은행 정보시스템 감사에 관한 사례 연구

황 경 태[†]·김 송 주[††]

요 약

은행업에 있어서 정보시스템의 중요성은 다른 산업에 비해서 매우 높다. 본 논문에서는 한 은행의 사례를 토대로 은행에서 실시하고 있는 정보시스템 감사 제도의 전반적인 현황을 분석하여 문제점 및 발전 방향을 제시한다. 주요한 문제점은 다음과 같다. 전반적으로 정보시스템 프로세스의 수행 정도가 미흡하고, 감사 실시 정도는 전반적으로 중요한 프로세스에는 적절히 대응하고 있으나 금융 및 전산사고 예방에만 초점을 맞추어 전략적인 측면의 대응이 미흡한 것으로 나타났다. 또한 감사 활동이 프로세스 수행에 긍정적인 영향을 미치지 못하고 있어서 감사 사후 관리를 개선할 필요성이 제기되었다. 감사 인력/조직적인 측면에서는 인력의 충원이 필요하고, 전략 기획 분야와 연구·개발 활동이 미흡하고, 감사인의 적격성 및 독립성 분야에서 기준 대비 미흡한 면이 있는 것으로 분석되었다. 여기에 대한 발전 방향으로는 내부 감사 부서들간의 적절한 감사 분담, 외부 감사의 활용, 감사 자동화 도구 도입, 자가통제평가 제도 도입, 감사인력에 대한 경력개발 제도 실시, 위험 기반 감사 제도 도입 등이 있다. 본 연구의 결과는 은행업, 더 나아가서 다른 산업의 기업들이 참고할 수 있는 사시점을 제공하고, 본 연구에서 활용한 분석 프레임워크는 향후 정보시스템 감사 분야의 학술적인 연구에서 활용될 수 있을 것이다.

A Case Study on the Information Systems Audit of a Bank

Kyung Tae Hwang[†] · Song Ju Kim[††]

ABSTRACT

Importance of Information Systems in banking industry is higher than that of other industries. This study, based on a case study of a bank, analyzes the current status of information systems (IS) audit and proposes future directions in the area of IS control and audit. Major problems identified in the study include deficiency of IS and audit process, and inability of audit function to improve IS process. In addition, deficiency of staffing level and investment in R&D, and lack of competency and independence of audit staff are identifed. In order to solve the problems, the following directions were proposed : proper division of functions among audit related departments, utilization of outside audit function, and adoption of CSA, CAAT, career path program, risk-based audit approach. The results of the study will provide valuable implications to banks and companies in other industries. Also the research framework employed in the study can be utilized in the future research in IS control and audit.

키워드 : 정보시스템 통제(Information Systems Control), 정보시스템 감사(Information Systems Audit)

1. 서 론

은행업은 국가 기반 산업의 하나로서 신뢰성과 명성을 바탕으로 자금의 수요와 공급을 조절해 주는 기능 즉 자금의 융통 기능을 주요한 사업으로 하고 있다. 은행업에 있어서 정보시스템의 중요성은 다른 산업에 비해서 매우 높다. 그 이유를 몇 가지만 정리해 보면 다음과 같다. 첫째, 정보와 이러한 정보를 제공하는 정보시스템에 대한 의존도가 높다. 한 은행의 정보시스템이 1시간만이라도 중단되면, 해당 은행의 업무 수행 및 고객과의 거래가 중단될 뿐만 아니라 국내 자금 시장의 흐름에도 큰 영향을 미치게 된다. 둘째, 사이버 범죄 등과 같은 다양한 종류의 위협에 노출될 수 있는 가능성이 증가하고 있다. 미국의 한 통계에 의하면, 금융 기관들은 컴퓨터 시스템에 침입한 해커들의 협박을 무마시키기 위해서 연간 수천만불을 지불하고 있다고 한다. 셋째, 정보와 정보시스템에 대한 투자 규모가 현재도 무시할 수 없는 수준이지만 향후에도 지속적으로 증가할 것으로 예상된다. 미국 금융 산업의 예를 들면, 총 설비 투자액의 75%가 정보기술에 투자되고 있다[13]. 넷째, 정보기술을 이용하여 업무 절차를 변화시키고, 새로운 기회를 창출하고, 비용을 절감시킬 수 있는 가능성이 증가하고 있다. 최근 들어 기업들이

※ 이 연구는 동국대학교 논문게재 연구비 지원에 의하여 이루어졌음.
† 정 회 원 : 동국대학교 경상대학 정보관리학과 교수
†† 정 회 원 : 국민은행 전산정보본부
논문접수 : 2001년 8월 20일, 심사완료 : 2002년 2월 15일

추진하고 있는 경영 혁신 프로그램(예 : BPR, SCM, CRM 등)은 정보시스템의 지원 없이는 실현할 수 없는 것들이 많이 있다.

이처럼 중요한 자원인 정보 및 정보시스템을 효과적으로 관리하기 위해서는 중요한 경영 자원인 자금에 대해서 회계 감사를 실시하듯이 정보시스템에 대해서도 적절한 통제 시스템을 수립하고 이러한 통제의 적정성을 검증하기 위한 감사 체계를 수립하여 실행하는 것이 필요하다.

본 논문에서는 한 은행의 사례를 토대로 은행에서 실시하고 있는 정보시스템 감사 제도의 전반적인 현황을 분석하여 문제점 및 발전 방향을 제시하고자 한다. 현재 국내에서는 정보시스템 감사가 잘 정착되지 못하고 있고, 정보시스템 감사에 관한 학술적인 연구가 미흡한 실정이다. 따라서 특정 은행의 정보시스템 감사 현황을 분석해 봄으로써 은행업 전반에서 참고할 수 있는 개선점과 다른 산업에서도 참고할 수 있는 시사점을 도출하고자 한다. 또한 본 연구에서는 향후 정보시스템 감사 분야의 학술적인 연구에서 활용될 수 있는 하나의 분석 프레임워크를 제시한다.

2. 연구 방법

본 연구에서는 사례 연구를 바탕으로 분석을 수행하고자 한다. 국내 은행의 전반적인 실태를 파악하는데는 사례 연구보다는 설문 조사(Survey)가 더 좋은 연구 방법일 수 있지만, 이 분야의 선행 연구가 미흡하고, 현상 자체만이 아니라 그 원인과 과정을 보다 심도있게 분석하기 위해서 사례 연구 방법을 선택하였다.

사례 분석 대상 은행은 국책 은행 중의 하나이다. 해당 은행의 신원 보호를 위해서 이하에서는 A은행으로 칭한다. A은행에서 시행하고 있는 정보시스템 감사의 전반적인 현황 등을 파악하기 위해서 감사 지침, 정보시스템 운영 매뉴얼 등과 같은 보고서 및 문서 분석, 내부 감사인들과의 면담, 내부 감사인을 대상으로 한 델파이 방법론(Delphi Method)을 이용한 합의 도출 세션 등을 병행·실시하였다. 면담 및 합의 도출 세션에서 사용한 분석 프레임워크는 다음의 4장에서 설명한다.

3. 정보시스템 감사의 전반적인 현황

현재 A은행에서 실시하고 있는 정보시스템 감사 활동은 크게 외부 감사와 내부 감사로 분류할 수 있다(<표 1> 참조).

〈표 1〉 A은행에서 실시하고 있는 정보시스템 감사의 종류

분 류	감사 주체	수행 목적
외부 감사	감독기관(금융감독원)	법률의 준거성, 시스템 안정성
내부 감사	은행 검사부	규정 준수
	정보시스템 부문 전산감사반	내부통제, 금융사고 예방

다음에서는 금융감독원의 외부 감사, A은행 검사부 및 전산감사반의 감사에 대한 주요 내용을 정리한다.

3.1 금융감독원의 감사

은행을 비롯한 금융기관을 감사하는 특별 법인인 금융감독원은 1997년부터 금융기관의 정보시스템에 대한 검사를 일반 부문 검사와 분리하여 정보시스템 검사 전담반에서 독자적인 검사 및 평가를 실시하도록 검사 제도를 개편하였다. 금융감독원에서 실시하고 있는 정보시스템 감사의 평가 항목 및 그 주요 내용은 다음의 <표 2>에 정리되어 있다[1].

위의 4개 부문에 대한 개별 등급 평가 결과를 토대로 해당 기관의 정보시스템 부문 전체에 대한 종합 평가를 실시하고, 종합 평가 등급에 따라 차등화된 조치를 취하고 있다(<표 3> 참조).

〈표 2〉 금융감독원의 정보시스템 감사 내용

평가 항목	주요 내용	세부 평가 항목
정보시스템 감사	감사 조직의 독립성, 감사 요원의 자질 및 인원수, 감사 범위 및 기준과 감사 내용의 적정성 평가	• 정보시스템 감사 일반 • 정보시스템 감사 조직 및 인원 • 감사 내용
정보시스템 경영 관리	정보시스템 부문 경영의 효율성, 내부 통제, 중장기 계획 수립 상황과 경영정보시스템의 적정성 평가	• 경영 일반(경영 효율성) • 취약 내용의 시정 • 계획 및 방향 제시 • 경영정보시스템 • 비상 계획
시스템 및 프로그래밍	시스템 개발 조직, 표준화 및 절차, 시스템 개발 및 유지보수, 문서화, 내부 통제, 물리적 보안 관리 등의 적정성 평가	• 조직 및 인원 • 내부 통제 • 지침 및 절차 • 문서화 및 보안 대책
컴퓨터 운영	컴퓨터 운영 조직 및 요원 관리의 효율성, 정보시스템 센터의 안전 관리, 운영 통제, 자료 관리, 통신망 관리, 최종사용자 컴퓨팅 등의 적정성 평가	• 조직 및 인원 • 지침 및 절차 • 시설 및 장비 • 운영 통제 • 백업 및 비상 대책 • 통신망 • 보안 • 최종사용자 컴퓨팅 • 전자자금 이체

〈표 3〉 금융감독원 감사의 평가 내용 및 조치

종합평가 등 급	종 합 평 가 내 용	조 치
1 등 급	• 정보시스템부문 전반에 걸쳐 운영상태가 건전함 • 감독기관의 주의 불필요	다음 검사시 검사기간 및 검사범위 축소
2 등 급	• 근본적으로 건전하나 정보시스템 운영 과정에서 해결 가능한 약간의 취약점을 내포하고 있음 • 제한적인 감독 필요	다음 검사시 통상적인 검사 실시
3 등 급	• 즉각적인 시정을 요하는 다양한 취약점을 내포하고 있음 • 통상 수준이상의 감독상의 주의 요구	취약 부문에 대한 개선 계획 징구 (비공식 조치)
4 등 급	• 취약점이 심각하여 장래 정보시스템 업무 처리 자체가 위험하게 될 가능성이 있음 • 감독당국의 면밀한 주의가 요구되고 시정을 위한 명확한 계획 필요	종합개선계획 징구(비공식 조치)
5 등 급	• 취약점이 매우 심각하여 정상적인 정보 처리를 할 수 없는 상황임 • 감독당국의 즉각적인 조치 필요	해당 금융기관에 대해 공식적인 개선 지시

3.2 A은행 검사부의 내부 감사

OECD 권고에 따라 금융감독위원회는 국내 금융기관에 감사위원회를 설치·운영하게 하고 있다. A은행의 경우에도 감사위원회를 설치하여 사외이사 4인과 상근감사위원 1인으로 위원회를 구성하고 있다. 감사위원회는 그 임무 수행을 위하여 보조 기구인 독립된 검사부라는 조직을 두고 있다. 검사부는 상임감사위원의 지휘 하에 약 60명의 검사 인력이 본부 및 전 영업점의 활동에 대하여 감사 활동을 펼치고 있다.

아래에서는 본 논문의 주제와 직접적인 관련이 없는 일반적인 업무 수행에 대한 감사는 제외하고, 정보시스템 부문에 관련한 내용만을 요약 정리한다[9].

검사부에서 정보시스템에 대해서 수행하는 감사는 크게 다음과 같은 4가지로 분류할 수 있다. ① 일반 검사, ② 결산 검사, ③ 상시검사, ④ 일상검사. 첫째, 일반 검사는 1년에 2회 정도 실시하고 있다. 검사실시 기간은 평균 4~5일간 4~5명이 검사 영역을 분담하여 감사한다. 둘째, 결산 검사의 경우에는 년 1회 연도말에 실시되는 결산의 사전, 사후 작업에 대하여 결과의 타당성 및 결산 프로그램의 정당성을 검증한다. 셋째, 상시검사의 경우에는 전담 검사역이 정보시스템 부문에서 이루어지는 전산원장의 변경, 중요한 프로그램의 변경 내역 등에 대한 관리에 대하여 상시적인 감사 활동을 수행한다. 마지막으로 일상검사는 은행의 다른 업무 영역과 마찬가지로 부문장 이상이 결재하는 사항 중에서 중요 사항에 대해서 실시하는 감사를 말한다.

검사부는 관련법규 및 규정, 지침, 시달문서, 기안문서 등에서 정하는 업무 기준 및 절차에 따라 검사를 실시한다. 검사 후 그 결과는 일정한 절차를 거쳐서 보고되며, 일정한 시한 내에 검사 지적 사항에 대하여 조치를 요구하고, 인사상의 제재가 필요한 경우에는 인사위원회에 회부하고 있다.

3.3 A은행 전산감사반의 내부 감사

A은행에서는 IT 부문의 최고 경영자(부행장) 직속 부서인 전산감사반이 업무의 효율적인 관리와 사고를 미연에 방지하여 정보시스템의 신뢰성, 안전성, 효율성을 기하기 위한 목적으로 전산 업무의 일상 처리내용 및 사고발생 취약부분에 대하여 그 처리사항 및 출력물을 점검하여 오류, 불비, 부당, 기타 문제점을 조기 발견하고 시정 조치하는 등 정보시스템 부문에 대한 자체적인 감사를 실시하여 개선이 필요한 사항을 권고하고 있다.

전산감사반에서 수행하는 감사는 크게 다음과 같은 3가지로 분류할 수 있다. ① 일일검사, ② 특명 검사, ③ 전산 검사. 첫째, 일일 검사는 일상적인 전산업무(7개 항목)에 대한 적부 여부를 전산 출력하여 그 정당성 여부를 익영업일까지 실시하는 것을 말하고, 이 검사는 사고 예방의 성격을 갖는다. 둘째, 특명 감사는 업무 전반에 걸쳐 사고 발생 취약점 또는 문제점이 있는 분야에 대하여 검사사항(필수 및 선택 항목 20개 항목)을 업무의 중요성과 검사 빈도 등을 고려하여, 분기 2회 이상 특명검사일지에 의하여 불시에 실시한다. 또한 상근감사위원이 명한 불특정 검사사항을 검사 명령일에 실시할 수도 있다. 셋째, 전산검사의 경우에는 예방 통제의 일환으로 사전 배치(Batch) 작업에 대한 감사, 전산원장 변경에 대한 내부통제, 프로그램 변경 통제 등 운영에 영향을 미치는 일상적인 업무에 대하여 사전 감사를 실시한다. 이외에도 1개월에 1항목 이상을 자체 검사 계획에 의거 항목을 선정하고 1~2주 동안 해당 검사항목에 관련된 사항을 다양한 관점에서 제시하는 중점검사도 있다.

위에서 설명한 다양한 감사 활동들을 종합적으로 정리해 보면 다음과 같다. 먼저, 감독 당국의 감사는 외부 감사로서 공익적인 목적을 달성(법규나 기준의 준수 여부를 확인)하기 위한 준거성(compliance) 감사이다. 정보시스템 감사의 주요한 목적은 자산 보호, 데이터 무결성, 효과성, 효율성 등을 확보하는 것이다[14]. 이러한 목적에 비추어 본다면, 외부 감사는 효과성, 효율성보다는 자산 보호와 데이터 무결성 등에 초점을 맞추게 된다. 따라서 외부 감사에 대한 준비와 개선 권고안에 대한 조치를 취하고, 효율성/효과성에 초점을 맞추어 정보시스템에 대한 내부 통제를 검증하여 경영진에 정보를 제공하기 위한 기능, 즉 내부 감사 활동은 은행에 있어서 매

우 중요한 기능 중의 하나이다. 본 연구에서는 이처럼 중요한 기능 중의 하나인 A은행 자체의 내부 감사에 초점을 맞추어 분석한다.

4. 정보시스템 내부 감사의 현황 및 문제점

4.1 분석 프레임워크

다음에서는 A은행의 정보시스템 내부 감사의 현황 및 문제점을 파악하기 위한 분석 프레임워크에 대해서 설명한다. 본 연구에서는 A은행의 정보시스템 내부 감사의 현황 및 문제점을 크게 ① 감사 프로세스, ② 내부 감사 인력 및 조직의 두 가지 측면을 중심으로 평가한다.

감사 프로세스 측면에서는 정보시스템에 관련하여 A은행에서 수행하고 있는 모든 프로세스와 여기에 대한 감사 프로세스를 분석한다. 정보시스템에 관련된 프로세스를 파악하는 이유는 정보시스템 감사의 주요한 기능이 정보시스템 관련 프로세스에 대한 내부 통제의 존재 여부와 내부 통제의 효율성 및 효과성을 검증하고 여기에 대한 권고안을 제시하는 것이기 때문이다.

본 연구에서는 CobiT이라는 감사 지침을 기반으로 현재 A은행에서 수행하고 있는 IT 프로세스와 감사의 내용을 평가한다. CobiT(Control OBjectives for Information and related Technology)은 미국의 ISACA[1]라는 기관에서 개발하여 전세계적으로 활용되고 있는 감사 지침이다[10, 11]. CobiT에는 IT 자원(데이터, 응용 시스템, 기술, 시설, 인력)을 최적으로 활용하고, 조직이 생성/보유/사용하고 있는 정보가 자신들이 필요로 하는 특성(효과성, 효율성, 기밀성, 무결성, 가용성, 준거성, 신뢰성)을 가질 수 있도록 하기 위해서 수행해야 할 활동들을 4개의 업무 영역, 34개의 프로세스, 302개의 활동 및 작업으로 제시하고 있다. 다음의 <표 4>에는 CobiT에서 제시하고 있는 4개의 업무 영역, 각 업무 영역에서 수행해야 할 프로세스(총 34개 프로세스)가 정리되어 있다.

본 연구에서는 CobiT의 34개 프로세스 중에서 하나(M4 : 독립적인 감사 시행)를 제외한 33개 프로세스에 대해서 A은행에 있어서의 중요도, 각 프로세스의 수행 정도, 각 프로세스에 대한 감사 실시 정도 등의 항목을 분석하였다. 'M4 : 독립적인 감사 시행' 프로세스를 제외한 이유는 본 연구에서 각 프로세스에 대한 감사 수행 여부를 평가하기 때문이다.

감사 인력/조직의 측면에서는 다음과 같은 항목들을 분석하였다 : ① 인원 및 조직 현황, ② 감사 직무 활동 내역, ③ 감사 인력에 대한 일반 기준의 충족도. 첫째로 인원 및 조직 현황은 내부 감사 인력의 수와 및 감사 조직의 조직 내 위치를 평가하였다. 둘째로 감사 직무 활동에서는 직무 분석표를 바탕으로 감사 인력들이 어떤 업무를 수행하고 있는지를 평가하였다. 셋째로 감사 인력의 일반 기준에서는 감사 인력의 적격성(실무 경력, 교육, 경력관리)과 독립성(정신적 독립성, 외

〈표 4〉 COBIT의 업무 영역 및 프로세스

업무 영역	계획 및 조직 (Planning & Organization)		도입 및 구축 (Acquisition & Implementation)		운영 및 지원 (Delivery & Support)		모니터링 (Monitoring)	
프로세스	PO1	IT 전략 계획 수립	AI1	솔루션 도출	DS1	서비스 수준 정의	M1	프로세스 모니터링
	PO2	정보 아키텍처 정의	AI2	응용 소프트웨어 도입 및 유지·보수	DS2	외부업체 서비스 관리	M2	내부 통제의 적절성 평가
	PO3	기술 방향 결정	AI3	기술 아키텍쳐 도입 및 유지·보수	DS3	성능 및 용량 관리	M3	독립적인 보증 획득
	PO4	IT 조직 및 관계 정의	AI4	IT 절차 개발 및 유지·보수	DS4	서비스의 지속성 확보	M4	독립적인 감사 시행
	PO5	IT 투자 관리	AI5	시스템 설치 및 인가	DS5	시스템의 보안성 확보		
	PO6	경영진의 관리목표 및 방침 전파	AI6	변경 관리	DS6	비용 산정 및 배분		
	PO7	인적 자원 관리			DS7	사용자 교육 및 훈련		
	PO8	외부 요구사항의 준수			DS8	IT 고객의 지원 및 자문		
	PO9	위험 평가			DS9	형상 관리		
	PO10	프로젝트 관리			DS10	문제 및 사고 관리		
	PO11	품질 관리			DS11	데이터 관리		
					DS12	시설 관리		
					DS13	운영 관리		

1) ISACA(Information Systems Audit and Control Association)는 정보시스템 감사, 통제 및 보안 분야의 발전을 목적으로 1969년에 설립된 미국의 전문협회이다. 전세계 100개국에 140여개의 지부가 있고 20,000명 이상의 정보시스템 감사 전문가들이 회원으로 가입되어 있다. 이 협회는 1978년부터 CISA(Cerfified Information Systems Auditor) 자격인증 제도를 실시하고 있다. 국내에는 1987년에 최초로 1명이 합격한 이래 2001년 현재 약 900여명이 CISA 시험에 합격하였다.

관상 독립성)을 평가하였다.

본 연구의 분석 항목 및 측정 방법에 대한 내용은 다음의 <표 5>에 정리되어 있다.

〈표 5〉 분석 항목 및 측정 방법

분석 대상	세부 항목	측정 방법
감사 프로세스	IT 프로세스의 중요도	델파이 방법론(감사 인력 전원) 5점 척도 (1 : 전혀 중요하지 않음, 3 : 보통 5 : 매우 중요함)
	IT 프로세스의 수행 정도	델파이 방법론(감사 인력 전원) 5점 척도 (1 : 매우 미흡함, 3 : 보통 5 : 매우 잘 하고 있음)
	감사 실시 정도	델파이 방법론(감사 인력 전원) 5점 척도 (1 : 매우 미흡함, 3 : 보통 5 : 매우 잘 하고 있음)
내부 감사 인력 및 조직	인원 및 조직	업무 분장표/조직도 분석, 면담(감사 인력 전원)
	직무 활동 내역	직무분석표 분석
	감사 기준 충족도	감사지침 분석, 면담(감사 인력 전원)

4.2 감사 프로세스에 대한 분석

위에서 설명한 분석 프레임워크를 바탕으로 A은행의 내부 감사 프로세스를 분석하였다. 위의 <표 6>에서 정리되어 있는 바와 각 프로세스의 중요도, 수행 정도, 감사 실시 정도 등은 A은행의 모든 내부 감사인(3명)을 대상으로 한 델파이 방법론(Delphi Method)을 통해서 5점 척도에서 합의를 도출하였다. 델파이 방법론은 1950년대에 Rand Corporation이 객관적인 사실보다는 의견을 처리하기 위한 수단으로 개발되었다. 이 방법은 경영 분야의 연구에서 특정 문제에 대한 상대적인 중요성에 대해서 그룹의 일치된 의견을 도출하는데 많이 사용되고 있다[12].

분석 결과는 다음의 <표 6>에 정리되어 있다.

4.2.1 정보시스템 프로세스의 중요도

A은행의 내부 감사인들은 CobiT에서 제시하고 있는 33개 프로세스가 조직의 성공적인 운영에 중요한 프로세스로 인식하고 있는 것으로 나타났다(<표 7> 참조). 이것은 은행에 있어서 정보시스템의 중요성을 다시 한번 확인할 수 있는 결과이다.

4개의 업무 영역별로 봤을 때, 중요성은 계획 및 조직(4.75), 도입 및 구축(4.67), 모니터링(4.67), 운영 및 지원(4.38)의 순으로 나타났다. 각 영역간에 큰 차이는 없으나, 운영 및 지원이 가장 중요성이 낮게 나타난 이유는 은행에서 정보시스템을 운영해 온 역사가 길기 때문에, 유지·보수가 비교적 잘 되어 왔고 현 시스템에 대한 노하우가 축적되어 있기 때문인 것으로 판단된다. 이에 비해서 계획 및 조직 분야의 중요성이 높게 나타난 이유는 잘못된 의사결정으로 시스템을 신규 도

〈표 6〉 분석 결과

IT 프로세스		중요도	수행 정도	감사 정도
계획 및 조직(Planning & Organization)				
PO 1	IT 전략 계획 수립	5	3	2
PO 2	정보 아키텍쳐 정의	4	3	2
PO 3	기술 방향 결정	5	4	2
PO 4	IT 조직 및 관계 정의	5	3	2
PO 5	IT 투자 관리	5	3	2
PO 6	경영진의 관리 목표 및 방침 전파	4	3	2
PO 7	인적 자원 관리	4	2	2
PO 8	외부 요구사항의 준수	5	4	4
PO 9	위험 평가	5	2	2
PO 10	프로젝트 관리	5	3	2
PO 11	품질 관리	5	3	4
평 균		4.75	2.88	2.50
도입 및 구축(Acquisition & Implementation)				
AI 1	솔루션 도출	5	2	2
AI 2	응용 소프트웨어 도입 및 유지·보수	4	3	3
AI 3	기술 아키텍쳐 도입 및 유지·보수	5	2	2
AI 4	IT 절차 개발 및 유지·보수	5	2	4
AI 5	시스템 설치 및 인가	4	2	2
AI 6	변경 관리	5	3	4
평 균		4.67	2.33	2.83
운영 및 지원(Delivery & Support)				
DS 1	서비스 수준 정의	4	2	2
DS 2	외부업체 서비스 관리	4	3	2
DS 3	성능 및 용량 관리	4	3	3
DS 4	서비스의 지속성 확보	5	2	2
DS 5	시스템의 보안성 확보	5	3	4
DS 6	비용 산정 및 배분	4	2	2
DS 7	사용자 교육 및 훈련	4	3	2
DS 8	IT 고객의 지원 및 자문	4	2	2
DS 9	형상 관리	5	3	4
DS 10	문제 및 사고 관리	5	3	4
DS 11	데이터 관리	5	3	3
DS 12	시설 관리	4	3	2
DS 13	운영 관리	4	3	2
평 균		4.38	2.69	2.62
모니터링(Monitoring)				
M 1	프로세스 모니터링	5	2	4
M 2	내부 통제의 적절성 평가	5	2	2
M 3	독립적인 보증 획득	4	2	2
평 균		4.67	2.00	2.67
전 체 평 균		4.58	2.67	2.58

입하였을 경우 엄청난 비용의 낭비를 초래하고, 조직의 업무를 전략적으로 지원하지 못하는 것을 많이 경험했기 때문인 것으로 보인다.

〈표 7〉 프로세스의 중요도에 대한 인식

중 요 도	프로세스의 수	평 균
1점 (전혀 중요하지 않음)	0개	4.48
2점 (중요하지 않음)	0개	
3점 (보통)	0개	
4점 (중요함)	14개	
5점 (매우 중요함)	19개	
합 계	33개	

4.2.2 정보시스템 프로세스의 수행 정도

전체적으로 정보시스템 프로세스의 수행 정도는 보통 수준 이하로 나타났다(<표 8> 참조). 이 중에서도 특히 모니터링 영역의 프로세스가 가장 잘 수행되고 있지 않는 것으로 나타났다(평균 : 2.0).

〈표 8〉 정보시스템 프로세스의 수행 정도에 대한 인식

수행 정도	프로세스의 수	평 균
1점 (매우 미흡함)	0개	2.67
2점 (미흡함)	13개	
3점 (보통)	18개	
4점 (잘 하고 있음)	2개	
5점 (매우 잘 하고 있음)	0개	
합 계	33개	

프로세스의 수행 정도를 프로세스의 중요도와 비교·분석해 보았다. 즉 프로세스의 전반적인 수행 정도는 좋지 않더라도, 매우 중요한 프로세스는 매우 잘 수행하고 있고, 전혀 중요하지 않은 프로세스는 미흡하게 수행하고 있다면, 긍정적인 결과로 볼 수 있을 것이다. 이러한 분석을 위해서 프로세스의 중요도와 프로세스의 수행 정도간의 상관계수를 계산하였다. 다음의 <표 9>에는 각 변수들간의 상관계수와 유의 확률(괄호안의 수치)이 정리되어 있다. 중요도와 수행 정도간의 상관 계수는 0.1395로서 통계적으로 유의하지 않은 것으로 나타났다. 이것은 전반적인 수행정도도 좋지 않을 뿐만 아니라 중요성이 높은 프로세스를 상대적으로 잘 수행하고 있지도 못하다는 것을 나타내는 결과이다.

이에 따라 중요성은 높으나 수행이 잘 되고 있지 않는 프로세스를 식별하기 위해서 중요도와 수행 정도간의 차이를 살펴보았다. 그 결과는 다음의 <표 10>에 정리되어 있다. 이 중에서 특히 중요도와 수행 정도의 차이가 가장 많이 나는 7개의 프로세스는 다음과 같다 : PO9 : 위험 평가, AI1 : 솔루션 도출, AI3 : 기술 아키텍쳐 도입 및 유지보수, AI4 : 시스템 설치 및 인가, DS4 : 서비스의 지속성 확보, M1 : 프로세스 모니터링, M2 : 내부 통제의 적절성 평가. 이러한 프로세스에 대해서는 경영진이 관리 활동을 계획하고, 감사인들이 감사 활동을 계획할 때, 노력을 집중시켜야 할 부문으로 판단된다.

〈표 9〉 변수들간의 상관계수

	중 요 도	수행 정도	감사 정도
중 요 도	-	0.1395 (0.439)	0.4352* (0.011)
수행 정도		-	0.2624 (0.140)
감사 정도			-

* : 0.05 수준에서 유의

〈표 10〉 중요도와 수행 정도간의 차이

중요도와 수행 정도와의 차이	프로세스의 수
1점	10개
2점	16개
3점	7개
합 계	33개

4.2.3 감사 실시 정도

감사인들 자신들은 전반적으로 감사 실시 정도가 보통 수준 이하인 것으로 평가하였다(<표 11> 참조). 각 업무 영역간에 큰 차이는 없었으나, 감사 실시 정도는 도입 및 구축(2.83), 모니터링(2.67), 운영 및 지원(2.62), 계획 및 조직(2.50)의 순으로 나타났다.

〈표 11〉 감사 실시 정도에 대한 인식

감사 실시 정도	프로세스의 수	평 균
1점 (매우 미흡함)	0개	2.58
2점 (미흡함)	22개	
3점 (보통)	3개	
4점 (잘 하고 있음)	8개	
5점 (매우 잘 하고 있음)	0개	
합 계	33개	

감사 실시 정도와 프로세스의 중요도간의 상관 관계를 분석하였다. 이것은 전반적인 감사 실시 정도는 좋지 않더라도, 중요도가 높은 프로세스에 대해서 상대적으로 감사를 잘 시행하고 있는지를 살펴 보기 위해서이다. 상관계수는 위의 <표 9>에서 볼 수 있는 바와 같이 0.4352로서 0.05수준에서 통계적으로 유의한 것으로 나타났다. 이 결과는 정보시스템 감사가 중요한 프로세스에 초점을 맞추고 있다는 긍정적인 결과이다.

이에 비해서 감사 실시 정도와 수행 정도와의 관계는 다소 부정적인 결과를 제시하고 있다. 즉 상관 계수는 0.2614로서 통계적으로 유의하지 못하고, 이러한 결과는 감사가 프로세스의 수행에 긍정적인 영향을 미치지 못하고 있다는 것을 의

미한다. 특히 중요성과 수행 정도가 차이가 많이 나는 7개 프로세스를 살펴본 결과가 다음의 <표 12>에 정리되어 있다. 이를 통해서 다음과 같은 2가지 사항을 살펴볼 수 있다. 첫째, 전반적으로 7개 프로세스에 대한 감사가 잘 이루어지지 않고 있다는 것을 알 수 있다. 둘째로는 이 중 2개 프로세스(AI4, M1)에 대해서는 감사가 잘 시행되고 있으나 그 결과는 좋지 않다는 점이다. 이러한 결과의 원인으로는 다음과 같은 것들을 들 수 있다. 감사 권고사항이 적절하지 못했거나, 감사 권고사항을 현업에서 잘 따르지 않았거나, 권고사항의 이행여부를 감사부서에서 사후관리하지 못했거나 이행하도록 할 만한 권한이 부족한 것 등으로 해석될 수 있다.

〈표 12〉 7개 프로세스에 대한 감사실시 정도

프 로 세 스	감사실시 정도
PO9 : 위험 평가	2
AI1 : 솔루션 도출	2
AI3 : 기술 아키텍처 도입 및 유지보수	2
AI4 : IT절차 개발 및 유지보수	4
DS4 : 서비스의 지속성 확보	2
M1 : 프로세스 모니터링	4
M2 : 내부 통제의 적절성 평가	2

4.3 감사 인력/조직에 대한 분석

4.3.1 인원 및 조직 현황

현재 A은행에서 정보시스템 감사 기능을 수행하는 모든 조직을 망라해 보면 크게 ① 감사위원회 산하의 검사부, ② 정보기술 부문장 산하의 전산감사반, ③ 정보기획팀 산하의 품질 관리 등의 세 가지 조직이 수 있다.

첫째, 감사위원회 산하 검사부의 대부분의 인력들은 일선 영업부서의 영업 활동에 관련된 사항(예 : 여신의 부실, 위험 탐지 등)을 감사하고 있고, 제 3장에서 설명한 바와 같이 IT 부문에 대한 감사로는 매일 수행하는 상시검사와 1년에 2회 실시하는 일반검사가 있다. 따라서 검사부에서 정보시스템 감사에 관련된 인원을 산정하기 위해서 Man Day의 개념을 적용하였다. 아래의 <표 13>에서 볼 수 있는 바와 같이 검사부의 정보시스템 관련 인원은 0.67명으로 볼 수 있다.

〈표 13〉 검사부의 IT 감사 인력 수 산정

검사부의 전체 Man Day(M/D)	60명×365일 = 21,900 M/D
IT 검사인력(전담)	0.5명×365일 = 205 M/D
분기별 정기검사 인력	(5명×4일)×2(1년에 2회) = 40 M/D
IT 검사 인력 합계	245 M/D 245 M/D / 365일 = 0.67명

둘째, 정보기술 부문장 산하의 전산감사반은 3명으로 구성되어 있고(4급 직원(대리) 1명, 5급직원(행원) 2명), 이들의 경력은 다음의 <표 14>와 같다.

〈표 14〉 전산감사반 감사인력의 경력

감사인	정보시스템 경력	감사 경력	보유 전문자격
1	10년	2년	
2	8년	2년	
3	1년	1년	CISA

셋째, 정보기획팀 산하의 품질 관리조직의 경우, 총 8명으로 구성되어 있고, 주요한 기능은 서비스 수준 관리, 업무개선, 방법론, 품질보증, 형상관리, 프로젝트관리 등의 업무를 수행하고 있다[8]. 이 중에서 정보시스템 감사와 관련된 기능으로는 사후 품질관리 활동을 들 수 있는데, 여기에는 1명이 다른 업무와 겸임을 하고 있으므로 0.5명으로 산정할 수 있다.

따라서 A은행에서 정보시스템 감사에 관련된 모든 인력의 수는 최대 4.17명으로 볼 수 있다. 적정 감사 인력의 수에 대한 일반적인 기준은 존재하지 않지만, 활용할 수 있는 하나의 평가 모델은 단순 인력 규모에 의한 감사 소요 인력 추정 모델[6]이다. 이 모델에서는 다음과 같은 기준을 제시하고 있다(<표 15> 참조).

〈표 15〉 감사 소요 인력 추정 모델

전산조직의 규모 (인원수)	전산인력에 대한 전산감사 인력의 비율
소규모 (0~40명)	10명~15명에 대해 1인
중규모 (40~400명)	20명~30명에 대해 1인
대규모 (400~1,500명)	40명~50명에 대해 1인
초대형 (1,500~5,000명)	75명~100명에 대해 1인

이 모델을 기준으로 하면, A은행의 경우 전산 인력의 수는 약 400명이고 따라서 감사 인력의 수는 최소 8명에서 최대 10명까지 필요한 것으로 추정된다. 따라서 A은행의 경우에는 4~6명이 부족한 것으로 판단된다.

4.3.2 감사 직무 활동 내역

A은행의 감사 인력들이 수행하는 직무의 내용을 분석해 보았다. 2000년도 ABC 직무 분석표를 기준으로 활동을 분석한 결과는 다음의 <표 16>에 정리되어 있다.

아래의 표에서 볼 수 있는 바와 같이 3명의 전담 감사인들이 자신들의 업무 시간의 90%를 전산 감사 고유업무에 할애하고 있는 것으로 조사되었다. 그러나 현재 수행하고 있는 정보시스템감사 분야는 주로 정보시스템의 운영에 관련된 기술적인 감사에 국한되어 있고, 관리나 기획, 시스템 설계 및 개발 등과 같은 부문에 대한 감사는 이루어지지 않고 있다는 것을 알 수 있다. 또한 정보시스템에 관련된 내부 통제 연구 등과 같은 연구 조사 업무에 0.15명이 할애되고 있어서 신기술을 연구하고 새로운 감사 기법을 연구할 시간적 여유가 없는 것으로 판단된다.

〈표 16〉 2000년도 감사 인력의 직무 내용 분석

담당 업무	세부 업무	정규 인력의 수 (비중)
고유 업무	전사 감사 수행	1.50 (50%)
	계정계 작업통제 시스템 내부 통제	0.30 (10%)
	부문별 자기 검사 제도 운영	0.30 (10%)
	자원접근통제설비 운영업무 감사 및 프로그램 변경관리 업무 내부 통제	0.45 (15%)
	정보기술 부문 내부 통제 연구	0.15 (5%)
	소 계	2.70 (90%)
지원 업무	감사 수감 (검사부, 금융감독원, 회계 법인 등)	0.15 (5%)
타부서 업무	감사 관련 행정 업무 협조	0.15 (5%)
합 계		3.0명 (100%)

4.3.3 감사 인력에 대한 일반 기준의 충족도

감사 인력에 대한 일반 기준의 충족도를 분석하였다. 일반 기준에는 적격성, 독립성 등이 포함된다[5].

먼저 감사 인력의 적격성이란 해당 분야에 대한 충분한 지식과 실무 경험 및 전문 직업인으로서의 책임을 다 할 수 있는 자질을 보유하고 있어야 한다는 것을 말한다. 적격성의 평가를 위해서 실무 경력, 교육 체계, 경력 관리 프로그램 등을 분석하였다. 첫째, 실무 경력 측면에서는 전절에서 본 바와 같이 현재 A은행의 감사 인력들은 1명의 신입 인력을 제외하면 정보시스템에 관한 실무 경력은 보유하고 있지만, 감사에 관한 실무 경험은 다소 미흡한 것으로 판단된다. 둘째로 감사 관련 교육 체계의 측면에서는 인력이 소수인 관계로 감사 관련 교육 체계가 존재하지 않고, 정보시스템에 관련된 일반적인 교육을 이수하고 있는 것으로 파악되었다. 셋째로, 경력관리 프로그램 측면에서는 개인의 업무별 경력 관리는 시행하고 있으나, 이것은 감사 목적이 아닌 정보시스템 전체 인력 관리를 위한 것으로 감사 인력에 대한 지속적인 경력관리는 시행하지 못하고 있는 것으로 조사되었다.

다음으로 감사 인력의 독립성이란 감사와 관련된 업무를 수행함에 있어서 정신적인 독립성을 유지하고 외관상으로 독립성에 의문을 초래할만한 이해 관계가 있는 경우에는 해당 감사에 관여해서는 안된다는 것을 의미한다. A은행의 경우, 감사업무 지침 상 감사 인력의 독립성이 보장되어 있고, 직제상 감사 대상 인력들로부터 신분적으로 분리되어 있어서 외관상의 독립성을 유지하고 있는 것으로 보인다. 그러나 A은행은 전산감사반의 인력과 정보시스템 부문의 인력의 직무를 순환 보직하고 있기 때문에 감사 인력과 감사 대상 인력들과의 정신적인 독립성을 유지하기가 어려운 것으로 판단된다.

5. 정보시스템 내부 감사의 문제점 및 개선 방안

앞에서 분석한 결과를 바탕으로 현재 A은행의 정보시스템 감사 부문이 안고 있는 문제점은 크게 다음과 같은 세 가지 측면에서 정리해 볼 수 있다 : ① 정보시스템 내부 감사 조직, ② 정보시스템 감사에 대한 전문성, ③ 정보시스템 감사 프로세스. 아래에서는 이러한 세 가지 측면의 문제점을 설명하고, 여기에 대한 개선 방향을 제시하도록 한다.

첫째, 감사 조직적인 측면에서 A은행은 전산감사반의 독립성 부족, 감사 조직의 이원화 및 연계성 부족, 감사 인력의 부족 등의 문제점을 가지고 있다.

전산감사반의 독립성 부족 : A은행의 전산감사반은 정보시스템 부서장 직속으로 되어 있으나 감사를 받는 정보시스템 부서에 속해 있고, 감사 인력들이 정보시스템 인력과 순환 보직을 하고 있기 때문에 독립성을 유지하지 못하고 있다. 이러한 문제를 해결하기 위해서는 전산감사반을 독립적인 검사부에 통합하는 것이 가장 이상적이지만, 단기적으로는 검사부가 정보시스템 부문의 관리자들의 의사결정에 대한 타당성을 감사한다면 전산감사반의 독립성 부족을 보완할 수 있을 것이다. 또한 외부의 전문 정보시스템 감사 기관을 활용하는 방안도 타당성이 있을 것이다. 외부 감사는 자체 감사가 가지고 있는 독립성의 한계를 극복할 수 있고, 사회 및 시장에서 원하는 시각에 따라 정보시스템을 감사할 수 있을 것이다. 외부 감사를 실시하게 되면, 은행 자체의 정보가 외부에 알려지게 되고, 이에 따라 은행은 정보시스템의 내부통제 활동을 강화하도록 하는 동기를 부여하게 될 수 있을 것이다.

감사 조직의 이원화 및 연계성 부족 : A은행의 정보시스템 감사 담당 조직은 감사위원회 산하의 검사부와 정보시스템 부서장 산하의 전산감사반으로 이원화되어 있고, 이들간에 긴밀한 연계 관계를 가지고 있지 못하다. 이러한 문제를 개선하기 위한 방안으로는 장기적으로는 두 조직을 통합하거나 단기적으로는 두 조직간의 적절한 역할 분담을 통해서 이러한 문제점을 보완할 수 있을 것이다. 예를 들면, 전산감사반은 주로 준거성 감사에 초점을 맞추어 지침의 이행 여부, 절차의 준수 여부 등을 주로 감사하고, 검사부는 시스템 개발 및 운영의 효율성 및 시스템 활용 성과에 대한 효과성 감사를 수행하는 방안을 들 수 있다.

감사 인력의 부족 : A은행에 있어서 감사 인력의 수는 부족한 실정이다. 이에 따라 정보시스템 감사의 초점은 사고 예방 수준에 머물고 있고, 정보시스템 분야의 신기술을 연구하고 새로운 감사 기법을 연구할 시간적 여유를 가지지 못하고 있다. 이러한 문제를 해결하기 위해서는 적정 규모의 검사 인력을 충원해야 할 필요가 있다. 장기적으로는 인력 수급 계획을 수립하여 이 계획 하에서 외부 인력의 충원과 내부 인력 등을 평가하고, 이 계획에 따라 전문성을 갖춘 인력을 확보할 필요가 있다. 그러나 단기적으로는 다음과 같은 세 가지 방안을 고려할 필요가 있다. 첫째, 정보시스템 인력 중에서 업무 경험이 풍부하거나 감사 관련 지식을 갖추고 있는 내부 인력

을 배치하는 방안을 고려할 필요가 있다. 둘째, 감사 도구의 개발 및 적극적인 활용을 통해서 감사의 생산성 및 효율성을 향상시킬 수 있을 것이다. 정보시스템 감사, 그 중에서도 특히 데이터와 응용에 대한 감사에 있어서의 어려움은 거래 증적(audit trail)의 무가시성으로 인하여 감사 업무 수행 자체가 불가능하거나, 입출력 자료만으로 컴퓨터 주변감사(audit around the computer)를 수행하는 경우 자료의 양이 방대하여 많은 시간을 소요하게 되는 경우에는 적극적으로 감사 도구를 활용할 필요가 있다. 감사 도구의 활용은 감사 인력의 부족 현상을 보완할 수 있을 것이다. 셋째, 자가통제평가(Control of Self Assessment) 제도의 도입을 고려할 필요가 있다. 정보시스템에 대한 감사 통제에 있어서 각 부문별 담당자가 자신의 전문기술, 지식, 경험, 통찰력 등을 바탕으로 직접 자기가 담당하고 있는 업무에 대한 위험성을 평가하고, 프로세스를 통제하고 개선하는 것이 자가통제평가 제도이다. 물론, 자가통제평가 제도는 독립성에 문제가 있지만, 감사 인력 부족 현상을 보완할 수 있는 제도이다.

둘째, 정보시스템 감사에 대한 전문성 측면에서 A은행은 정보시스템 감사 지침의 미비, 감사 인력에 대한 교육 및 경력관리 체계 미흡 등의 문제점을 가지고 있다.

정보시스템 감사 매뉴얼의 미비 : 현재 A은행은 협업에 대한 규정 및 지침이 세분화되어 일정 수준의 지식관리가 되고 있다. 그러나 정보시스템 감사 기능에 대해서는 감사 인력이 소수이고 관련 업무가 명확하게 규정되어 있지 않아서 감사 인력들이 감사시 참고하고 준수해야 할 감사 지침 매뉴얼의 내용이 미흡하고, 감사인 개인의 암묵적인 지식에 의존하는 경향이 높다. 따라서 CobiT 등과 같은 선진 감사 지침을 참조하여 감사 업무를 표준화하고, 감사 업무에 대한 세부적인 지침을 작성할 필요가 있다. 기존의 감사 매뉴얼로는 새로운 기술 발전으로 빠르게 변화하고 복잡해져가는 IT IT 환경의 수요를 감당하기 어렵다. 따라서 이러한 변화에 수반되는 위험을 적절하게 관리하기 위해서는 감사반 내에 별도의 인력을 할당하여 감사 항목과 방법을 지속적으로 연구 · 개발하여 기존의 감사 지침에 반영할 필요가 있다.

감사 인력에 대한 교육 및 경력관리 체계 미흡 : A은행의 경우, 감사 관련 교육 체계가 존재하지 않고, 감사인력을 대상으로한 경력 관리 프로그램이 시행되지 못하고 있다. 전문성 있는 감사를 통해서 품질 높은 감사 결과를 얻기 위해서는 인력의 채용에서부터 경력 관리, 교육, 성과 보상에 이르는 전반적인 인력관리 모델을 수립하여 이를 시행할 필요가 있다. 감사인력에 대한 적격성 기준을 수립하여 이에 부합하는 인력을 채용하고, 기존의 감사 인력을 지속적으로 재교육을 할 수 있는 교육 및 경력 관리 프로그램의 도입하고, 감사 인력의 성과를 객관적으로 평가하여 적절한 보상을 제공함으로써 감사의 품질을 향상시킬 수 있을 것이다.

마지막으로 A은행은 감사 프로세스적인 측면에서 감사 계획의 미흡, 감사 사후 관리의 미흡 등의 문제를 가지고 있다.

감사 계획의 미흡 : 현재 A은행의 정보시스템 감사는 중요한 프로세스에 초점을 맞추고 있다는 긍정적인 증거도 있지만, 중요하지만 잘 수행되고 있지 않은 프로세스에 대한 감사가 제대로 수행되지 않고 있다(<표 12> 참조). 현재 A은행의 감사 계획은 이전의 감사 결과, 프로세스의 수행 정보 등을 바탕으로 효과적인 감사 계획이 수립되지 못하고 있다고 판단된다. 따라서 제한된 감사 자원을 효율적이고 효과적으로 활용하기 위해서는 프로세스에 대한 정확한 평가를 바탕으로 한 감사 계획이 수립되어야 한다. 한정된 인력과 자원하에서 이러한 문제를 보완하는 방안으로는 미국의 연방금융기관 검사협의회(FFIEC)[2]의 위험 기반 검사 제도를(Risk-based Audit) 도입할 필요가 있다. 감사 계획 수립 시 정보기술 분야에 대한 위험 수준과 위험 관리 수준을 평가하여 취약한 분야에 중점적으로 감사 계획을 수립하고 실시함으로써 감사의 효과를 높일 수 있다.

감사 사후 관리의 미흡 : 감사의 궁극적인 목적은 잘못된 사항의 지적이 아니라 개선 및 향상이다. 따라서 감사 프로세스의 종료 시점은 감사의 실행 완료 시점이 아니라 감사를 통해서 지적한 권고사항이 적시에 제대로 이행되었는지를 검증하는 사후관리가 완료되었을 때이다. A은행의 경우에는, 감사를 잘 시행한 것으로 인식하고 있는 프로세스 중에서 수행 정도가 낮은 프로세스들이 존재하고 있다(<표 12> 참조). 따라서 감사부서에서는 권고사항들의 이행 여부를 검토하는 사후 관리 프로세스를 강화하고, 감사부서가 감사권고 사항을 현업에서 잘 따를 수 있도록 경영진은 감사부서에 적절한 권한을 부여해야 할 것으로 판단된다.

6. 결 론

현재 국내의 은행들은 구조 조정 과정을 겪고 있고, 따라서 현재의 시점에서는 정보시스템 및 정보시스템 감사에 대한 관심이 구조 조정보다는 우선 순위가 낮을 수밖에 없다. 그러나 구조 조정이 완료된 후 정상적인 운영 상태에서는 정보시스템의 효율적/효과적인 운영은 은행의 생존 및 경쟁력 확보에 매우 중대한 영향을 미칠 것이다.

본 연구에서는 선진 감사 지침(CobiT)을 바탕으로 A은행에 있어서의 정보시스템 감사의 현황 및 문제점을 진단하고 개선 방안을 제시하였다. 따라서 본 연구의 결과는 은행업, 더 나아가서 다른 산업에 속한 기업들도 참고할 수 있는 시사점을 제공할 수 있을 것으로 판단된다. 또한 본 연구에서

2) Federal Financial Institutions Examination Council

활용한 분석 프레임워크는 향후 정보시스템 감사 분야의 학술적인 연구에서 활용될 수 있을 것이다.

그러나 본 연구는 다음과 같은 몇 가지 한계점을 가지고 있다. 첫째, 연구 방법적인 측면에서 사례 연구 방법을 택함으로써 연구의 결과를 일반화시킬 수 없다는 한계점을 가지고 있다. 둘째, 변수의 측정 측면에서, 감사 프로세스에 대한 분석 항목인 IT 프로세스의 중요도, 수행정도, 감사실시 정도 등을 감사인만을 대상으로 하였고, 또한 감사인들의 주관적인 인식에 의존하였다. 셋째, 문제점 분석을 바탕으로 제시한 개선안은 세부적인 방안이라기 보다 전반적인 방향만을 제시하였다. 따라서 향후 연구의 방향은 변수의 보다 객관적인 측정을 위한 연구와 이를 바탕으로 설문조사(Survey) 연구 방법을 통해서 연구 결과를 일반화시키는 연구가 이루어져야 할 것으로 판단된다.

오늘날 정보시스템 감사의 개념은 정보기술의 종합적인 관리(IT Governance)의 개념으로 확대 발전하고 있다. 따라서 정보 및 정보시스템의 중요성이 매우 높은 은행업에서는 정보시스템 감사에 대한 인식을 제고하여 정비하고, 학술적으로는 보다 심도있는 연구가 수행되어야 할 것으로 판단된다.

참 고 문 헌

[1] 금융감독원, *금융기관 IT 경영 평가 지침 및 세부 항목*, 금융감독원, 1999.

[2] 김현수, *정보시스템 진단과 감리*, 법영사, 1998.

[3] 김회섭, "사이버범죄 1년새 4배 늘어", *조선일보*, 2000.

[4] 문대원, 장시영, *정보시스템 감리*, 명경사, 1998.

[5] 박태승, *신회계감사*, 세학사, 1999.

[6] 이재권, "정보시스템 통제 및 감사", *정보시스템 감사와 정보보안 체계 구축 및 운영과정 세미나*, 서강대학교 정보공학연구회, 1996.

[7] 전영하, "금융기관 IT 평가 실태 대응사례", *정보시스템 감사 통제 세미나*, 2001.

[8] A은행, 직무기술서, 2001.

[9] A은행 검사부, *지점 검사 및 금융 사고 예방 업무*, A은행, 1999.

[10] Information Systems Audit and Control Association(ISACA), *CobiT II*, ISACA, 1998.

[11] Information Systems Audit and Control Association(ISACA), *CobiT III*, ISACA, 2000.

[12] Schmidt, R. C., "Managing Delphi Surveys Using Nonparametric Statistical Techniques," Decision Sciences, Vol. 28. Issue 3, Summer 1997, pp.763-774.

[13] U.S. Department of Commerce, *Emerging Digital Economy*, U.S. Department of Commerce, 1998.

[14] Weber, R., *Information Systems Control and Audit*, Prentice Hall, 1999.

황 경 태

e-mail : kthwang@dongguk.edu

1983년 연세대학교 상경대학 응용통계학과 졸업(경제학사)

1986년 George Washington대학 경영학과 졸업(경영학 석사)

1991년 State University of New York at Buffalo 경영정보학과 졸업(경영학 박사)

1993년~1994년, 삼성데이타시스템 컨설팅팀 팀장, 삼성회장비서실 정보전략 담당

1994년~현재, 동국대학교 경상대학 정보관리학과 부교수

관심분야 : 정보시스템 전략, 통제 및 감사, e-비즈니스

김 송 주

e-mail : cisakim@hanmail.net

1997년 동국대학교 경상대학 정보관리학과 졸업(경영학사)

2000년 동국대학교 언론정보대학원 졸업(경영학 석사)

1988년~현재 국민은행 전산정보본부

관심분야 : 정보시스템 감사 통제, 정보시스템 보안