韓國 컴퓨터情報 學會誌
第11卷 第1號, 2003. 12

정보시스템 구축과 내부 감사 제어에 대한 고찰

변 진 식

The Study of Information System Creation and Internal Audit Controls

Byun jinsik

요 약

우리나라에서도 정보통신부는 국가 및 공공기관의 전산망 품질수준을 제고하고 효율적인 정보시스템 구축을 지원하기 위해 공공부문 정보화사업에 대한 감리 제도의 활성화, 정보시스템 감리 자격제 도입, 민간 감리 기관의 육성 등을 주요 내용으로 하는「정보시스템 감리 제도 도입계획」을 마련해 본격 시행에 들어가기로 했다. 정통부가 이번에 정보시스템 감리제도를 크게 강화하기로 한 것은 최근 들어 국가 및 공공기관을 중심으로 정보시스템 분야의 감리 수요가 폭발적으로 증가하고 있음에도 불구하고 한국전산원에 감리 업무가 집중되고 있어 공공부문의 감리 수요를 충족시키기 힘든 데다 국가정보화 사업에 대한 감리 제도의 도입 필요성이 점차 높아지고 있기 때문으로 풀이된다. 정통부는 감리 제도를 활성화하기 위해 공공부문 정보시스템 감리를 정보화사업과 연계해 제도화한다는 방침을 세우고 공공부문 정보화사업에 대한 감리를 주관기관의 판단에 일임하되 정보화 추진위원회가 정한 국가적인 중요 사업에 대해선 감리를 의무화하기로 했다. 이에 대해 내, 외부 감사중 내부감사에 대해 그 내용을 파악해 보자는 데 그 목적이 있다.

Abstract

Along with trends of other countries, the Ministry of Information and Communication in Korea decided to operate an Information System Audit Institution for raising quality of computer network facilitated in state organ and public institution, and to construct effective construction of information

1) 동명대학 영상정보과 교수

system. The aim of the audit institution is applying it to public information business, establishing an information system audit qualification system, and upbringing private audit organs. The Ministry of Information and Communication realized that although the demand of information system area audit is explosively expanding, the National Computerization Agency cannot satisfies the demand and realize to have audit control for the information of national business as well. The Ministry of Information and Communication plan to enforce the audit on public information business by correlate with information business. The ministry enforce that the supervisory company has major roll to audit and national import business decided by the Information Promotion Committee is subject to have audit control. Therefore, in this paper, the contents of internal audit among internal/external audit will be presented.

▶ KEY WORDS : 정보시스템 감리제도 : 「정보시스템 감리 제도 도입계획」 내부감사 감사의 착안점

Ⅰ. 서론

1960년대 후반부터 조직(기업 등)에서의 컴퓨터를 이용한 정보처리가 가속화되었다. 이러한 상황에서의 초기 정보시스템 감리는 "내부통제를 위한 표준. 규정, 조직의 확립 및 유효성을 조사"하는 형태로 시작되었다. 70년대 후반 정보시스템감사에 관련된 연구가 활발해지고 금융기관에서부터 시작된 내부감사제도가 일반화되고, 보안에 대한 인식이 확산되기 시작하였다. 80년대 후반 들어 정보화의 역기능은 컴퓨터 범죄로 이어졌으며 정보시스템 감사의 필요성을 심각하게 인식하게 되는 계기가 되었다. 미국에서 1969년 EDPAA라는 이름으로 오늘날 ISACA(Information System Audit and Control Association : 정보시스템 감사통제협회)가 창설되었다. 협회에서는 1980년부터 CISA (Certified Information Systems Auditor : 국제공인 정보시스템 감사사)라는 시험제도를 실시해오고 있으며 전세계적으로 10,000여명이 활발히 활동하고 있다. 또한 국내에서도 1987년 1명의 합격자를 필두로 100여명의 CISA가 탄생하였다. 미국과 유럽의 경우는 CISA를 CPA(공인회계사)와 동일한 수준에서 정보시스템 감사를 하는 전문가로 인정하고 있으며, 일본은 CISA와 1986년부터 정보처리기술자 시험 합격자를 같이 인정하고 있는 실정이다. 동남아 국가에서도 CISA의 활동이 활발한 상황이다. 국내에서는 1987년 국가기관 등의 "전산망사업에 대한 타당성 검토 및 감리" 등의 수행업무를 목적으로 설립된 한국전산원에서 공공기관을 중심으로 정보시스템 감리를 수행하고 있으며, 최근 들어 정보시스템감사/감리만을 전문적으로 서비스하는 민간법인이 활동하고 있다. 현재의 산업, 사회 환경은 정보를 중심으로 네트워크화 된 형태로 변화되고 있으며, 정보화의 명암 또는 허실에 대한 통찰력을 요구하고 있다

Ⅱ. 내부통제 정보시스템 감사

내부통제는 컴퓨터를 이용하는 조직이 점차 증가하고, 이에 따라 회계관리업무를 포함한 대부분의 업무가 전산화되기 시작하면서 차츰 전산업무분야에서도 통용되기 시작하였다. 즉, 회계사에 의한 전산시스템(주로 회계 관리 전산화

시스템)의 감사가 실시되면서부터 자연스럽게 등장한 것이다.

이와 같은 내부통제의 정의에 기초하여 전산환경에서의 내부통제를 정의하면, 내부통제는 조직의 목적을 달성하기 위해 전산체계를 보호하고 데이터의 정확성과 완전성을 높이며, 이를 저해하는 위험요소들을 제거하기 위한 모든 수단 및 절차라고 정의할 수 있다. 전산감리는 이러한 전산환경에서의 내부통제를 검증하고 평가하는 행위라고 할 수 있다.

[내부통제 개념의 비교]

구분	경영통제이론상의 통제	회계감사이론	
		전통적 내부통제	새로운 내부통제
개념	· 목표(계획)의 달성을 위한 계획과 집행 결과의 차이분석 및 사후 조치	· 관리통제 · 회계통제	· 통제환경 · 회계제도 · 통제절차
목적	· 목표달성정도의 확인 및 차기목표수립의 기초자료제공	· 경영능률의 촉진 · 경영정책준수의 촉진 · 자산과 기록의 보호 · 신뢰성있는 회계정보 제공	· 기업의 특정한 경영목표 달성에 합리적 확신을 제공

III. 감사의 종류

감사의 종류는 다음과 같다.

(1) Application 시스템 통제의 감사
(2) Data Integrity의 감사
(3) 시스템 개발 Life cycle의 감사
(4) Application 개발의 감사
(5) Application 시스템 통제의 감사
(6) 안전통제(Security)의 감사
(7) 시스템 소프트웨어의 감사
(8) 보수절차(Maintenance)의 감사
(9) 컴퓨터 자원 취득에 관한 감사
(10) 데이터 처리 자원관리의 감사
(11) 정보시스템 감사의 관리

이중 본 논고에서는 컴퓨터 자원 취득에 관한 감사에 대해 알아보고자 한다.

(1) 개 요

컴퓨터 자원의 취득에 관한 감사의 목적은 다음과 같은 것을 검증하는 것이다.

a. 취득하려고 하는 하드웨어, 소프트웨어 및 서비스가 사업체의 요구를 충족시키는데 적절하다는 것을 보증할 수 있도록 충분한 계획이 수립되어 있다.
b. 메이커의 제안을 평가하기 위하여 사용한 방법 및 기준이 적절하고 타당하다.
c. 사업체의 이익을 보호하기 위하여 다른 공정한 계약도 고려하고 있다.

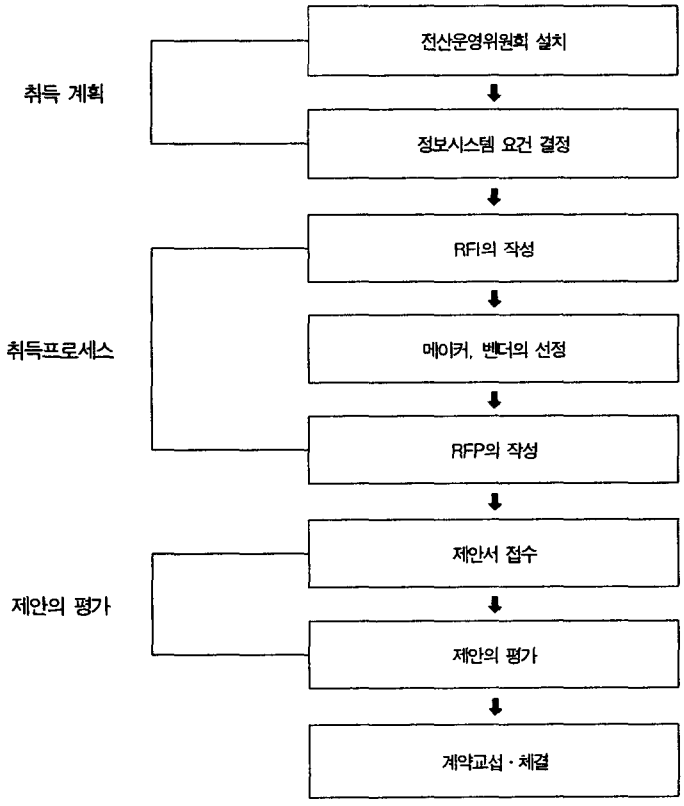
컴퓨터 자원의 취득은 초기취득(사업체가 하드웨어, 소프트웨어 또는 컴퓨터 서비스를 처음 취득하는 경우)으로 나눌 수가 있다. 초기취득은 추가취득의 경우에 기본적으로는 같은 방법을 채택해야 한다. 마찬가지로 이 프로세스는 대형 컴퓨터의 취득에도 미니 컴퓨터의 취득에도 적용된다. 주요한 차이점은 취득하려고 하는 하드웨어, 소프트웨어 또는 서비스의 복잡도이다.

(2) 취득계획(Acquisition Planning)

데이터 처리자원의 취득 시에는 일정한 규범과 치밀성이 요구된다. 가장 먼저 해야 할 일은 기업의 정보시스템 요구를 명확히 하는 것이다. 대부분의 사업체에서는 정보시스템 요구를 파악하고, 거기에 우선순위를 매기는 임무를 하게 되는 전산운영위원회를 두고 있다.

(3) 취득 프로세스(Acquisition Process)

정보시스템 요건에 대한 결정이 끝나면 컴퓨터 하드웨어, 소프트웨어 및 서비스를 취득하게 된다(그림 1 참조). 경우에 따라서는 자료 의뢰서(RFI, Request for Information)가 작성되는데, 이는 필요한 하드웨어 및 소프트웨어의 제공에 관심이 있는 적절한 메이커를 찾아내는 것을 목적으로 한다.



〈그림 1〉 취득과정

(4) 제안의 평가(Evaluation of Proposals)

정보시스템 감사인은 메이커 제안에 대한 타당한 평가계획이 만들어져 있고 또 적절한 평가기준이 확립되어 있는가를 확인해야 한다.

(5) 협상(Contract Negotiations)

협상의 주요목적은 사업체가 필요로 하는 컴퓨터 자원을 공평한 조건을 토대로 타당한 가격으로 취득하는데

있다. 따라서 협상은 RFP 송부시부터 시작된다. 적절한 RFP를 작성해야만 예측하지 못한 요건이 생겼을 때, RFP나 제안 내용만을 고집하는 메이커의 구실을 주지 않게 된다. 내용에 허점이 있으면 협상의 부담이 생기며 궁극적으로는 비용의 상승을 초래하게 되기 때문에 정보시스템 감사인은 RFP의 정확성, 완전성 및 메이커 제안에 대한 반응에 상당히 유의해야 한다.

(6) 사이트 선정(Site Selection)

컴퓨터 시설의 설치장소를 선정할 때 유의 사항은 해당 사이트가 완전한 환경으로 신뢰성이 높고, 효율적으로 데이터 처리를 지원할 수 있어야 하는 것이다. 정보시스템 감사인은 데이터 처리 사이트의 이들 특징을 확인하여 중요한 결함이 있는 경우 이를 경영자에게 보고해야 한다. 사이트 선정은 일반적인 입지 조건 및 사이트 환경이라는 두 관점에서 검토할 수가 있다.

(7) 소프트웨어의 취득(Software Acquisition)

시스템 요건이 정의되고 타당성 분석(Feasibility Analysis)이 끝나 전산화를 추진하기로 결정이 내려지면, 그 다음에는 소프트웨어 취득방법을 검토해야 한다. 여기에는 자체개발, 용역개발, 패키지 구입의 세 가지 방법(그리고 이들의 조합)이 있다. 소프트웨어를 자체 개발할 경우, 사업체 담당자가 계획, 시스템의 정의, 분석, 설계, 프로그래밍 및 적용을 해야 한다. 다음의 용역 개발은 컴퓨터 소프트웨어 하우스와 시스템 설계 및 프로그래밍 용역계약을 맺는 것이다. 그 다음엔 패키지 구입 또는 라이선스 계약에 따른 다른 회사로부터 컴퓨터 소프트웨어를 취득하는 것이다.

(8) 서비스 센터(Service Bureau)

컴퓨터를 자체 도입하는 대신 컴퓨터 서비스 제공업자의 것을 이용할 수 있다. 대부분의 이들 컴퓨터 센터는 컴퓨터 처리, 프로그래밍, 데이터 수집 및 배포, 입력 데이터 작성 : 검증, 계획 및 적용에 관한 지원등 광범위하게 서비스하고 있다.

Ⅳ. 평가기준

평점의 부여방법은 각 소항목에 대한 평가만 실시하고 대항목은 자동적으로 산출되도록 하며 평가의 등급은 5 단계로 실시하며 등급판정은 Check List에 작성된 검사 요점을 고려하여 평점을 해당란에 기입한다.

평가위원의 평가가 끝나면 평점이 기입된 Check List를 제출토록 하여 각각의 평가위원의 평균치를 산출하여 평점의 집계표를 산출한다.

평가의 등급

아주 좋음 : 1.0	좋음 : 0.8	보통 : 0.5	나쁨 : 0.3	아주나쁨 : 0.1	미기재 : 0.0

(1) 컴퓨터 시스템

대요인	소 요 인	가중치	대요인	소 요 인	가중치
H/W 0·9	C P U	1.0		PACKAGE	0.5
	Main Memory	0.7			
	외부기억장치	0.9	메이커의 지 원 0·6	지원 사항	1.0
	입출력장치	0.5		납품 실적	0.5
	I/O Control Un	0.9		교 육	0.5
	확장성	0.4		보 수	0.7
	COMM, 장비	0.8			
S/W 0·8	O/S	1.0	가 격 1·0	H/W 가격	1.0
	Processor Management	0.6		S/W 가격	1.0
	Service Prog	0.8		보 수 비	0.9
	Peripheral Management	0.5			
	File Management	0.5			
	Language	0.6		제안서 작성 성실도	0.9
	DBMS	0.9		기계설치에 관한 사항	0.8
	Communication Software	1.0		타사제품의 책임	0.7

(2) NETWORK SYSTEM

대 항 목	소 항 목	가중치
LAN의 구성 1.0	Backbone Network	1.0
	Sub-network	0.9
	본교 전산화에 따른 단계별 망의 발전형태 대처능력	0.6
	LAN to LAN의 신뢰성 및 안정성	0.8
	NETWORK의 성능 (Performance)	0.8
전송속도 0.9	Backbone	0.8
	Sub-network	0.6
	LAN1 - LAN2	0.7
ACCESS기능 0.8	CRT - HOST	0.8
	Point to point	0.5
	표준 프로토콜	0.5
외부 NETWORK와의 접속능력 0.8	PROTOCOL 제공여부	0.6
	X.3, X.25, X.28 연결 여부	0.7
	PS수 가입자의 접속 PC에서의 ACCESS 지원	0.6
	Bitnet 및 DACOM망 연결	0.7
	Terminal에서의 Access 지원	0.6

보유장비의 인터페이스 0.7	VAX780, VAX750의 Ethernet Interface HW module	0.8
	〃 SW 〃	0.6
	PC adaptor card	0.7
	CRT (terminal sever)	0.5
NETWORK Service 기능 0.6	표준 PROTOCOL 지원	0.9
	PC-to-PC, PC-to-HOST, HOST-to-HOST Networking 기능	0.7
	이기종 및 주변기기간의 접속능력	0.7
	File전송시 한글코드처리방법	0.5
	다양한 응용 Service 기능	0.4
	BACKUP 및 분산처리 기능	0.4
	MULTI - MEDIA 통신	0.3
	연동기능	0.5
한글처리 0.5	KS5601 행정망용 한글코드지원	0.5
	지원하는 PC용 한글코드의 종료	0.5
NETWORK MANAGER 0.9	중앙에서 모든 Interface장비 및 System 통합관리 여부	1.0
	광 Backbone	0.8
	Subnet	0.5
	시스템 Failure 재구성 및 경보기능	0.5
확 장 성 0.5	광 Ethernet-Fddi이전 가능성	0.4
	적용업무 증가시의 대처방안	0.5
	Async Port, PC, W/S, Cabinet증설비용	0.6
	LAN1과 LAN2의 최대 확장길이	0.5
	최대 접속 NODE수 및 Port	0.7
	H/W, S/W Upgrade 방안	0.4
장 애 대 책 0.8	FDDI Backbone 장애대책	0.8
	Sub-network 장애대책	0.8
	정전으로 인한 DATA 손실대책	0.7
	Network Server 장애대책	0.7
	Inter-Network 장애대책	0.7
각 단계별 망 구성에 소요되는 비용 0.9	1단계 소프트웨어 비용 하드웨어 비용 2단계 SW, HW 3단계 SW, HW	0.9
기술지원분야 0.9	설치	0.5
	설치 공사비	0.9
	정보보수지원	0.8
	지 원	0.8
	교육지원	0.5
	연구개발	0.5
기술축적도 0.7	관련업체와의 관계	
	LAN관련 제품 개발 실적	
	국내외 업체 관련 정도	
비 용 분 야 1.0	소요비용의 경제성	
	계 약 방 식	
납 품 실 적 0.5	학 교	
	공 공 기 관	
	일 반 기 업 체	
기 타 사 항 0.6	제안서 작성의 성실성	
	충분하고 적절한 참고자료 제출	
	요구사항에 대한 응답 및 대책의 명확성	
	요구자료의 첨부정도	

평가구조는 Tree structure로 되어 있으며 종합평가치(FOM)는 FOMj, 함수로 처리하며 따라서 평가 함수 식은 다음과 같다.

$$Wk \Big/ \sum_{k=1}^{n} Wk$$

$$FOMj = \{ \prod_{k=1}^{n} FOMjk \}$$

FOM = 메리트 계수

FOMj = j 단계에서의 메리트계수

FOMjk = j 단계에서의 FOM에 관한 k번째의 메리트계수

n = FOMj에 속한 메리트계수의 항목

Wk = 상대적인 중요도를 나타내는 가중치 재수치

$\sum_{k=1}^{n} Wk$ = 정상화 계수치

단, 가중치 부여는 $0 < W < 1.0$ 의 범위에서 부여한다.

V. 결론

컴퓨터의 도입목표를 어디에 두는가에 따라 효과가 어느 부분에서 1차적으로 발생하는가를 결정한다. 도입목표를 확실히 하지 않으면 컴퓨터화의 대상업무선정이 단편적으로 되고, 기계화의 level, 범위, 순서를 정하기가 곤란하게 된다.

제약조건을 방침으로 명확히 한다는 것은 회사내 line과 staff 간 컴퓨터 시스템이 무엇을 기대하며, 무엇을 기대하지 않는다는 것을 알리는 것이 되며, 계획을 추진하는 담당자 사이에 협력하기 위한 수단이 된다. 시스템의 목적은 궁극적으로 기업체의 이윤을 추구하는데 있다. 그러나, 대량 업무를 처리하는 기계화하여 경비를 절약하자는 것인가, 적극적인 시장조사를 하여 매출액을 올리자는 것인가, 최적투자를 이한 계산만을 목적으로 하는 것인가, 의사결정과 정보처리를 중심으로 기업의 체질을 개선하는 것인가 등 고려해야 될 점이 많이 있다.

이러한 목적과 시간대는 각 기업의 특성과 객관적 조건에 따라 결정하여야 하며, 장기적인 안목에서 목적 설정을 신중히 하여야 한다. 이러한 목적이 결정되면 목적달성을 위한 방침을 결정하여 최고경영자로부터 문서지시가 있어야 한다. 이는,

① 최고경영자자신이 결의를 확실히 한다는 점
② 사내 협력 체제를 만든다는 점
③ 계획을 계속적으로 추진한다는 점

등의 뜻이 포함되며, 기본방침 중에는 시스템의 목적, 구상, 목적하는 효과, 적용범위, 한계), 목표시기, 추진조직의 성격 등이 포함되어야 한다.

이에 감사의 착안점은 다음과 같다.

① 각 application 의 시스템 계획 및 개발은 의사결정자의 목적을 정확히 나타내고 있는가.
② 시스템 계획은 여러 대체 안을 체계적으로 검토한 후에 결정하였는가.
③ 의사결정자의 문제점 해결을 위해 활용할 수 있는 시스템인가.
④ 의사결정자가 경영 계획이나 경영 관리를 실행하기 위하여 필요한 자료를 제공하는 시스템인가.
⑤ 시스템 계획 시 효과를 계량화할 수 있도록 검토되었는가.
⑥ 시스템 계획이 여러 가지로 입안되고 개발에 요하는 비용과 시스템 개발 후 발생할 수 있는 계산이 적절히 되어 있는가.
⑦ 시스템 계획 및 개발단계에서 세부적 검토가 사용자와 충분히 되었는가.
⑧ 검토결과가 문서화되어 일정기간 보관되고 있는가.
⑨ 시스템 개발 우선순위는 개발부서의 효과보다 사용자부서의 효과를 전제로 한 것인가.
⑩ 개발하여 실시되고 있는 시스템의 를 정기적으로 실시하고 있는가.
⑪ 신기종 교체에 대한 대비책을 가지고 있는가.
⑫ 장기계획(5~10년), 중 단기계획(1~3년)이 마련되고 있는가.

참고문헌

[1] 김영철, "정보시스템 구축과 운영 및 감사는", 대림, pp16-41, 1995
[2] 삼일경제경영연구원 역, "시스템감사개론", 세명서관, pp307-322, 1989
[3] 정창덕, "정보시스템감사사 시험과 실무", 인솔미디어, pp292-298, 1999
[4] 조이남외 1명, "EDP시스템감사", 정익사, pp11-295, 1984
[5] GLEIM' S CIA REVIEW(Tenth Edition) Part I Internal Audit Process
[6] GLEIM' S CIA REVIEW(Tenth Edition) Part II Internal Audit Skills
[7] GLEIM' S CIA REVIEW(Tenth Edition) Part III Management Control and Information Technology
[8] GLEIM' S CIA REVIEW(Tenth Edition) Part IV The Audit Environment