정보시스템 감리프레임워크 구축 및 운영 방안

심승배, 최헌준
한국국방연구원 정보화연구센터

The Method of Construction and Operation for Information System Audit Framework

Sim, Seung Bae · Choi, Heon Jun
KIDA (Korea Institute for Defense Analyses)
E-mail: sbsim@kida.re.kr, chj@kida.re.kr

요 약

정보시스템의 효과적인 개발 및 운영을 지원하기 위한 활동에는 품질 보증, 감리 등이 있다. 이 중에서 감리는 정보시스템의 전체 개발 수명주기에 걸쳐서 시스템의 품질을 개선시키기 위한 핵심 활동이라고 할 수 있다.

현재 공공 정보시스템 감리는 기존의 정보시스템감리기준(정보통신부고시제1999-104호)를 활용하여 수행하고 있지만, 감리영역이나 점검사항이 현재 IT 환경과 맞지 않고 실제 감리에 적용하기 어렵다. 또한, 정보시스템 개발수명주기에 걸쳐서 감리를 수행해야함에도 불구하고, 현실은 그렇지 않으며 수명주기별 감리기준도 명확하지가 않다.

본 연구에서는 ISACA(Information Systems Audit and Control Association)의 COBIT(Control Objectives for Information and related Technology)와 IT 관련 국제 표준들을 벤치마킹하여 정보시스템 감리프레임워크를 제시하였고, 이의 운영 및 활용 방안을 제안하였다.

1. 서론

정보시스템을 효과적으로 개발하고 운영하기 위한 활동으로는 품질 보증, 감리 등이 있다. 품질 보증 활동이 발주자나 사업관리자 관점의 내부 품질 보증에 초점을 맞추고 있는 반면, 감리는 정보시스템의 전체 개발 수명주기에 걸쳐서 시스템의 품질을 개선시키기 위한 독립적인 품질 보증 활동에 초점을 맞추고 있다.

국내에서는 한국전산원이 1986년 「전산망보급확장과이용촉진에관한법률」에 의거하여 전산감리 임무를 부여 받은 이래로, 국가 정보화의 진전에 따라 정보통신부는 1999년 1월 정보화촉진법에 감리에 대한 근거 규정을 마련하고, 동 법에 의거하여 제정 고시된 정보시스템 감리기준에 따라 정보시스템 감리를 시행하고 있다.

현행 정보시스템 감리는 제도적으로 정보화사업 발주기관이 준수해야 할 의무사항이 아니므로 공공

부문의 정보화 사업에 한정적으로 적용하고 있다.

정보통신부 고시 감리기준은 감리인 요건, 감리절차, 감리 기본 점검표 등 감리절차상의 세부 준수사항으로 구성되어 있다. 그러나, 현행 감리기준은 감리 업무 수행에 필요한 최소한의 요건만을 정의하고 있어, 체계적인 관리체계 부족으로 인한 부실 감리, 감리 품질 저하 등의 문제가 발생하고 있다. [1,2]

예를 들어, 현재 공공 정보시스템 감리는 기존의 정보시스템감리기준(정보통신부고시제1999-104호)를 활용하여 수행하고 있지만, 감리영역이나 점검사항이 현재 IT 환경과 맞지 않고 실제 감리에 적용하기 어렵다. 또한, 정보시스템 개발수명주기에 걸쳐서 감리를 수행해야함에도 불구하고, 현실은 그렇지 않으며 수명주기별 감리기준도 명확하지가 않다.

국외에서는 미국의 경우 ISACA(Information Systems Audit and Control Association)에서 개발한 정보시스템 감리기준인 COBIT(Control Objectives for Information and related Technology)을 활용하고 있다. COBIT은 4가지 업무영역(Domain)과 34개 프로세스로 구성되어 있으며, 세부적으로는 각 프로세스에 대한 세부통제기준 및 관리기준으로 구성되어 있다. [6,7,8]

본 연구에서는 ISACA의 COBIT과 IT 관련 국제표준들을 벤치마킹하여 정보시스템 감리프레임워크를 제시하였고, 이의 운영 및 활용 방안을 제안하였다.

본 연구의 나머지 구성은 다음과 같다.

2장에서는 국내 정보시스템 감리기준으로 정보통신부와 국방부의 정보시스템 감리기준을 분석하였고, 3장에서는 ISACA의 감리기준인 COBIT을 설명하고, 4장에서는 COBIT과 관련 표준을 벤치마킹하여 구축한 정보시스템 감리 프레임워크와 운영방안을 제시하였다. 마지막 5장에서는 향후 연구 및 개선 방향에 대하여 논의하였다.

2. 국내 정보시스템 감리기준

2.1 정보통신부 정보시스템 감리기준

정보통신부가 1999년에 고시한 정보시스템 감리기준은 공정에 따라서 기획, 개발, 운영, 유지보수로 나누어 감리기준을 제시하는 한편, 일반적인 범위관리, 일정관리, 위험관리 등과 같은 관리 영역에 대한 감리기준을 <표 1>과 같이 제시하고 있다.

감리절차는 감리계약 체결부터 감리결과 검토까지 7단계로 구성되어 있으며, 최종 감리검토의견은 적정[1], 보통[2], 부적정[3]의 3단계로 되어 있다.

<표 1> 정보통신부 정보시스템 감리기준

구분		내용
고시처		정보통신부(1999.12.22)
감리 영역 구분	공정별	기획/개발/운영/유지보수
	일반 감리	범위관리/일정관리/위험관리 형상관리/품질관리/프로젝트표준 및 기타
감리절차		7단계로 구성 • 감리계약 체결 • 감리계획 수립 • 감리착수회의 개최 • 감리 시행 • 감리종료회의 개최 • 감리보고서 작성 및 통보 • 감리결과 검토
감리시행 기간 및 투입인력		사업비별 감리시행 기간/투입인력 제시
감리기준 (점검표)		• 공정별 점검표 • 일반관리 점검표
감리평가기준 (검토의견)		• 적정 • 보통 • 부적정

그러나, 앞서 언급했듯이 감리영역이나 점검사항이 현재 IT 환경과 맞지 않고 실제 감리에 적용하

[1] 적정 : 중대한 문제점이 발견되지 않았으며 사전에 정의된 주요 요구사항이 충족된 상태

[2] 보통 : 문제점이 발견되었으나 사전에 계획된 자원의 범위 내에서 개선가능하여 정의된 주요 요구사항을 충족할 수 있는 상태

[3] 부적정 : 중대한 문제점이 존재하며 사전에 계획된 자원의 범위내에서 개선이 불가능하여 정의된 주요 요구사항을 충족할 수 없는 상태

기 어려우며, 정보시스템 개발수명주기별 감리기준도 명확하지가 않다.

2.2 국방부 정보시스템 감리기준

대규모 정보화사업을 발주하고 있는 국방부에서는 2001년 10월에 정보통신부 감리기준을 기반으로 국방정보체계 감리지침을 제정하였다. 국방정보체계 감리지침에서는 감리를 크게 사업감리와 운영감리로 구분하고, 사업감리는 다시 감리수행시점에 따라 사전감리, 진행감리, 사후감리로 나누어진다. 또한 수행주체에 따라서 내부 요원 중심의 내부감리와 외부의 독립적인 요원을 활용하는 외부감리로 구분할 수 있다. <표 2>는 국방정보체계 감리의 정의 및 구분을 설명하고 있다. [3,4]

그러나, 정보통신부의 감리기준에서 변경된 부분이 거의 없으며, 국방 분야에서도 감리영역이나 점검사항이 현재 국방 IT 환경과 맞지 않고 실제 감리에 적용하기 어려우며, 정보시스템 개발수명주기별 감리기준도 명확하지가 않다.

<표 2> 국방정보체계 감리의 정의 및 구분

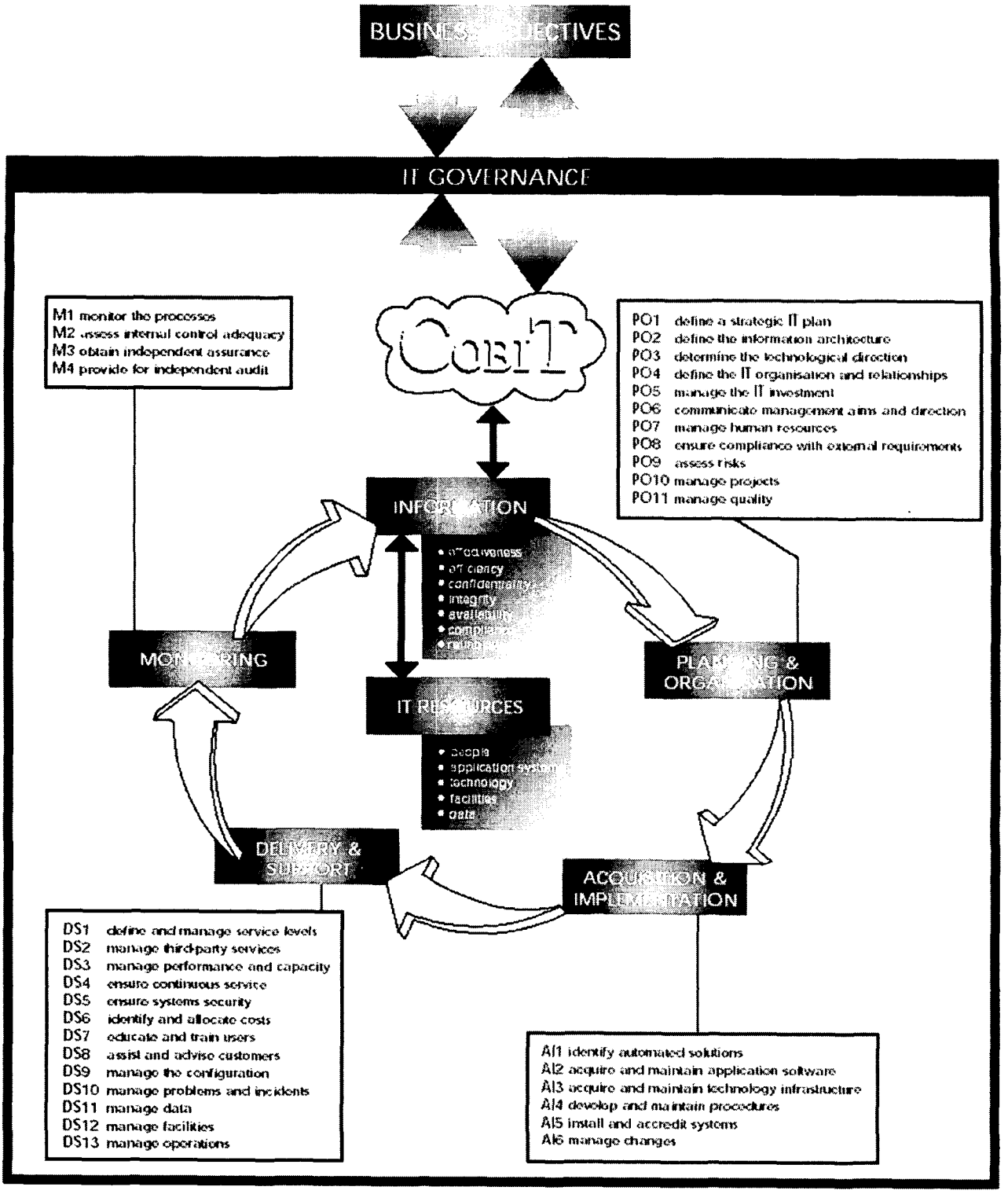
감리구분		감리목적	감리수행 형태
사업감리	사전감리	계획(세부일정계획 및 자원배분계획)의 타당성 및 적정성을 검토 평가	불명확
	진행감리	계획된 사업이 합당하게 진척되고 있는가 판단	외부감리
	사후감리	산출물의 신뢰성, 안정성, 효율성 및 투자자원의 적정성 등을 확인, 분석, 평가	내부감리
운영감리		운영중인 국방정보체계에 대한 유지보수 및 운영상태를 측정	주로 내부감리

감리구분	감리대상	비고
외부감리	국방부통제사업	사업비에 감리비 반영
내부감리	외부감리 대상이 아닌 사업에 대한 사업감리와 운영감리	예산편성기준에 의한 자체 예산 반영

3. COBIT

COBIT(Control Objectives for Information and related Technology)은 ISACA(Information Systems Audit and Control Association)에서 개발한 정보시스템 통제기준으로 정보시스템 감리를 위해 활용할 수 있다. COBIT은 정보와 조직의 IT 자원을 통제하기 위한 기준이며, 통제를 위해서 계획 및 조직(Planning and Organization), 도입 및 구축(Acquisition and Implementation), 운영 및 지원(Delivery and Support), 모니터링(Monitoring)의 4가지 업무영역(Domain)과 각 업무영역에 속하는 총 34개 프로세스로 구성되어 있다. 각 프로세스는 통제 목적과 통제 내용으로 구성된 세부기준으로 구성되며, 통제 결과를 평가하기 위한 기준을 카네기멜론대학의 소프트웨어공학연구소에서 개발한 CMM(Capability Maturity Model)의 개념을 기반으로 제시하고 있다. [6,7,8]

<그림 1>은 이러한 COBIT 프레임워크를 나타내고 있다.



<그림 1> COBIT 감리 프레임워크

COBIT은 조직의 기획/계획 측면과 구축된 시스템의 운영 측면을 강조하고 있는 기준이다. ISACA에서는 COBIT 프레임워크를 비롯해서 관리지침서, 세부통제목적, 감사지침서, 적용도구 및 사례집 등을 지속적으로 제공하고 있다.

4. 정보시스템 감리 프레임워크

4.1 정보시스템 감리 프레임워크

본 연구에서는 기존의 감리지침이나 기준을 분석하고, COBIT을 비롯한 관련 표준을 벤치마킹하여 <그림 2>와 같은 정보시스템 감리 프레임워크를 제안하였다.

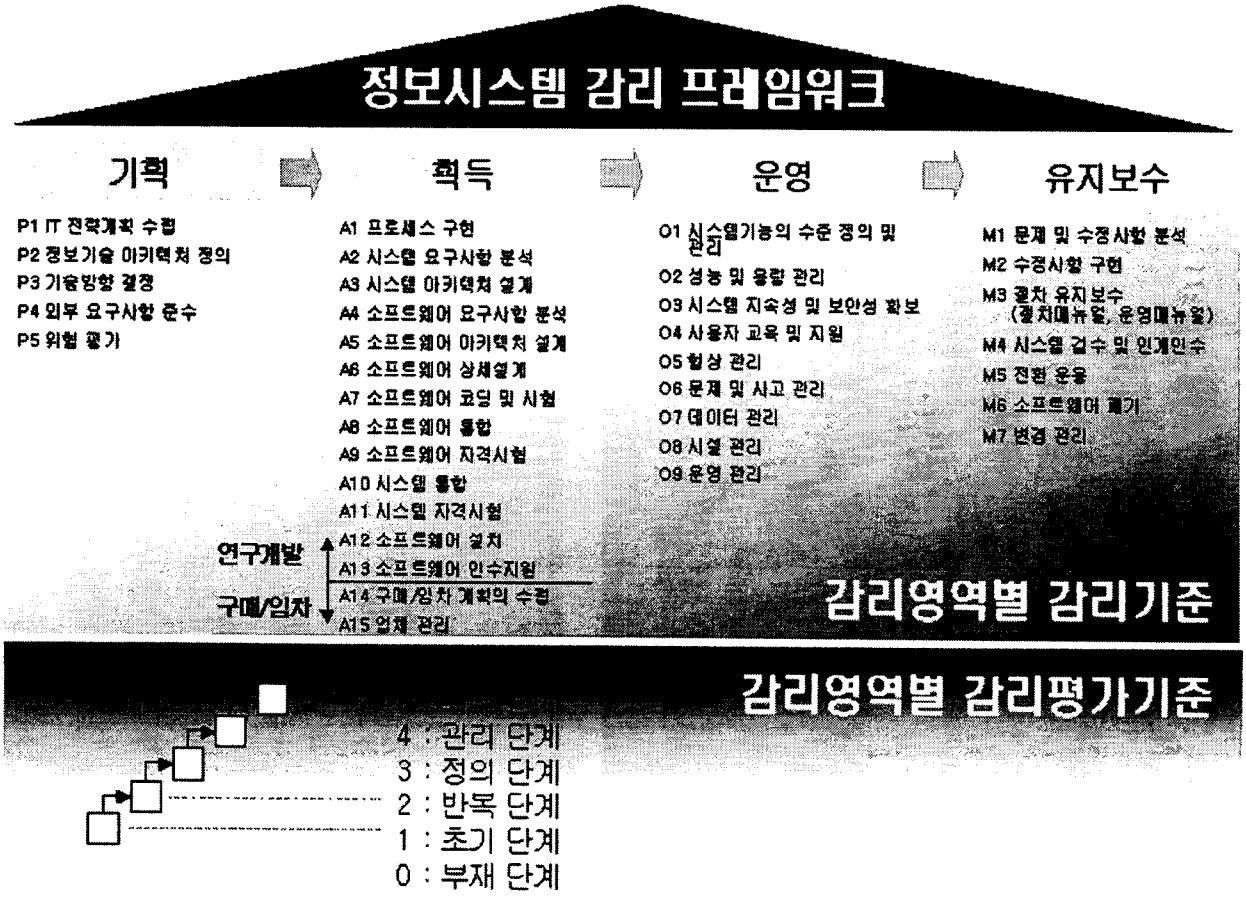
정보시스템 감리 프레임워크는 기획, 획득, 운영, 유지보수의 4개의 감리영역으로 구분되며, 감리영역에 대한 총 36개의 프로세스로 구성된다. 각 감리 프로세스에 대한 감리평가기준은 COBIT에서와 마찬가지로 CMM을 활용하였다.

감리 프로세스에 대한 감리 기준의 구성은 다음과 같다.

- 프로세스명
- 감리 목적
- 감리 기준 목록
- 감리 기준

그리고, 감리 프로세스에 대한 감리평가기준은 다음과 같다.

- 프로세스명
- 감리 목적
- 평가 단계별 기준
  - 0 부재
  - 1 초기
  - 2 반복
  - 3 정의
  - 4 관리
  - 5 최적



<그림 2> 정보시스템 감리 프레임워크

4.2 정보시스템 감리 프레임워크 운영 방안

본 연구에서 제시한 정보시스템 감리프레임워크는 ISO/IEC 12207, 즉 소프트웨어 개발수명주기 프로세스 표준에서 정보시스템에 대한 획득 및 유지보수 부분에 대한 벤치마킹을 수행했으며, COBIT에서 기획 및 운영에 대한 부분을 벤치마킹하여 새롭게 구성하였다. 특히, 획득 부분에서는 소프트웨어를 개발하는 연구 개발 부분과 상용 소프트웨어(COTS)를 구매 또는 임차하는 부분으로 나누어 현실을 고려하였다. [4, 5]

제시한 정보시스템 감리 프레임워크는 각 수명주기별로 감리에 이용되어야 하며, 해당 환경에 맞게 감리기준을 테일러링해서 사용해야 한다.

또한, 현재 적정, 보통, 미흡, 부적정 등으로 구성된 감리 평가기준과 권고사항, 통상개선, 긴급개선과 같은 평가의견을 감리 프레임워크에서 제시한 5단계 평가기준(부재, 초기, 반복, 정의, 관리, 최적)에 다음의 <표 3>, <표 4>와 같이 대응시켜 적용해야 한다.

<표 3> 일반적인 감리 평가기준과 평가의견

평가기준		요구사항만족	허용자원	의미
적정	개선지속	문제 없음	-	사전에 정의된 주요 요구사항이 충족된 상태
보통	권고사항	일반적인 문제점	있음	일반적인 문제점이 발견되었으나 사전에 계획된 자원이 범위 내에서 개선 가능하여 정의된 주요 요구사항을 충족할 수 있는 상태
미흡	통상개선	중대한 문제점	있음	중대한 문제점이 발견되었으나 사전에 계획된 자원과 추가적으로 약간의 자원 투입을 통해서 개선 가능하며, 이를 통해 주요 요구사항을 일정 부분 충족할 수 있는 상태
부적정	긴급개선	중대한 문제점	없음	중대한 문제점이 존재하며 사전에 계획된 자원의 범위 내에서 요구사항을 충족할 수 없는 상태

<표 4> 일반적인 감리 평가기준과 감리 프레임워크의 평가 기준과의 대응 관계

평가 기준	성숙 단계	설명
부적정	0 부재	중대한 문제점이 존재하며 사전에 계획된 자원의 범위 내에서 요구사항을 충족할 수 없는 상태
미흡	1 초기	중대한 문제점이 발견되었으나 사전에 계획된 자원과 추가적으로 약간의 자원 투입을 통해서 개선 가능하며, 이를 통해 주요 요구사항을 일정 부분 충족할 수 있는 상태
보통	2 반복	일반적인 문제점이 발견되었으나 사전에 계획된 자원이 범위 내에서 개선 가능하여 정의된 주요 요구사항을 충족할 수 있는 상태
적정	3 정의	사전에 정의된 주요 요구사항이 충족된 상태 - 요구사항 관리 프로세스가 존재하는 경우
적정	4 관리	사전에 정의된 주요 요구사항이 충족된 상태 - 요구사항이 정량적으로 측정되고 있는 경우
적정	5 최적	사전에 정의된 주요 요구사항이 충족된 상태 - 요구사항이 지속적으로 반영되고 있는 경우

5. 결론

본 연구에서는 국내외 정보시스템 감리기준을 분석하고, 현재 기준의 문제점을 해결 및 보완하기 위해서 ISACA의 COBIT과 정보시스템 관련 표준들을 벤치마킹하여 정보시스템 감리 프레임워크를 제시하였다.

실제 감리를 수행할 때에는 감리 프레임워크에서 필요한 단계 및 부분을 선택해야 하며, 감리 기준과 감리평가기준에 대하여 감리인과 감리의뢰인이 의견을 조율해야한다.

향후 연구 분야로는 현재 정보시스템 감리 프레임워크의 감리기준 및 감리평가기준의 지속적인 보완, 특정 영역에 대한 중점 감리기준의 구축 등이

있다.

6. 참고문헌

[1] 최헌준, 서예영, 심승배, 국방정보화 감리절차 개선방안 연구, 한국국방연구원, 2003.11

[2] 정보시스템감리기준, 정보통신부,1999.12.22

[3] 국방정보체계 감리지침, 국방부, 2001.10

[4] 국방획득관리규정, 국방부, 2003

[5] IEEE/EIA 12207.0, "Software Life Cycle Processes", March 1998

[6] COBIT(Control Objectives for Information and related Technology) 3rd edition - Framework, ISACA, July 2000

[7] COBIT(Control Objectives for Information and related Technology) 3rd edition – Control Objectives, ISACA, July 2000

[8] COBIT(Control Objectives for Information and related Technology) 3rd edition – Management Guidelines, ISACA, July 2000