정보시스템 감사/통제 성숙도 모델(CobiT)의 기본개념 및 적용 사례

황경태*

*동국대학교 경영대학 정보관리학과

Concepts and Cases of Information Systems Audit/Control Maturity Model(CobiT)

Hwang, Kyung Tae
Dongguk University
E-mail: kthwang@dgu.edu

요 약

오늘날 정보와 정보시스템은 조직의 핵심 자원 중의 하나이다. 이러한 자원이 효율적이고 효과적으로 활용되지 못하면, 조직의 전략적인 목표 달성에 지장을 초래하게 된다. 이처럼 중요한 자원을 효율적이고 효과적으로 관리하기 위해서는 정보시스템에 대한 적절한 통제가 수립되고 이러한 통제가 적절하게 작동하는지를 점검하고, 여기에 대해서 조언을 해 주는 기능, 즉 정보시스템 감사 기능을 수립하여 실행하는 것이 필요하다. 그러나 정보시스템 통제/감사 체계를 도입하더라도 그 수준은 조직에 따라서 달라질 필요가 있다. 본 논문에서는 이러한 정보시스템 감사/통제 성숙수준을 평가할 수 있는 한 모델인 CobiT의 기본 개념과 적용 사례에 대해서 알아본다.

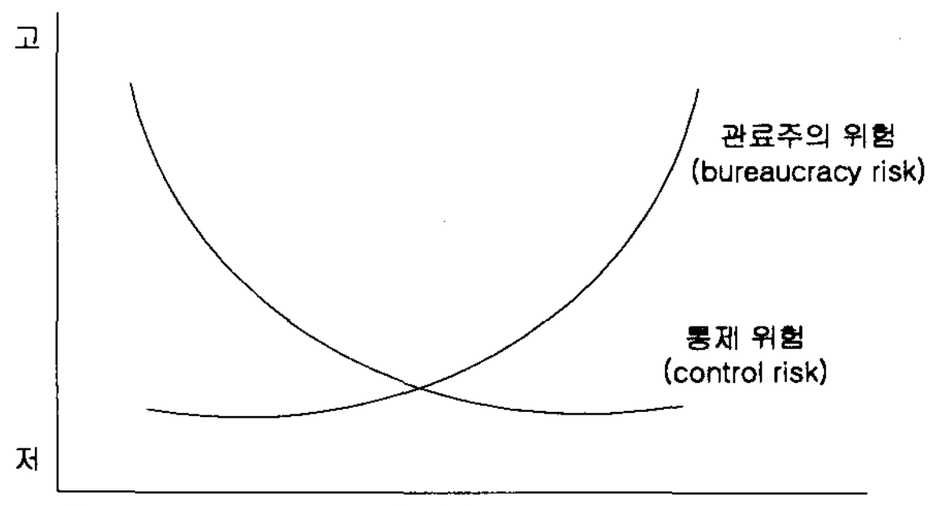
1. 서론

오늘날 정보와 정보시스템은 조직의 핵심 자원 중의 하나이다. 이러한 자원이 효율적이고 효과적으로 활용되지 못하면, 조직의 전략적인 목표 달성에 지장을 초래하게 된다. 이처럼 중요한 자원을 효율적이고 효과적으로 관리하기 위해서는 정보시스템에 대한 적절한 통제가 수립되고 이러한 통제가 적절하게 작동하는지를 점검하고, 여기에 대해서 조언을 해 주는 기능, 즉 정보시스템 감사 기능을 수립하여 실행하는 것이 필요하다.

보다 이론적인 관점에서 정보시스템 통제/감사의 필요성을 생각해 볼 수 있는 하나의 프레임워크는 조직의 공식화 정도와 조직의 위험에 관한 이론이다(<그림 1> 참조)[1]. 공식화 정도란 조직의 업무 절차나 조직 구조가 문서화되고 정형화되어 있는 정도를 말한다. 관료주의적인 위험이란 모든 활동의 평가 기준이 규정 준수에만 초점을 맞추게 되어 효과성과 유연성을 잃게 되는 위험을 말한다. 통제 위험이란 조직에서 원하지 않는 사건의 발생을 방지, 적발, 수정하지 못할 위험을 말한다. 일반적으로 조직의 공식화 정도가 높아지면, 관료주의적인 위험은 높아지는 반면, 통제 위험은 낮아지고, 조직의 전체적인 위험은 관료주의적인 위험과 통제 위험이 교차하는 지점에서 최소화된다.

정보시스템 통제/감사 측면에서 이 프레임워크가 시사하는 바는 무엇인가? 정보시스템 통제/감사 체계를 수립한 기업은 그렇지 않은 기업에 비해서 공식화 정도가 높다. 정보시스템을 도입하여 사용한 기간이 오래 되지 않은 조직의 경우에는 시스템의 사용을 장려하고 확산시킬 수 있도록 가능하면 공식화의 정도를 낮추어야 하고, 따라서 정

보시스템에 대한 지나친 통제 체계를 도입하는 것은 바람직하지 못한 결과를 초래할 수도 있다. 그러나 우리 나라의 경우, 민간 부분의 대기업과 공공 부문은 전반적으로 정보시스템을 도입한 역사가 적어도 20년 이상이 되었고, 무제한적인 기술의 사용을 장려해야 할 시기는 지난 것으로 판단된다. 정보시스템의 효율성, 효과성, 안전성 등을 평가하여 정보시스템에 관련된 경영 목적을 달성하지 못하는 통제 위험을 적정한 수준으로 관리하기 위해서 정보시스템에 대한 통제/감사 체계를 도입하여 조직의 전반적인 위험 수준을 최소화하는 것이 필요한 시점으로 판단된다.



<그림 1> 조직의 공식화 정도와 조직의 위험

그러나 정보시스템 통제/감사 체계를 도입하더라도 그 수준은 조직에 따라서 달라질 필요가 있다. 즉 새로이 설립된 조직이나 새로운 기술을 도입하는 경우에는 업무 수행에 있어서 독창성을 발휘하도록 하고 신기술의 사용을 장려해야 한다. 따라서 이러한 경우에는 통제 위험은 다소 높아지더라도 관료주의적인 위험을 낮추기 위해서 낮은 수준의 공식화의 정도를 유지할 필요가 있다. 그러나 성숙한 조직이나 성숙한 기술에 대해서는 공식화 정도를 높여서 전반적인 위험 수준을 최소화시켜야 할 필요가 있다.

본 논문에서는 이러한 정보시스템 통제/감사의 성숙수준을 평가할 수 있는 하나의 모델인 CobiT(Control Objectives for Info. & related Technology)에 대해서 알아본다. 다음에서는 CobiT의 기본 개념과 성숙단계 모델에 대해서 알아보고, Cobit의 성숙단계 모델을 적용하여 전사적인 차원의 품질 개선을 추구하고 있는 사례에 대해서 알아보도록 한다.

2. CobiT

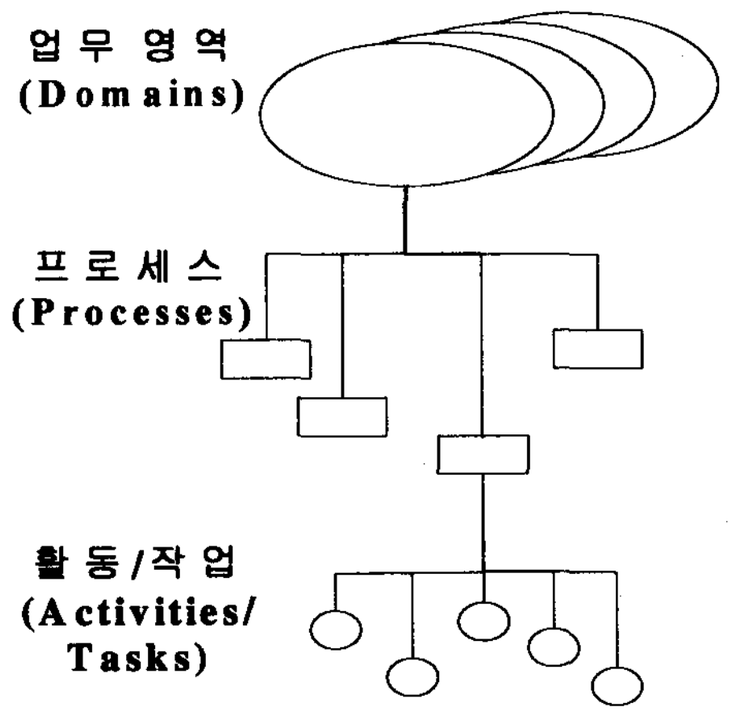
(1) CobiT의 기본 개념

COBIT의 기본적인 출발점은 경영자가 정보와 IT를 기업의 주요 자산으로 인정한다면, 다음과 같은 두 가지 사항을 만족시켜야 한다는 것이다.[2]

첫째, IT 자원의 최적 활용. 즉 경영진은 정보를 생산/저장/처리하는 IT 자원이 최적으로 활용되도록 해야 한다. IT 자원에는 데이터, 응용 시스템, 기술, 시설, 인력 등이 포함된다.

둘째, 정보에 대한 경영상의 요구 사항 충족. 즉 IT를 통해서 생산되는 정보가 보유하고 있어야 할 기준을 가질 수 있도록 해야 한다. COBIT에서는 다음과 같은 7가지의 정보 기준을 제시하고 있다: 효과성, 효율성, 기밀성, 무결성, 가용성, 준거성, 신뢰성.

그러면 경영자들이 위에서 언급한 두 가지 임무를 수행하기 위해서 해야 할 일은 무엇인가? COBIT에서 제시하는 해답은 '일련의 업무 프로세스로 분할하여 IT 자원을 관리해야 한다'는 것이다. IT 업무 프로세스는 업무 영역, 프로세스, 활동/작업 등으로 세분화된다 (<그림 2> 참조).



<그림 2> IT 업무 프로세스 체계

COBIT에서는 4개의 업무 영역, 34개의 프로세스, 302개의 활동/작업을 제시하고 있다. 다음의 <요약표>에는 4개의 업무 영역, 각 업무 영역에서 수행해야 할 프로세스 (총 34개 프로세스), 각 프로세스가 정보 기준을 충족시키는 정도, 각 프로세스가 영향을 미치는 IT 자원 등이 정리되어 있다.

요 약 표

업무 영역		프로세스	정보 기준							IT 자원					
			효과적인	효율적인	기밀적인	무결적인	가용적인	준거적인	신뢰적인	인 적	응용시스템	기 술	시 설	데 이 터
계획 및 조직	PO1	IT 전략 계획 수립	주	부										
	PO2	정보 아키텍쳐 정의	주	부	부	부					√			√
	PO3	기술 방향 결정	주	부								√	√	
	PO4	IT 조직 및 관계 정의	주	부						√				
	PO5	IT 투자 관리	주	주					부	√	√	√	√	
	PO6	경영진의 관리 목표 및 방침 전파	주					부		√				
	PO7	인적 자원 관리	주	주						√				
	PO8	외부 요구사항의 준수	주					주	부	√	√			√
	PO9	위험 평가	부	부	주	주	주	부	부	√	√	√	√	√
	PO10	프로젝트 관리	주	주						√	√	√	√	
	PO11	품질 관리	주	주		주			부	√	√			
도입 및 구축	AI1	솔루션 도출	주	부							√	√	√	
	AI2	응용 소프트웨어 도입 및 유지·보수	주	주		부		부	부		√			
	AI3	기술 아키텍쳐 도입 및 유지·보수	주	주		주						√		
	AI4	IT 절차 개발 및 유지·보수	주	주		부		부		√	√	√	√	
	AI5	시스템 설치 및 인가	주			부	부			√	√	√	√	√
	AI6	변경 관리	주	주		주	주		부	√	√	√	√	√
운영 및 지원	DS1	서비스 수준 정의	주	주	부	부	부	부	부	√	√	√	√	√
	DS2	외부업체 서비스 관리	주	주	부	부	부	부	부	√	√	√	√	√
	DS3	성능 및 용량 관리	주	주			부				√	√	√	
	DS4	서비스의 지속성 확보	주	부			주			√	√	√	√	√
	DS5	시스템의 보안성 확보			주	주	부	부	부	√	√	√	√	√
	DS6	비용 산정 및 배분		주					주	√	√	√	√	√
	DS7	사용자 교육 및 훈련	주	부						√				
	DS8	IT 고객의 지원 및 자문	주							√	√			
	DS9	형상 관리	주				부		부		√	√	√	
	DS10	문제 및 사고 관리	주	주			부			√	√	√	√	√
	DS11	데이터 관리				주			주					√
	DS12	시설 관리				주	주						√	
	DS13	운영 관리	주	주		부	부			√	√		√	√
모니터링	M1	프로세스 모니터링	주	부	부	부	부	부	부	√	√	√	√	√
	M2	내부 통제의 적절성 평가	주	주	부	부	부	부	부	√	√	√	√	√
	M3	독립적인 보증 획득	주	주	부	부	부	부	부	√	√	√	√	√
	M4	독립적인 감사 시행	주	주	부	부	부	부	부	√	√	√	√	√

주: 프로세스가 직접적인 영향을 미치는 경우
부: 프로세스가 간접적인 영향을 미치거나, 극히 일부만을 충족시키는 경우
공란: 적용 가능한 면도 있지만 해당 정보 기준이 다른 프로세스에 의해서 보다 적절하게 충족되는 경우

(2) 성숙단계 모델

오늘날 거의 모든 산업에 걸쳐서 정보시스템의 중요성이 높아지고는 있지만, 모든 조직이 동일한 수준의 정보시스템 통제/감사 체계를 적용할 필요는 없다. 각 조직에 적절 정보시스템 통제/감사의 수준은 다음과 같은 여러 가지 요인에 따라 결정될 것이다: 경영 목적, 정보시스템에 대한 의존도, 사용하는 기술의 복잡성 및 정교성, 정보의 가치 등.

조직이 어느 정도 수준의 통제/감사 체계를 도입하는 것이 자신들에게 적절한가를 판단하기 위해서는 먼저 다음과 같은 사항들을 파악해야 한다: ① 자신의 현재 수준, ② 업계 Best Practice 또는 세계적인 표준의 수준, ③ 자신들의 목표 수준. 즉 현재 자신들이 위치한 수준과 업계의 Best Practice나 세계적인 표준의 수준을 파악하고, 이를 비교하여 향후에 자신들이 목표로 하는 수준을 결정해야 한다. 또한 목표 수준을 수립하여 이를 실행하는 과정에서는 목표 대비 진척도 즉 목표에 대비해서 얼마나 잘 수행하고 있는가를 파악하는 것이 필요하다.

이러한 활동의 수행을 지원해 줄 수 있는 접근 방법 중의 하나가 2000년에 ISACA에서 출간한 CobiT III의 관리지침서(Management Guideline)이다[3]. 관리지침서에 포함되어 있는 주요한 내용은 34개 주요 IT 프로세스에 각각에 대한 ① 성숙단계 모델(Maturity Model), ② 핵심성공요인(Critical Success Factor: CSF), ③ 핵심수행지표(Key Performance Indicator: KPI), ④ 핵심목표지표(Key Goal Indicator: KGI) 등이다. 성숙단계 모델은 조직이 자신들의 수준을 파악하고, 업계 Best Practice 등과의 비교를 통해서 목표 수준을 설정하는 것을 도와 준다. CSF, KPI, KGI 등은 목표 수준을 수립하여 실행하는 과정에서는 목표 대비 진척도를 파악하는 것을 지원한다. 아래에서는 이러한 네 가지 항목에 대해서 보다 자세하게 살펴보도록 한다.

1) 성숙단계 모델

CobiT III에서는 정보시스템 통제 및 감사의 성숙단계를 CMM(Capability Maturity Model)과 유사하게 다음과 같은 6단계로 분류하고 있다.

단계	설 명
0. 부재 단계	관리 프로세스가 전혀 존재하지 않는다
1. 초기 단계	프로세스가 응기응변적이고 조직화되어 있지 않다
2. 직관적 단계	프로세스가 일정한 패턴을 따르고 있다
3. 정의 단계	프로세스가 문서화되고 전파되고 있다.
4. 관리 단계	프로세스가 모니터되고 측정되고 있다.
5. 최적 단계	Best Practice가 준수되고 자동화되어 있다

이러한 성숙단계 분류의 기본적인 바탕은 단계가 높아짐에 따라 다음과 같은 6가지 영역에 대한 업무수행방법 및 원칙들이 점차 더 많이 추가되고 정교화된다는 것이다: ① 위험 및 통제 관련 이슈에 대한 이해 및 인식, ② 이러한 이슈에 대한 훈련 및 전파, ③ 실행되는 프로세스 및 업무수행방법, ④ 프로세스의 효율성과 효과성을 높이기 위한 기법 및 자동화, ⑤ 내부 정책, 법규의 준수 정도, ⑥ 사용되는 전문성의 종류와 정도.

2) 핵심성공요인

핵심성공요인(Critical Success Factor: 이하 CSF)은 IT 프로세스가 최적의 성공을 거두기 위해서 필요한 사항이나 조건과 수행해야 할 가장 중요한 활동들을 말한다. 여기에는 전략적, 기술적, 조직적, 절차적인 측면에서 수행해야 할 중요한 사항들이 모두 포함된다.

모든 프로세스에 적용될 수 있는 일반적인 CSF로는 다음과 같은 것들이 있다.

- 프로세스의 정의 및 문서화
- 정책의 정의 및 문서화
- 책임 소재의 명확화
- 경영진의 강력한 지원 및 의지
- 이해 관계가 있는 내부 및 외부 인력과의 적절한 의사소통
- 수행 성과 및 목표 달성에 대한 일관성 있는 측정

3) 핵심수행지표 및 핵심목표지표

핵심수행지표(Key Performance Indicator: 이하 KPI)는 IT 프로세스가 얼마나 잘 수행되고 있는지에 관한 지표이다. 핵심목표지표(Key Goal Indicator: 이하 KGI)는 IT 프로세스 수행의 결과

로 궁극적인 목표의 달성 정도를 나타내는 지표이다. KGI는 "무엇"에 초점을 맞추고 있는데 반해서 KPI는 "어떻게"에 초점을 맞추고 있는 지표이다.

IT 전반에 적용될 수 있는 일반적인 KPI와 KGI의 예가 다음에 정리되어 있다.

KPI

- 프로세스의 비용 효율성
- 오류 및 재작업의 양
- 이해관계자들의 만족도
- 서비스의 가용성 및 응답 시간
- 통신 대역폭 및 컴퓨팅 파워의 활용도
- 품질 및 혁신의 향상

KGI

- 목표 투자 수익률 또는 효익 달성
- IT 위험의 감소
- 생산성 향상
- 공급 체인의 통합
- 판매 증가
- 새로운 고객의 유치 및 기존 고객의 만족도 증가
- 새로운 서비스 제공 채널의 창출
- 프로세스 고객의 예산 및 일정에 대한 기대 및 요구 사항 충족

KPI와 KGI의 두 지표는 상호 연관관계를 가지고 있는데, 이러한 연관관계는 BSC(Balanced Scorecard)의 네 가지 측면(재무, 고객, 내부 프로세스, 학습/혁신)에서 살펴볼 수 있다. 먼저 KPI는 내부 프로세스와 학습/혁신 측면에 초점을 맞추고 있는 지표이고, KGI는 재무 및 고객 측면에 관련된 지표이다. 재무적인 결과와 고객 만족은 보통 경영 목표의 달성에 관한 지표이고 현상이 일어난 이후에 측정되므로, KGI는 '사후적인' 지표이다. 이에 비해서 프로세스의 우수성과 학습하고 혁신할 수 있는 능력은 조직이 얼마나 잘 수행하고 있는지를 나타내는 지표이고 현상이 일어나기 이전에 성공을 거둘 수 있는 가능성을 나타내 주므로, KPI는 '선행적인' 지표이다.

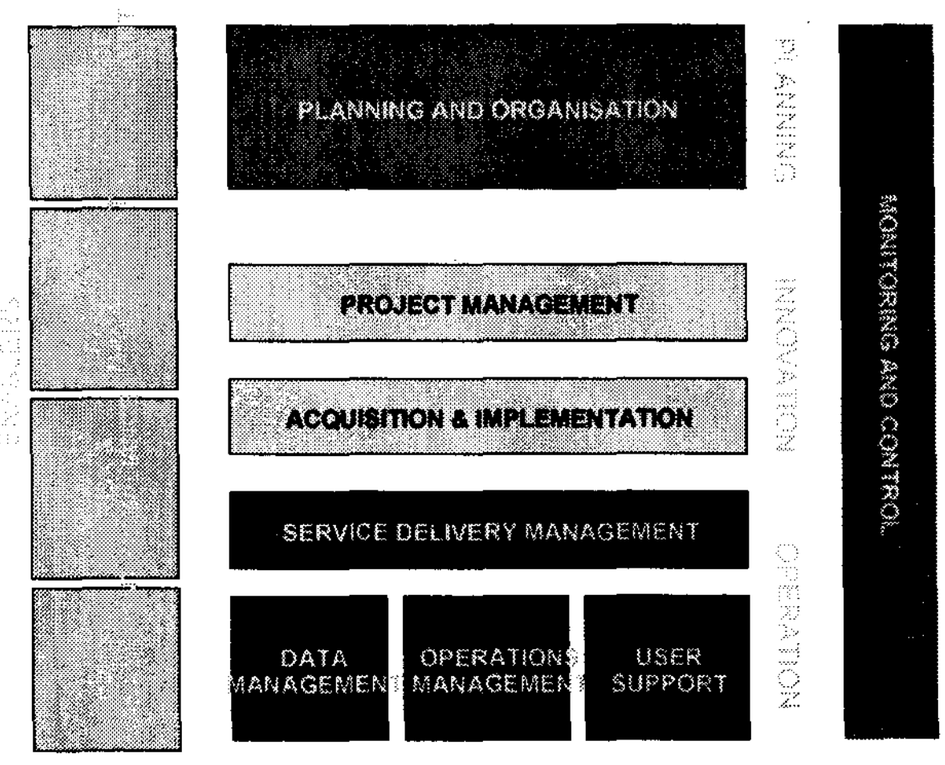
3. CobiT 적용 사례

다음에서는 CobiT의 정보시스템 감사/통제 성숙단계 모델을 도입하여 IT 관리 프로세스의 수준을 평가·분석하고 이를 개선하기 위한 노력을 펼치고 있는 Philips사의 사례에 대해서 알아본다.[4]

Philips사가 추진한 작업은 크게 다음과 같은 5단계로 정리해 볼 수 있다

- 핵심 프로세스의 정의
- 평가 척도 개발
- 각 프로세스에 대한 현행 및 목표 성숙단계 결정
- 갭 분석(Gap Analysis)
- 실행계획 수립 및 사후 점검

첫째, 핵심 프로세스의 정의: Phillips사는 CobiT의 34개 프로세스를 기반으로 자사에 적합한 IT 관리 프로세스로 다음과 같은 12개의 핵심 프로세스를 결정하였다(<그림 3> 참조).

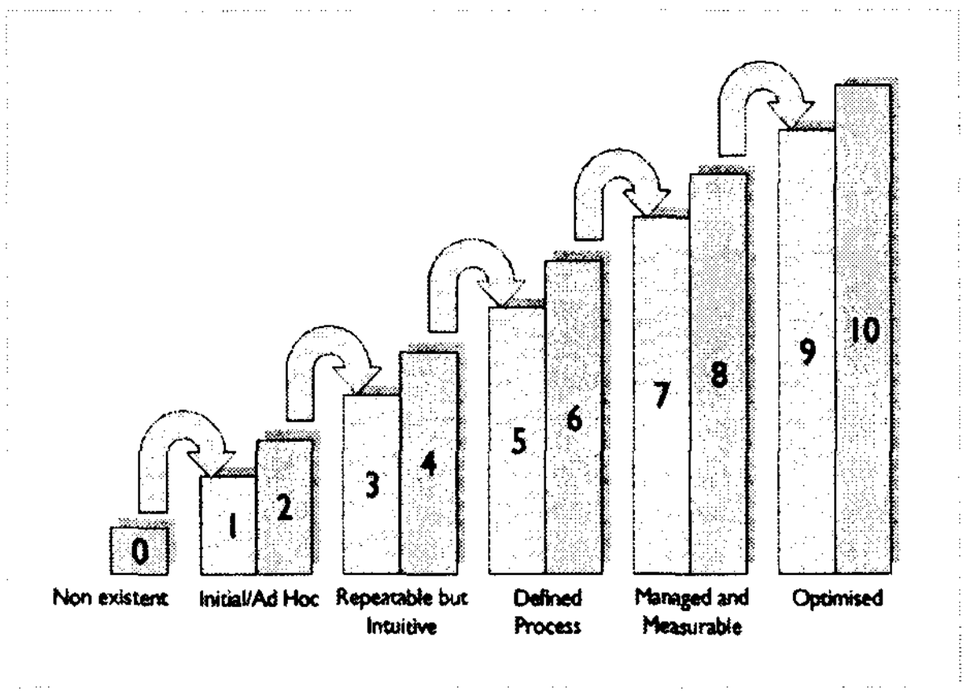


<그림 3> 핵심 프로세스

둘째, 평가 척도 개발: Phillips사는 CobiT의 성숙단계 모델을 이용하여 IT 관리 프로세스의 수준을 평가하기 위한 척도를 개발하였다. 성숙단계는 기본적으로 CobiT이 제시하고 있는 6단계에 다음 단계로의 전환 단계(transitionary level)를 추가하여 0단계에서 10단계까지로 구분하였다(<그림 4> 참조).

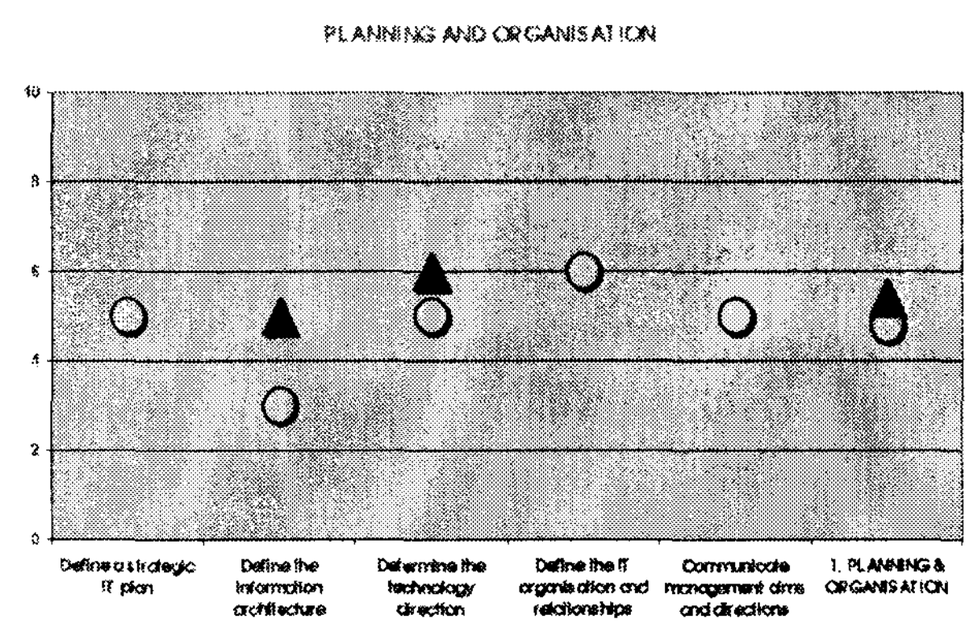
셋째, 각 프로세스의 현행/목표 성숙단계 결정: 앞에서 정의한 평가 척도로 핵심 프로세스에 대한 평가를 수행하였다. 평가에는 IT 인력, 현업 실무자들로 6-8명이 참여하였고, 진행 방법은 1일 또는 반일 정도의 워크숍 형식으로 진행되었다. 워크숍에서는 먼저 핵심 프로세스와 평가 척도에 대한 교육이 이루어졌고, 그 이후 각 프로세스별로 1시간 정도에 걸쳐서 개인별 평가와 그룹의 합의를

이루기 위한 토의가 이루어졌다. 다음으로는 내년도의 목표 수준과 이를 위해서 수행해야 할 개선 활동 등이 결정되었다.



<그림 4> 평가 척도

넷째, 갭 분석: 현행 수준과 목표 수준에 대한 갭 분석이 이루어졌다. 다음의 <그림 5>에는 몇 개의 프로세스에 대한 갭 분석의 결과가 정리되어 있다.



<그림 5> 갭 분석 결과

다섯째: 실행계획 수립 및 사후 점검. 갭 분석의 내용을 바탕으로 개선을 위한 단계별 실행계획을 수립하였다. 실행계획에 따라 개선활동을 수행하면서, 그 수행결과를 점검하기 위해서 다음과 같은 평가 방법을 도입하였다.

- 3 < 성숙수준 < 5: 동료 감사(peer audit)
- 성숙수준 > 5: 공식적인 감사

4. 결론

우리 나라의 경우, 민간 부분의 대기업과 공공부문은 전반적으로 정보시스템을 도입한 역사가 적어도 20년 이상이 되었고, 무제한적인 기술의 사용을 장려해야 할 시기는 지난 것으로 판단된다. 정보시스템의 효율성, 효과성, 안전성 등을 평가하여 정보시스템에 관련된 경영 목적을 달성하지 못하는 통제 위험을 적정한 수준으로 관리하기 위해서 정보시스템에 대한 통제/감사 체계를 도입하여 조직의 전반적인 위험 수준을 최소화하는 것이 필요한 시점으로 판단된다. 그러나 정보시스템 통제/감사 체계를 도입하더라도 그 수준은 조직에 따라서 달라질 필요가 있다.

본 논문에서 살펴 본 CobiT에서 제시하고 있는 IT 프로세스와 성숙단계 모델은 이러한 정보시스템 감사/통제 체계를 구축하는데 참조할 수 있는 유용한 모델로 판단된다. 우리 나라의 공공부문과 민간 부분에서는 CobiT에서 제시하고 있는 IT 프로세스를 자신들의 상황에 적합하도록 수정보완하여 도입하고, 성숙단계 모델을 이용하여 현재의 수준을 평가하고, 동종업계 또는 세계적인 수준 등을 고려한 목표 수준을 수립하여 정보시스템에 관련된 위험을 관리하고 경영목적을 달성할 수 있도록 노력을 기울이는 것이 필요한 시점으로 판단된다.

[참고문헌]

[1] Edwin E. Tozer. Strategic IS/IT Planning. Butterworth Heinemann, 1996.

[2] ISACA, CobiT III: Control Objectives, 2000.

[3] ISACA, CobiT III: Management Guideline, 2000.

[4] Pieter Kock, "Let's Make Things Better", IT Governance Forum: Trust and Understanding for the Business and the Board, Paris, France, June 2001.