활용하는 것으로 나타났으며 그중 전략, 정보기술품질, 인력, 보안 등의 분야에 감사초점을 두고 IT감사를 실시하는 것으로 파악되었다. GAO는 감사보고서 내에 구체적으로 어떠한 방법으로 감사를 하였는지 그 내용을 포함하여 어떤 기준에 의하여 감사가 이루어졌는지 확인할 수 있다.

〈표 3-7〉 GAO의 IT감사사례

감사보고서	감사초점	감사방법
"Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls"(2009)	전에 발견한 정보보안의 취약점에 대한 개선여부 점검**(보안)**	- FISCAM 등 관련 기준 및 지침 이용 - FISMA[13] 법조항 검토 - GAO의 지난 감사보고서 검토 - 보안담당자 및 임원 인터뷰
	주요 재정시스템의 효과성 여부**(정보기술품질)**	
	증권거래위원회의 위험평가 검토**(전략)**	
	보안교육 기록 검토**(인력)**	
"Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization" (2009)	투자 관리**(비용, 편익)**	- IT투자관리 프레임워크 등 참조 - 최고운영책임자 등 임원 인터뷰 - FDA 외부의 이해관계자 인터뷰
	프로젝트 관리**(전략)**	
	정보보안**(보안)**	
	EA(Enterprise Architecture) 개발**(인프라)**	
	인력자본 관리**(인력)**	

13) FISMA(Federal Information Security Management Act)는 미국정부가 전자정부의 정보보호를 강화하기 위하여 제정한 법으로 보안에 대한 규정을 제시하고 있다.

감사보고서	감사초점	감사방법
“Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weakness” (2009)	정보보안정책의 적정성 및 효과성**(전략)**	- FISMA 법조항 검토 - OMB FISMA 보고서 검토 - FISCAM 등 지침 검토 - OMB, 평가기관과의 회의
	FISMA 요구사항에 따른 구축 정도 평가**(보안)**	
“Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data” (2009)	정보보안정책의 실효성 제고**(전략)**	- FISMA 법조항 검토 - FISCAM 등 지침 검토 - 보안 담당자 및 임원 등 인터뷰 - GAO의 지난 감사보고서 검토
	시스템 위험평가**(전략)**	
	보안교육 기록 검토**(인력)**	
	어플리케이션, 데이터베이스, 네트워크 통제 평가**(정보기술품질)**	
	정보시스템에 대한 접근통제 평가**(보안)**	
“Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS”(2009)	전에 발견한 정보보안의 취약점에 대한 개선 여부 점검**(보안)**	- GAO의 지난 감사보고서 검토 - FISCAM 등 관련 기준 및 지침 이용 - FISMA 법조항 검토 - 보안담당자 및 임원 인터뷰
	주요 재정 및 조세시스템의 효과성 여부**(정보기술품질)**	
	IRS의 위험평가 검토**(전략)**	
	보안교육 기록 검토**(인력)**	
“Information Technology: DOD Needs to Strengthen Management of Its Statutorily Mandated Software and System Process Improvement Efforts” (2009)	소프트웨어 구매 및 개발 등과 관련 절차 개선 여부**(정보기술품질)**	- 관련 지침, 계획서 등 서류 검토 - 관련 책임 담당자 인터뷰 - 관련 법과 지침 비교 - 차이 나는 부분에 대한 책임 담당자 인터뷰 재확인 - GAO의 지난 감사보고서 검토 - DOD의 내부감사보고서 검토
	DOD의 절차 개선 노력 효과 분석**(정보기술품질)**	
	중복투자 여부 점검**(비용, 편익)**	
	통합·연계 미흡**(표준화)**	
	정보시스템 부실 개발**(정보기술품질)**	
	활용이 저조한 시스템의 활용률 제고 방안 강구**(정보기술품질)**	
“Electronic Health Records: DOD’s and VA’s Sharing of Information Could Benefit from Improved Management”(2009)	두 기관 간의 건강정보(health information) 공유 노력 점검**(표준화)**	- 관련 법조항 검토 - 연방정부 상호호환기준, 구축 사양, 인증기준 검토 - 관련 담당임원 등 인터뷰 - GAO의 지난 감사보고서 검토
	두 기관의 건강기록시스템 개발계획 평가**(전략)**	
	기관 간 조정업무를 담당하는 기구(Interagency Program Office)의 운영 실태 점검**(조직)**	

감사보고서	감사초점	감사방법
“Information Technology: Federal Agencies Need to Strengthen Investment Board Oversight of Poorly Planned and Performing Projects”(2009)	연방부처 내 투자심의위원회(IRB)의 정보기술 관련 운영 실태 점검**(조직)**	- 관련 법조항 검토 - 관련 지침 및 기준 검토 - 투자검토보고서 확인
	감독기능 점검을 위한 프로젝트 비용**(비용)**, 편익**(편익)**, 프로젝트 일정**(전략)**, 위험 데이터 조사**(전략)**	
“Information Technology: HUD Needs to Strengthen Its Capacity to Manage and Modernize Its Environment”(2009)	IT전략계획**(전략)** 검토 및 성과평가**(정보기술품질)**	- IT전략계획서 검토 - 관련 담당자 인터뷰 - GAO 및 해당기관의 IT 투자기준 검토 - IT인력관리계획서 검토 - GAO의 지난 감사보고서 검토 - 관련 기준 및 지침 검토
	IT투자관리 평가**(비용, 편익)**	
	IT인력자본 관리**(인력)**	
	시스템 구조 개발 및 활용**(표준화)**	
	관리 현대화를 위한 책임성 확보**(프로세스)**	

한편, 미국 GAO는 연간 약 1,000개의 감사보고서를 발표하고 있는데 이 중에서 약 50개 내외(전체 5%) 정도가 정보관리(Information Management) 분야에 해당되는 것으로 파악되어 6년 평균 IT감사 비중이 4.8%이나 다른 분야에서도 기본적으로 IT와 관련된 감사를 실시하고 있는 사례를 발견할 수 있어 GAO가 실시하는 감사의 10% 정도는 IT를 대상으로 하는 감사라고 할 수 있다. IT감사를 담당하는 인원은 전체 직원 수 3,250명 중에 106명으로 전체 인원수의 4%가 IT감사 전문인력으로 구성되어 있다(Mitsubishi UFJ Research and Consulting, 2009).

〈표 3-8〉 GAO의 IT감사비율

연도	2003	2004	2005	2006	2007	2008
감사보고서 수	963	923	894	1,000	1,008	1,013
정보관리 관련 감사보고서 수	49	56	42	48	40	39
비율(평균: 4.8%)	**5.1%**	**6.1%**	**4.7%**	**4.8%**	**4.0%**	**3.8%**

제4절 영국 NAO

영국 NAO는 2003년부터 주요 영국 정부부처의 IT기능에 대한 별도의 검토를 수행해오고 있다. 주요 검토사항으로는 IT의 최상위 조직과 부처가 IT 시스템을 어떻게 사용하고 관리하는지에 초점을 맞추고 있다. 특히 NAO는 IT거버넌스 이슈들을 감사계획단계의 한 부분으로 고려하고 있는 점이 특징적이다. 이러한 IT거버넌스 이슈들은 업무의 이해 차원에서 검토되고 있다. NAO는 IT거버넌스 검토를 위한 정식적인 방법론을 사용하고 있지 않지만 주로 ISACA의 COBIT에서 추천하고 있는 내부통제들을 이용하고 있다. IT거버넌스 검토결과는 대중에게 공개되지는 않고 각 부처의 감사위원회에 제출되며, 권고사항 이행은 각 부처의 내부감사에 의해 모니터링되고, 감사위원회에 보고된다. IT거버넌스 검토는 IT전문지식을 가지고 있는 IT 전문감사인이 수행할 필요는 없고, 대신 필요한 조언을 제공하고 있다(IntoIT, 2007).

NAO의 IT감사사례를 보면 감사의 품질 제고를 위해 외부전문가를 많이 활용하고 있다는 점과, 감사기관의 입장뿐만 아니라 관련 있는 이해관계자 등 다양한 시각을 반영하려는 것이 특징적이다. 또한 외부컨설팅기관과 외주계약을 맺고 감사업무의 일부분을 대행하도록 하고 있다.

〈표 3-9〉 NAO의 IT감사사례

감사보고서	감사초점	감사방법
"The Defense Information Infrastructure(DII)"(2008)	DII 개발을 위한 전략 검토**(전략)**	- 관련 문서 검토 - 이해관계자 포함 관련자 인터뷰 - 재무자료 및 비재무자료를 이용한 정량분석 - DII가 설치된 사이트 방문 - 해외 벤치마킹(미국) - 감사품질보증을 위한 외부전문가 검토 - NAO의 지난 감사보고서 검토
	IT투자 수준 평가**(비용, 편익)**	
	시스템 구축 진척도 점검**(전략)**	
	주요 소프트웨어 기능 점검**(정보기술 품질)**	
	DII를 통한 어플리케이션 접근성 점검**(보안)**	

감사보고서	감사초점	감사방법
"The National Program for IT in the National Health Service(NHS)"(2008)	사업진행의 적정성**(전략)**	- 관련자 인터뷰 - 주요 관련 문서 검토 - 관련 사이트 방문 - 외부기관의 자문(영국의학협회 등) - 감사품질 보증을 위한 외부전문가 검토(MIT 등)
	사업의 예상 비용의 적정성**(비용)**	
	사업의 예상 편익분석**(편익)**	
	시스템의 기술적 성과평가**(정보기술 품질)**	
"The National Offender Management Information System"(2009)	국가범죄자관리서비스(National Offender Management Service)의 가치(value for money) 평가**(비용, 편익)**	- 관련 문서 검토 - NAO 등 지침 참조 - 이해관계자 자문 - 관련자 인터뷰 - 재무자료 및 비재무자료를 이용한 정량분석 - 내부감사자료 검토
	초기 사업에 대한 의사결정의 적정성**(전략)**	
	임원진의 프로젝트 참여도 검토**(전략)**	
	주요 일정에 따른 프로젝트 진행 상황 점검**(전략)**	
	목적 달성을 위한 기술적인 타당성 검토**(정보기술품질)**	

영국 NAO는 연간 약 70~90개의 감사보고서를 발표하는데 감사제목에 정보 또는 IT가 포함되어 있는 보고서 수는 대략 연간 5개 미만으로 6년 평균 IT감사 비중이 전체의 약 3.1% 정도를 차지하고 있지만 미국과 마찬가지로 IT와 연관된 감사도 실시하는 사례가 있으므로 IT감사 비중은 약 5% 정도로 파악된다(Mitsubishi UFJ Research and Consulting, 2009).

〈표 3-10〉 NAO의 IT감사비율

연도	2003	2004	2005	2006	2007	2008
감사보고서 수	71	71	72	98	90	90
정보 또는 IT 관련 감사보고서 수	3	1	0	5	4	3
비율(평균: 3.1%)	**4.2%**	**1.4%**	**0%**	**5.1%**	**4.4%**	**3.3%**

제5절 호주 ANAO

호주 ANAO의 IT감사팀은 결산/재무감사 서비스그룹(Assurance Audit Services Group)의 한 부분으로 모든 감사팀에 종합적인 지원업무를 제공한다. 즉, 결산/재무감사 서비스그룹 외에 또 다른 성과감사 서비스그룹(Performance Audit Services Group)에도 동일한 지원업무를 수행한다. IT감사팀의 주요 목적은 호주 정부부처가 기존의 기술과 새로 도입할 기술에 대한 위험을 발견하고 평가하는 일련의 독립적인 정보기술 보증(assurance) 기능을 제공한다(IntoIT, 2005).

2008년 현재 IT감사팀 정규직 인원은 2005년 17명에서 6명이 증가한 23명이고, 다양한 교육 및 업무 경험을 보유하고 있다(IntoIT, 2008).

IT감사사례의 특징을 살펴보면 ANAO의 2008년과 2009년 IT감사사례가 주로 전략과 정보기술품질에 감사초점이 주로 편중되어 있음을 알 수 있다. 이외 보안과 사용자 만족 등이 있지만 나머지 감사초점은 없는 것으로 나타났다. NAO와 마찬가지로 인터뷰를 할 때 이해관계자를 포함하여 다양한 시각을 반영하려고 노력하고 있으며, 특히 전산감사기법을 이용한 IT감사를 수행한다는 것이 특징적이다. 그리고 관련 법이나 지침 등을 참조한 감사접근방법은 GAO나 NAO처럼 직접적으로 명시하지 않아 확인할 수 없었다.

〈표 3-11〉 ANAO의 IT감사사례

감사보고서	감사초점	감사방법
“Management of Personnel Security - Follow-up Audit”(2008)	부처 구성원의 보안에 대한 보안지침 준수 여부 점검**(보안)**	- 보안지침 검토 - 보안 관련 문서 검토 - 보안 관련 담당자 인터뷰 - 지난 ANAO 감사보고서 권고사항에 대한 개선 여부 파악

감사보고서	감사초점	감사방법
"DIAC(Department of Immigration and Citizenship)'s Management of the Introduction of Biometric Technologies"(2008)	DIAC의 생체인식기술 사업검토과정의 적정성**(전략, 비용, 편익)**	- 외부전문가 자문을 통한 감사 기준(criteria) 개발 - 관련 임원 및 담당자 인터뷰 - ANAO IT감사 전문가 활용 - 외부기관 자문 - 관련 문서 검토
	DIAC의 생체인식기술 권한의 적정성**(보안)**	
	DIAC의 생체인식기술 IT거버넌스 적정성**(전략)**	
	DIAC의 생체인식기술 프로젝트 관리의 적정성**(전략)**	
	DIAC의 생체인식기술 시스템 개발의 적정성**(정보기술품질)**	
"Government Agencies' Management of their Websites"(2008)	웹사이트 관리의 적정성 평가**(정보기술품질)**	- 40개 기관에 대한 설문조사 실시 - 부처 웹사이트 관리 문서 평가를 위해 ANAO가 직접 개발한 의사결정트리(decision tree)를 이용 웹사이트 기능과 관련된 위험 수준 분류 - 웹사이트에 대한 적절성, 범위, 적시성, 조직목표와의 연계성 평가
	웹사이트 위험관리 및 계획 점검**(전략)**	
	웹사이트 정책 점검**(전략)**	
	웹사이트 콘텐츠 관리 절차 점검**(정보기술품질)**	
	웹사이트 성과 모니터링 및 보고 체계 점검**(정보기술품질, 비용)**	
	웹사이트 상세개발 및 테스팅 점검**(정보기술품질)**	
	웹사이트 기술지원 점검**(사용자 만족)**	
	웹사이트 보안 점검**(보안)**	
"Quality and Integrity of the Department of Veteran's Affairs**(**DVA) Income Support Records"(2009)	소득지원기록의 질과 무결성 점검**(정보기술품질)**	- 데이터추출 프로그램을 이용하여 약 26만 건의 소득지원기록 추출 - 전산감사기법을 이용하여 데이터의 질과 무결성 평가 - 관련 서류 검토 - 이해관계자 인터뷰 - 담당자 인터뷰
	DVA의 데이터 관리 점검**(정보기술품질)**	
	서비스 제공 및 고객지원에 관련 데이터의 질의 영향 점검**(사용자 만족)**	
"Management of the Movement Alert List (MAL)"(2009)	이민·시민권부[14]의 입국제한리스트(MAL) 데이터베이스 관리의 효과성 점검**(정보기술품질)**	- MAL 운영과 관련된 담당자와 타 부처 공무원 인터뷰 - 전산감사기법 이용
	MAL의 접근통제 점검**(보안)**	
	MAL의 개인 사생활보호 기능 점검**(보안)**	

14) Department of Immigration and Citizenship(DIAC).

호주 ANAO는 연간 약 60~90개의 감사보고서를 발표하고 있는데 2003년과 2007년에는 IT감사를 실시하지 않은 것으로 나타났으나 IT감사를 실시한 해에는 IT감사 비중이 GAO나 NAO보다 높은 것으로 파악되었다.

〈표 3-12〉 ANAO의 IT감사비율

연도	2003	2004	2005	2006	2007	2008
감사보고서 수	59	59	52	53	91	93
정보 또는 IT 관련 감사보고서 수	0	7	6	2	0	6
비율(평균: 5.6%)	**0%**	**11.9%**	**11.5%**	**3.8%**	**0%**	**6.5%**

제6절 캐나다 OAG

캐나다 OAG는 별도의 IT감사조직이 있는 것이 아니라 재무감사나 성과감사팀 내에 있으면서 그들의 감사를 수행하고 IT와 관련된 전문지식과 자원을 OAG 내 모든 다른 팀에게 제공하는 지원기능을 수행한다. 다시 말해 IT감사는 모든 감사업무의 한 부분이며 일반적인 감사보고서에 항상 포함되는 중요한 구성요소이다(IntoIT, 2006a). 이에 따라 2008년 현재 IT감사 전담인력을 6명에서 17명으로 증원하였다. IT감사인은 재무감사에서 자동화된 통제의 효과성을 평가하고, 결산검사(attest audit)팀의 재무감사를 지원하는 역할을 한다. 또한 성과감사에서는 범정부적인 IT감사를 수행하고, 성과감사에 있어서 IT와 관련된 사항이나 전산감사기법 등에 대해 다른 팀을 지원한다. IT감사팀은 매년 하나의 범정부적인 IT 관련 보고서를 의회에 제출하는데, 이것이 5~10개 부처의 성과감사 및 공기업 감사에 기여한다. 또한 대부분의 재무감사의 지원도 담당하고 있다.

OAG의 IT감사사례를 보면 감사초점이 전략과 정보기술품질에 집중되어 있음을 확인할 수 있었고, 감사방법은 특별히 다른 기관과 상이한 점은 발견하지 못하였다.

〈표 3-13〉 OAG의 IT감사사례

감사보고서	감사초점	감사방법
"Managing Severe Weather Warnings: Environment Canada" (2008)	기상경보시스템의 전략적 방향의 적정성 점검 **(전략)**	- 관련 문서 검토 - 관련자 인터뷰 - 관련 사이트 방문 - 해외 벤치마킹 - 관련 기준 및 지침 참조
	기상관측 네트워크 관리의 적정성 점검**(정보기술품질)**	
	새로 구현된 기상 워크스테이션의 적정성 점검 **(정보기술품질)**	
	기상경보 제공 및 검증의 적정성**(정보기술품질)**	
	기상경보에 대한 사용자 요구사항 반영 적정성 여부 점검**(사용자 만족)**	

감사보고서	감사초점	감사방법
“Managing Environmental Programming: Agriculture and Agri-Food Canada” (2008)	국토 및 수자원 정보서비스(National Land and Water Information Service) 프로젝트 관리의 적정성 점검**(전략)**	- COBIT 등 지침 검토
“Managing Information Technology Investments: Canada Revenue Agency(CRA)” (2008)	캐나다 국세청(CRA)의 IT투자관리의 적정성 점검**(비용, 편익)**	- 관련 문서 검토 - 관련자 인터뷰 - 관련 사이트 방문 - 관련 기준 및 지침 참조
	IT투자와 조직목표와의 연계성 점검**(전략)**	
“Managing Identify Information”(2009)	4개 기관의 신원정보 데이터베이스 관리의 적정성 점검**(정보기술품질)**	- 관련 문서 검토 - 관련자 인터뷰 - 데이터 전송 분석 - 데이터 분석 - 프로세스 점검
	신원정보 데이터 베이스 정보공유 유도**(표준화)**	

캐나다 OAG의 감사보고서의 경우는 1건당 하나의 보고서가 만들어지는 것이 아니라 여러 건을 하나의 감사보고서에 포함시키는 관계로 하나의 보고서 안에 여러 IT감사사항이 포함된 경우라도 이를 하나의 IT감사보고서로 인정하였다. 예를 들어 1개의 감사보고서에 6개의 서로 다른 IT감사사항이 있는 경우, 이를 6개의 감사보고서로 계산한 것이다. OAG의 IT감사비율은 6년 평균 10.6%로 GAO·NAO·ANAO보다 높은 것으로 나타났다.

〈표 3-14〉 OAG의 IT감사비율

연도	2003	2004	2005	2006	2007	2008
감사보고서 수	29	22	30	26	24	24
정보 또는 IT 관련 감사보고서 수	2	2	2	2	4	4
비율(평균: 10.6%)	**6.9%**	**9.1%**	**6.7%**	**7.7%**	**16.7%**	**16.7%**

제7절 비교·분석결과

우리 감사원을 포함한 5개 최고감사기구의 공통된 감사초점은 주로 '전략', '비용', '편익', '정보기술품질' 등의 순서로 나타났다.

기관별 감사초점의 특징을 살펴보면 우리 감사원의 경우 최근 몇 년 동안의 IT감사사례를 검토한 결과 '전략(33%)'과 '정보기술품질(29%)'에 주로 집중한 것으로 나타났다. GAO의 경우는 '전략(23%)'과 '정보기술품질(19%)'의 비율이 높은 것은 우리 감사원과 비슷하나, 다른 최고감사기구에 비해 '조직', '프로세스', '인력', '표준화' 등 다양한 부문에 감사초점을 두고 있는 것으로 나타났고, NAO의 경우는 '전략(38%)', '정보기술품질(19%)', '비용(19%)', '편익(19%)' 등을 주요 감사초점으로 고려하고 있는 것으로 나타났다. ANAO는 '정보기술품질(32%)'과 '전략(23%)', '보안(23%)'이 주요 감사초점으로 나타났고, OAG는 '전략(30%)'과 '정보기술품질(30%)'이 다른 부문의 감사초점보다 월등하게 높았다.

각 감사초점별 특징을 살펴보면 ANAO를 제외한 모든 기관들은 '전략'을 가장 비중 있게 다루고 있고, 그 다음은 '정보기술품질'로 나타났다. 기관별로는 ANAO를 제외하고 우리 감사원(33%), GAO(23%), NAO(38%), OAG(30%) 등은 '전략'에 대한 감사초점 비중이 가장 높은 것으로 나타났다. 한편, ANAO(32%)와 OAG(30%) 등은 '정보기술품질'이 감사초점 비중이 제일 높았다. '비용'과 '편익' 부분은 특히 NAO의 감사초점 비중(19%)이 다른 기관보다 상대적으로 높았다. 이는 NAO가 전통적으로 'Value-for-Money' 기반의 감사에 중점을 둔 결과라고 파악된다. '사용자 만족'의 경우 전반적으로 비중이 높지 않거나 감사초점에 포함되지 않은 것으로 나타났다. GAO, NAO, ANAO 등은 주요 감사초점에 포함되지 않았으나 OAG(10%), ANAO(9%), 우리 감사원(4%)이 주요 감사초점으로 '사용자 만족'을 포함하였다.

한편, GAO를 제외한 다른 기관들은 모두 '조직', '프로세스', '인력' 등을 감

사초점에 포함하지 않은 것으로 나타났다. '보안'부문은 OAG를 제외하고 모든 기관에서 주요 감사초점으로 여기는 반면, 다른 기관에 비해 우리 감사원(4%)의 감사초점 비중이 상대적으로 낮았고, ANAO가 23%로 가장 높았다. '사용자 참여'에 대한 감사초점은 5개 기관 모두 사례를 찾을 수 없었다.

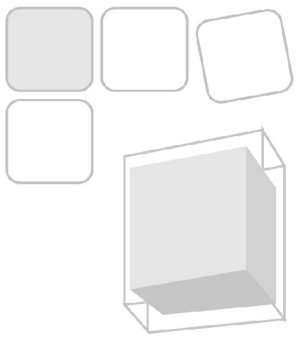
〈표 3-15〉 주요국 감사초점별 IT감사사례 비교(2008-2009년)

기관명 / IT감사 초점	BAI	GAO	NAO	ANAO	OAG
전략	**8(33%)**	**10(23%)**	**6(38%)**	**5(23%)**	**3(30%)**
조직	-	2(5%)	-	-	-
프로세스	-	1(2%)	-	-	-
인력	-	5(12%)	-	-	-
비용	2(8%)	4(9%)	3(19%)	2(9%)	1(10%)
편익	2(8%)	4(9%)	3(19%)	1(5%)	1(10%)
사용자 만족	1(4%)	-	-	2(9%)	1(10%)
사용자 참여	-	-	-	-	-
표준화	2(8%)	3(7%)	-	-	1(10%)
보안	1(4%)	5(12%)	1(6%)	5(23%)	-
정보기술품질	7(29%)	8(19%)	3(19%)	**7(32%)**	**3(30%)**
인프라	1(4%)	1(2%)	-	-	-
총 건수	**24 (100%)**	**43 (100%)**	**16 (100%)**	**22 (100%)**	**10 (100%)**

한편 감사초점으로 '사용자 만족'이나 '사용자 참여' 등이 포함되어 있지 않았지만 NAO와 ANAO는 감사방법으로 이해관계자의 인터뷰 등을 통한 사용자의 시각을 반영하고 있다는 점에서 IT감사가 이해관계자 등의 측면에서 고려되어야 한다는 것을 단적으로 보여준 예라고 할 수 있다. 우리나라의 경우 전자정부사업이나 정보화사업의 수혜자가 일반국민인 경우가 많다는

것을 감안하면 IT감사의 목적도 수요자 중심으로 바뀌어야 한다.

감사방법에 있어서 다른 기관과 우리 감사원과의 큰 차이점은 발견하지 못하였다. 수감기관의 관련 문서를 검토한다던지, 관련 지침이나 기준을 검토하고, 관련 담당자 인터뷰 등은 모든 기관이 일반적으로 시행하는 것으로 일반 감사이든 IT감사이든 큰 차이가 없었다. 다만 위에서 언급한 바와 같이 다양한 사용자 시각을 반영하려 하였다는 것, 외부기관과의 협업, 감사의 질 제고를 위하여 외부전문가의 자문을 받고 있다는 것은 IT감사를 체계적으로 실시하는 데 우리 감사원이 참고할 만한 부분이라고 판단된다.



제4장 결론 및 발전방향

제4장 결론 및 발전방향

제1절 결 론

본 연구에서는 IT감사기준을 계획·실시·보고 등 감사단계별로 분류하여 그 내용을 살펴보았다. 계획부분에서는 위험요소들을 먼저 파악하고 이에 따른 이슈들을 중심으로 감사계획을 수립하는 것이 특징이었고, 실시부분에서는 일반통제와 어플리케이션 통제 등 2개 부분으로 구분하여 통제의 적정성 여부를 파악하고 있으며, 보고부문에서는 감사방법론, 판단기준, 외부전문가 자문 등 감사결과에 대한 객관성 및 신뢰성을 강조하기 위한 내용들이 포함된 것이 특징적이다.

주요국 감사원의 IT감사사례를 감사절차에 따라 분석하고자 하였으나 IT감사보고서 내용이 감사계획, 실시, 보고 등의 체계에 맞추어 정리되어 있지 않아 이를 비교·분석의 틀로 적용하기는 어려웠다. 예를 들어 GAO의 경우 IT감사보고서의 내용은 일반적으로 감사결과 중심으로 기술되어 있고, 목적·범위·방법론 등이 추가적으로 포함되어 있었고 NAO 등 다른 감사원의 경우도 비슷하였다. 그래서 절차에 따른 비교·분석은 적합하지 않아 고려하지 않았고 그보다는 IT감사를 실시할 때 목적, 범위 등을 통한 감사초점 방향에 대한 비교가 가능하다고 판단하였다. 모든 기관이 IT감사보고서에 공통적으로 이러한 부분을 언급하였기 때문이다. 따라서 비교·분석의 틀로 일반적인 IT감사의 감사초점은 어디에 두는가를 알아보기 위하여 선행연구와 COBIT의 감사기준을 토대로 12개의 주요 감사초점을 추출한 것이다. 본 연구에서는 이를 통하여 우리 감사원과 다른 나라의 감사원이 IT감사를 실시하는데 IT감사초점과 관련되어 어떤 공통점과 차이점이 있는지를 설명하였고, 앞으로 어떤 점을 착안해서 봐야 하는지를 제시하였다.

제2절 발전방향

이상의 연구결과에서 우리 감사원이 앞으로 보다 효과적인 IT감사를 실시할 때 중요하게 고려해야 할 몇 가지 사항을 제안하고자 한다.

첫 번째로 IT감사기준의 확립이다. GAO는 하나의 정해진 감사기준은 없지만 정보시스템 보안 등과 관련 감사는 FISCAM을 주로 이용하고 있고, NAO 등 다른 감사원 역시 COBIT 등 국제적인 수준의 IT감사기준을 채택하여 감사에 이용하고 있다. 우리 감사원의 경우 ASOSAI 사무국을 운영하는 등 그 지위가 더욱 높아진 감사원의 위상에 걸맞게 감사의 질 제고를 위한 노력을 해야 한다. 외국의 감사원들이 감사기준이나 지침이 무엇인지 감사보고서에 밝히는 이유는 그들의 감사내용에 대한 신뢰성을 얻기 위한 것으로 우리 감사원의 경우 감사판단의 근거를 제공하는 것이 다른 나라에 비해서 미흡한 것이 사실이다. INTOSAI도 국제적인 감사기준에 상응하는 IT감사기준을 적용할 것을 권고하고 있는 만큼 우리 감사원도 이러한 요구에 부응하여 국제적인 수준의 IT감사기준을 독자적으로 개발하거나 도입하여 우리 실정에 맞도록 적용하는 방안을 적극 검토해야 한다.

두 번째로 IT감사계획에 있어서 위험평가의 도입이다. GAO 등 외국의 감사원들은 감사계획을 수립할 때 발생 가능한 위험요소가 무엇인지를 먼저 정의하고 이 위험요소의 우선순위에 따라 감사계획을 수립하는 것이 보편화되어 있다. 영·미계 국가에서 보편화되고 있는 위험기반의 감사접근방법에 대한 인식 및 이해가 상대적으로 부족하다. 정보시스템의 확산으로 내부통제가 보다 정교하고 복잡해지고 있는 감사환경을 고려할 때 조직의 위험평가에 기초한 감사접근법이 요구된다(이재권, 2001). 우리 감사원의 경우 취약점과 문제점 등을 중심으로 감사계획을 수립하고 있는데, 어떤 면에서는 위험평가와 유사한 점이 있으나 체계적이고 표준화된 절차에 의해서 제시되는 것이 아니라 특정한 취약점 및 문제점이 발견된 경우에 한정한다는 것에

서 차이가 있다. 감사계획을 수립할 때 이러한 점을 참고하여 체계적인 위험평가를 감사계획의 일부로 반드시 포함할 수 있도록 해야 한다. 한 예로 OAG는 IT감사에서 중요하게 고려해야 할 위험요소들을 영향력(impact) 측면과 발생가능성(likelihood) 측면으로 구분하여 위험평가의 기준으로 제시하고 있다(〈표 4-1〉 참조). 이에 따르면 대규모 프로젝트나 보안 및 통제와 관련된 위험요소는 발생할 가능성도 높고, 파급효과 또한 높은 반면, 시스템 및 서비스 공유와 시스템의 상호 운영성은 발생할 가능성은 높지만 파급효과는 높지 않다. 이들 점을 감안하여 감사계획 시에 참고하고 영향력이 높고, 발생가능성도 높은 위험요소에 좀 더 초점을 맞추는 것이 필요할 것이다.

〈표 4-1〉 위험요소의 영향력 및 발생가능성

위험요소	영향력	발생 가능성
대규모 IT 프로젝트	**높음**	**높음**
- 사업 목적이 불분명한 경우 - 새로운 시스템이 원래 의도대로 기능하지 못하는 경우 - 비용이 예산 및 기간을 초과한 경우		
보안 및 통제	**높음**	**높음**
- 중요 정부 시스템에 대한 접근 통제의 부적절한 경우		
국가안보 및 매우 민감한 시스템	**높음**	**중간**
- 국가안보를 담당하는 기관들이 정보를 공유하고 효과적이고 효율적으로 운영하는 것이 불가능한 경우		
재해복구 및 사업의 연속성	**높음**	**낮음**
- 재해복구 및 사업의 연속성 계획이 존재하지 않거나, 부적정하거나, 시험한 적이 없는 경우		
혁신 및 서비스 변환	**중간**	**높음**
- 정부의 온라인 서비스 이전이 국민의 기대에 부응하지 못하는 경우 - 정부가 국민보건 및 안전 등 중요한 정보를 유지하고 공유하는 데 실패한 경우		

위험요소	영향력	발생 가능성
시스템 및 서비스 공유	**중간**	**높음**
- 시스템 및 서비스 공유 기회를 놓치거나 잘못 관리하였을 경우		
새로운 시스템과 현재 시스템의 효율성	**중간**	**높음**
- 새로운 시스템과 현재 시스템이 경제적이고 효율적으로 정보자원을 사용하지 못하는 경우(예: 유사기능의 중복, 시스템 기능 미사용 등)		
시스템의 상호 운용성	**중간**	**높음**
- 현재 사용하는 기술과 새로 도입한 기술 간의 호환되지 않는 경우		

세 번째는 감사초점의 단편성이나 쏠림현상을 개선하는 것이다. IT감사사례 분석결과에서 언급한 바와 같이 우리 감사원의 경우 '전략'과 '정보기술품질'이 전체 감사초점의 62%가 된다. 물론 ANAO(55%), OAG(60%) 등도 비슷한 수준이기는 하나 2008년과 2009년 기간 동안의 IT감사보고서에 국한된 것이라 이를 일반화하기는 어렵고, 또한 이들 기관과 비슷한 수준이라 하더라도 IT감사초점을 '전략'과 '정보기술품질'에 치중한다고 문제될 것이 없다고 하는 것도 설득력이 떨어진다. 물론 IT감사를 실시할 때 12개의 모든 감사초점을 검토해야 한다는 것은 아니다. 본 연구가 제시한 12개의 감사초점은 정보시스템의 평가가 그만큼 복잡하고 다양한 측면을 요구한다는 것을 보여준다. 시스템 자체의 질 평가를 위한 기술적 측면도 중요하지만 이를 둘러싼 정보시스템 환경, 즉 조직문화와 인력 등 보이지 않는 측면도 고려해야 궁극적인 개선방향을 제시할 수 있는 것이다.

네 번째는 IT감사를 위한 전산감사기법을 적극적으로 활용할 필요가 있다. 예를 들어 ANAO는 부처 웹사이트 관리문서 평가를 위해 ANAO가 직접 개발한 의사결정트리(decision tree)를 이용하여 웹사이트 기능과 관련한 위험수준을 분류하는 등 전산감사기법을 이용한 IT감사를 실시하고 있다는 것을 확인할 수 있었다. 우리나라의 경우 거의 모든 행정업무가 전산화됨에 따라

감사증거가 될 수 있는 공문서와 장부 등이 줄어들고 시스템에 저장되어 있는 데이터가 그 역할을 대신하고 있다. 공무원의 비리가 시스템을 이용하여 이루어지고 점차 증가하는 추세이므로 비리 적발 역시 IT감사를 통해 효과를 얻을 수 있으며, 따라서 감사에 정보기술을 사용하지 않는다면 감사효율이나 효과를 기대하기 어렵다(이재권, 2001). 건강·실업보험, 사회복지, 조세분야 등 다양한 분야에서 발생하는 연금 부정 수급이나 예산 낭비 등을 적발할 때 이러한 기법은 필수적이며 또한 대외적으로는 ASOSAI 회의에서 우리 원이 사무총장국이 됨으로써 국제적인 위상이 높아지고, 회원국들이 IT를 활용한 감사능력의 배양에 대한 깊은 관심을 표명하면서 관련 분야에 대한 우리 원의 협조를 요청하고 있는 상황이다. 따라서 우리 원 차원에서 전산감사기법의 도입과 적용이 필요한 시점이다.

다섯 번째 우리 원의 IT감사역량을 제고하는 것이다. 최근 청와대 등 정부부처를 대상으로 사이버공격이 감행됨에 따라 그 어느 때보다도 정보보안에 대한 대책 마련이 시급한 시점에 우리 원이 자체적으로 역량을 축적해왔다면 이러한 문제들을 짚고넘어갈 수 있을 텐데 하는 아쉬움이 있었다. 이는 IT감사사례 비교에서 보았듯이 선진 주요국 감사원의 전체 감사에서 IT감사가 차지하는 비율이 평균 3~10%를 차지하는 반면 우리 원의 경우 1% 정도 밖에 안 된다는 것에서도 쉽게 알 수 있다. 이를 개선하기 위해서는 먼저 IT감사에 대한 원내의 인식이 바뀔 필요가 있다. IT감사의 범위가 전산감사기법을 이용하여 필요한 데이터들을 시스템에서 추출하고 문제점들을 밝혀내는 것에만 한정하는 것은 IT감사영역을 매우 좁은 의미로 해석하는 시각이다. 또한 IT감사가 성과감사나 재무감사와 다른 별도의 감사형태로 인식하는 경우가 많은데 물론 IT감사가 단독으로 IT시스템을 대상으로 실시하기도 한다. 그러나 본 연구에서 검토한 해외 IT감사기준을 보더라도 성과감사나 재무감사의 일부분으로 IT감사가 같이 실시되는 경우도 많다. 이는 대부분의 감사가 IT시스템을 중심으로 자료의 입력·가공·결과의 산출이 이루어지기 때문에 이를 제외하고 문서 위주의 문제점 파악이라는 것은 효과적인

감사를 실시할 수 없기 때문이다. 따라서 IT감사의 범위, 역할, 필요성에 대한 원내의 인식을 새롭게 하고 공감대가 형성될 수 있도록 IT감사교육을 활성화할 필요가 있다.

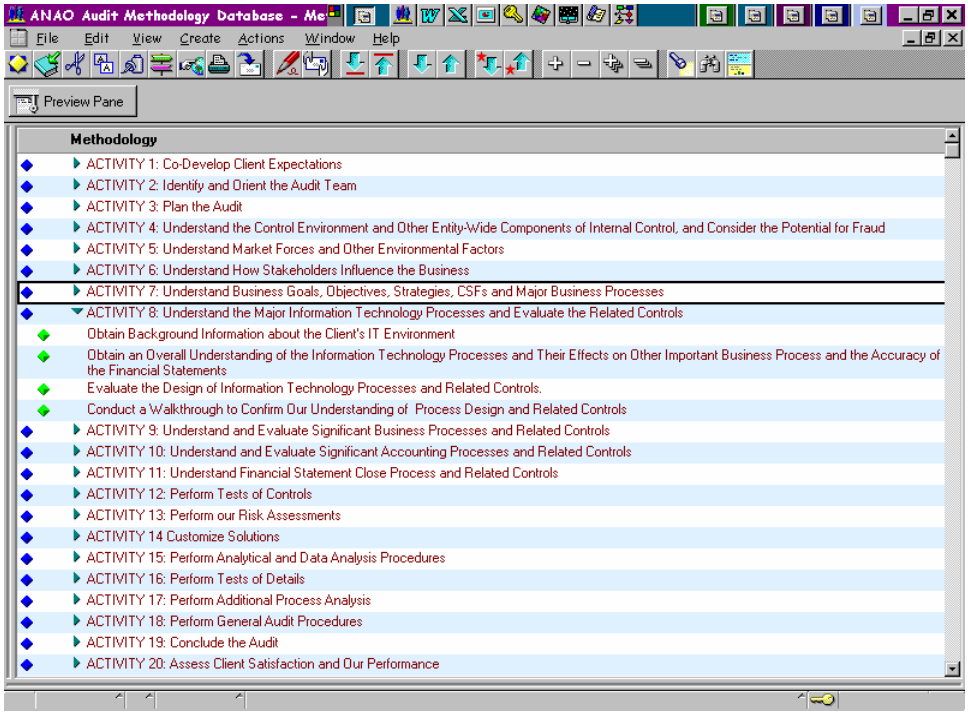
또한 IT감사역량을 제고하기 위하여 외부기관과의 협력관계를 모색해야 한다. NAO의 경우 외부 IT컨설팅 기관과의 협력을 통하여 IT감사의 질 제고에 노력하고 있다. 우리나라의 경우 정보화진흥원이 오랫동안 COBIT을 기반으로 정보시스템 감리에 대한 기준, 활용 등 다양한 노하우를 가지고 있으므로 현재 우리 원의 IT감사 전문인력이 부족한 것을 감안할 때 전략적 파트너십을 통한 협업이 좋은 대안이 될 수 있으며, 현장학습을 통한 우리 원의 IT감사 전문인력을 양성하는 데 도움이 될 수 있다.

여섯 번째로 효과적인 IT감사를 위한 인프라를 구축하는 것이다. 먼저 우리 원이 사용하고 있는 e-감사시스템은 내부의 정보 공유를 목적으로 이용할 뿐만 아니라 부처 사업진행이나 업무의 모니터링이 가능하도록 외부 시스템과의 연계가 필요하다. 우리 원이 원활한 IT감사수행을 위하여 온나라 시스템의 접근 권한을 보유할 필요가 있다. 현재는 국무총리실에서 모든 부처의 관련 서류를 온나라 시스템을 통하여 열람할 수 있는 권한이 있으나 부처의 온나라 시스템의 활용률이 저조하여 정보의 누락이 발생하고 있어 온나라 시스템의 접근 권한이 있더라도 효과적인 IT감사 수행을 하는데 한계가 있다는 우려가 있다. 이런 경우가 계속되면 일부 서류기반의 감사 병행이 불가피하여 효율적인 IT감사수행에 장애가 발생할 수 있다. 따라서 관련 기관과의 업무 협조를 통하여 이러한 문제를 원만히 해결할 수 있는 방안을 모색해야 할 것이다.

또한 우리 원 내부적으로는 IT감사방법론을 포함한 IT감사와 관련한 지식공유를 위한 데이터베이스 구축이 필요하다. 현재는 감사보고서와 감사처분요구서 등 결과 위주의 서류 중심으로 등록되어 있어 전체적인 감사절차별로 감사인이 무엇을 어떻게 해야 하는지를 파악하기 어렵다. 실제로 감사에 도움이 될 수 있는 시스템이 되려면 실제 감사를 실시할 때 필요한 지식과

경험을 공유할 수 있어야 한다. 예를 들어 호주 ANAO는 감사방법론 데이터베이스가 구축되어 있어 감사단계별로 필요한 파일을 참고할 수 있으며 어떤 활동을 해야 하는지를 제시함으로써 일관성 있는 감사를 실시할 수 있는 기반을 마련하고 있다. 따라서 우리 감사원도 e-감사시스템의 활용을 증대하려면 이러한 측면의 고려가 필요하다.

〈그림 4-1〉 ANAO의 감사방법론 데이터베이스 화면



마지막으로 우리 원의 IT감사의 역할 재정립이다. 1999년 금융감독원은 검사총괄실 내에 IT검사팀을 운영한 뒤 IT감독과 검사의 통합 필요성을 주장하며 2001년에 IT검사국(국장급)으로 조직을 확대하였다. 그러나 2002년 검사와 감독을 분리하면서 IT검사지원기법 개발을 담당하는 IT검사연구실(팀장급)로 축소되었다. 이후 2003년에는 다시 IT업무실(부서장급)로 확대되었고, 2005년에 다시 IT감독팀(팀장급)으로 축소되었다. 2009년 현재 리스크검사지원국 밑에 신용리스크팀, 시장리스크팀, 운영리스크팀, IT리스크팀 등

4개 팀으로 나누어져 있으며, IT리스크팀이 IT분야의 리스크 전문검사를 지원하고 있고 9명의 인원을 보유하고 있다. 조직상으로는 IT리스크팀이 IT감사를 총괄하는 유일한 팀이나 인력 및 전체적인 조직 기능 측면에서 비교해 보았을 때 현재의 IT감사 전문성이나 역량으로 금융기관을 대상으로 효과적인 IT검사를 하기에는 미흡하다고 판단된다. 한편, 정보화진흥원의 정보시스템 감리제도는 토지감정평가사처럼 감리를 담당하는 사기업이 증가하면서 감리품질 저하의 원인이 되고 있다. 또한 수천억 원의 예산이 투입된 전자정부 31대 로드맵 과제의 효과성 분석이 반드시 필요하며 이것을 수행할 수 있는 기관은 우리 원밖에 없다는 전문가의 의견이 많다. 이러한 현실적인 이슈들이 계속 제기되면서 총체적인 IT감사 구축체계를 확립하기 위하여 우리 원이 주도적인 역할을 수행해나갈 필요가 있다.

제3절 향후 연구방안

IT감사사례를 최근 2008년과 2009년으로 국한하였기 때문에 기관별로 감사보고서 개수의 차이가 많았다. GAO의 경우는 2008년만 39건이나 되어 다른 기관에 비해 월등히 많아서 이번 사례분석에는 2009년의 9건만 포함하였다. NAO 등 다른 기관의 경우는 IT감사보고서의 개수가 적은 편이라 어떤 결론을 종합적으로 내리기에는 다소 부족한 점이 있었다. 따라서 기간의 범위를 넓혀, 예를 들어 2005년부터 현재까지의 IT감사보고서의 내용을 검토하여 감사초점의 유형을 보다 면밀히 조사한다면 보다 확실한 결과를 얻어낼 수 있을 것으로 생각한다. 또한 본 연구가 제시한 12개의 IT감사초점을 기반으로 보다 구체적인 세부사항을 추가적으로 개발할 수 있을 것으로 기대된다. 이러한 세부사항들은 체크리스트 형태로 제공되어 IT감사를 실시할 때 일관성 있는 접근방법을 제시할 수 있는 툴로 활용될 수 있을 것이다.

참고문헌

- 감사원(2003),『전자정부 구현사업 추진 실태』.
- ———(2005a),『시스템 감사 일반』.
- ———(2005b),『전자정부사업 추진 실태』.
- ———(2008a),『통합지휘무선통신망 구축 실태』.
- ———(2008b),『행정정보 공유 및 구축 실태』.
- ———(2009a),『국가전자조달시스템 운영 실태』.
- ———(2009b),『국가정보화 및 전산화사업 추진 실태』.
- ———(2009c),『e-호조(지방재정관리시스템) 구축사업 추진 실태』.
- 경태원·김상국(2008),『정보시스템 감리 서비스 평가항목에 대한 이해당사자 간 우선수위 분석에 관한 연구』, Information Systems Review 10(1).
- 금융감독원(2006),『IT검사 매뉴얼』.
- 김인석(2002),「금융기관 IT부문 경영실태평가」,『월간손해보험』.
- 나종필(2005),「은행 COBIT 감사의 활성화 방안에 관한 연구: 은행의 기존 IT감사와 COBIT에 기반한 IT감사의 비교분석을 중심으로」, 성균관대학교 행정대학원 석사학위논문.
- 박종태(2006),「금융기관 정보시스템 감사의 성공요인에 관한 실증적 연구」, 광운대학교 박사학위논문.
- 신동익(2003),「정보시스템 감리체계」,『정보화정책』.
- 이미영·이영범(2009),「평가와 감사의 연계강화를 통한 정보화사업 평가 개선방안에 관한 연구」,『정책분석평가학회보』.
- 이분순(2004),「정보시스템 감리제도에 관한 연구」, 성균관대학교 석사학위논문.
- 이장형(1997),「정보시스템 감사개론 절차와 기법」,『경영감사』.
- 이재권(2001),「전산화된 환경에서의 내부통제와 감사체계화 방향」,『감사논집』.
- 이종세(2008),「금융회사 IT리스크의 효율적 관리방안」, Risk Review 봄호,

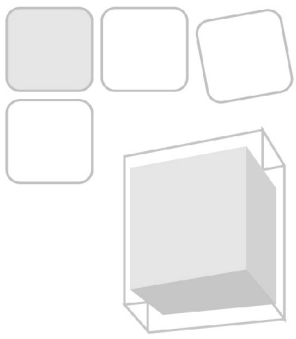
금융감독원.
- 장태범·김문오(2004),「감사실무 차원의 e-감사시스템의 활용기법」,『감사교육원 연구논문집』.
- 전영하(2004),「IT감사를 위한 새로운 프레임워크 및 적용사례」,『계간 감사』 봄호.
- 정보시스템의효율적도입및운영등에관한법률(2008).
- 한국전산원(2003),『정보시스템 감리 프레임워크 발전방안 연구(안)』.
- ————(2004),『해외정보시스템 감리 유사제도 비교연구』.
- 한국정보사회진흥원(2006),『정보시스템 감리점검 해설서(안) V.3.0』.
- ————————(2007),『정보시스템 감리기준 해설서』.
- ————————(2008),『정보시스템 감리와 국제 IT가이던스와의 비교분석연구』.
- 황경태(2002),『정보시스템 감사/통제 성숙도 모델(Cobit)의 기본개념 및 적용사례』, 한국IT서비스학회.
- 호진원(2006),「전자정부사업 성과지표 표준화를 위한 연구」, 한국정책분석평가학회 동계학술대회.
- 호진원·이미영(2008),「전자정부사업 평가를 위한 표준운영모델에 대한 타당성 연구」, Journal of Information Technology Applications & Management, 15(4).
- ANAO(2008a), "DIAC(Department of Immigration and Citizenship)'s Management of the Introduction of Biometric Technologies."
- ———(2008b), "Government Agencies' Management of their Websites."
- ———(2008c), "Management of Personnel Security - Follow-up Audit."
- ———(2009a), "Management of the Movement Alert List."
- ———(2009b), "Quality and Integrity of the Department of Veteran's Affairs Income Support Records."
- ASOSAI(2003), "IT Audit Guidelines."
- http://www.asosai.org/R_P_it_auditing/project6.pdf.

- Cascarino, R. E.(2007), *Auditor's Guide to Information Systems Auditing*, John Wiley & Sons, Inc., Hoboken, New Jersey.
- GAO(2009a), "Federal Information System Controls Audit Manual."
- ——(2009b), "Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls."
- ——(2009c), "Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization."
- ——(2009d), "Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weakness."
- ——(2009e), "Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data."
- ——(2009f), "Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS."
- ——(2009g), "Information Technology: DOD Needs to Strengthen Management of Its Statutorily Mandated Software and System Process Improvement Efforts."
- ——(2009h), "Electronic Health Records: DOD's VA's Sharing of Information Could Benefit from Improved Management."
- ——(2009i), "Information Technology: Federal Agencies Need to Strengthen Investment Board Oversight of Poorly Planned and Performing Projects."
- ——(2009j), "Information Technology: HUD Needs to Strengthen Its Capacity to Manage and Modernize Its Environment."
- IIA(2005), "Global Technology Audit Guide(GTAG): Information Technology Controls."
- ——(2006), "Global Technology Audit Guide(GTAG): Management of IT Auditing."
- ——(2008), "Global Technology Audit Guide(GTAG): Developing the IT Audit Plan."

- IntoIT(2005), "CAATs that Byte", *The INTOSAI IT Journal*, Issue 22.
- ———(2006a), "Canada: Country Focus", *The INTOSAI IT Journal*, Issue 23.
- ———(2006b), "GAO West", *The INTOSAI IT Journal*, Issue 24.
- ———(2007), "NAO Experience of IT Governance Reviews", *The INTOSAI IT Journal*, Issue 25.
- ———(2008), "Assuring SAP", *The INTOSAI IT Journal*, Issue 27.
- INTOSAI(2006a), "Methodological Recommendations for Information Systems Audit", 16th Meeting of the INTOSAI Working Group on IT Audit.
- ————(2006b), Information Systems Performance Audit.
- ————(2008), "Project on Auditing E-Government."
- ISACA(2007), "CISA Review Manual 2007."
- ———(2009), "IS Standards, Guidelines and Procedures for Auditing and Control Professionals."
- Majdalawieh, M. & Zaghloul, I.(2008), "Paradigm shift in information systems auditing", *Managerial Auditing Journal,* 24(4).
- Mitsubishi UFJ Research and Consulting(2009), "欧米主要国における IT化の進展に対応した 検査の手法と事例に関する調査研究."
- NAO(2008a), "The Defense Information Infrastructure."
- ——(2008b), "The National Program for IT in the NHS."
- ——(2009), "The National Offender Management Information System."
- OAG(2008a), "Managing Environmental Programming: Agriculture and Agri-Food Canada."
- ——(2008b), "Managing Information Technology Investments: Canada Revenue Agency."
- ——(2008c), "Managing Severe Weather Warnings: Environment Canada."
- ——(2009), "Managing Identify Information."
- Pathak, Jagdish(2005), "Information Technology Auditing: An Evolving

Agenda," Springer.

- Singleton, T. W.(2006), "COBIT- A Key to Success as an IT Auditor", *Information Systems Control Journal*, Volume 1.
- Tuttle, B. and Vandervelde, S. D.(2007), "An empirical examination of Cobit as an internal control framework for information technology", *International Journal of Accounting Information Systems*, 8.
- Weber, R.(1999), *Information Systems Control and Audit*, Prentice Hall.
- Westerman, G. & Hunter, R.(2007), "IT Risk: Turning Business Threats Into Completive Advantage."



부 록

IT감사사례분석을 위한 주요국의 IT감사보고서 목록

부록 IT감사사례분석을 위한 주요국의 IT감사보고서 목록

기관명	IT감사보고서 제목
BAI	① 전자정부 구현사업 추진 실태(2003) ② 전자정부사업 추진 실태(2005) ③ 행정정보 공유 및 관리 실태(2008) ④ 통합지휘 무선통신망 구축 실태(2008) ⑤ e-호조(지방재정관리시스템) 구축사업 추진 실태(2009) ⑥ 국가정보화 및 전산화사업 추진 실태(2009) ⑦ 국가전자조달시스템 운영 실태(2009)
GAO	① “Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls”(2009) ② “Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization”(2009) ③ “Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weakness”(2009) ④ “Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data”(2009) ⑤ “Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS”(2009) ⑥ “Information Technology: DOD Needs to Strengthen Management of Its Statutorily Mandated Software and System Process Improvement Efforts” (2009) ⑦ “Electronic Health Records: DOD’s VA’s Sharing of Information Could Benefit from Improved Management”(2009) ⑧ “Information Technology: Federal Agencies Need to Strengthen Investment Board Oversight of Poorly Planned and Performing Projects”(2009) ⑨ “Information Technology: HUD Needs to Strengthen Its Capacity to Manage and Modernize Its Environment”(2009)

기관명	IT감사보고서 제목
NAO	① “The Defense Information Infrastructure”(2008) ② “The National Program for IT in the NHS”(2008) ③ “The National Offender Management Information System”(2009)
ANAO	① “Management of Personnel Security - Follow-up Audit”(2008) ② “DIAC(Department of Immigration and Citizenship)’s Management of the Introduction of Biometric Technologies”(2008) ③ “Government Agencies’ Management of their Websites”(2008) ④ “Quality and Integrity of the Department of Veteran’s Affairs Income Support Records”(2009) ⑤ “Management of the Movement Alert List”(2009)
OAG	① “Managing Severe Weather Warnings: Environment Canada”(2008) ② “Managing Environmental Programming: Agriculture and Agri-Food Canada” (2008) ③ “Managing Information Technology Investments: Canada Revenue Agency” (2008) ④ “Managing Identify Information”(2009)

선진국의 IT감사기준 분석을 통한 IT감사체계 발전방안 연구

발행일 / 2010년 2월
발행처 / 감사원 감사연구원
(110-793) 서울특별시 종로구 계동 140-2 현대빌딩 7층
발행인 / 감사연구원장
편 집 / 감사연구원 연구부
인 쇄 / 타라그래픽스