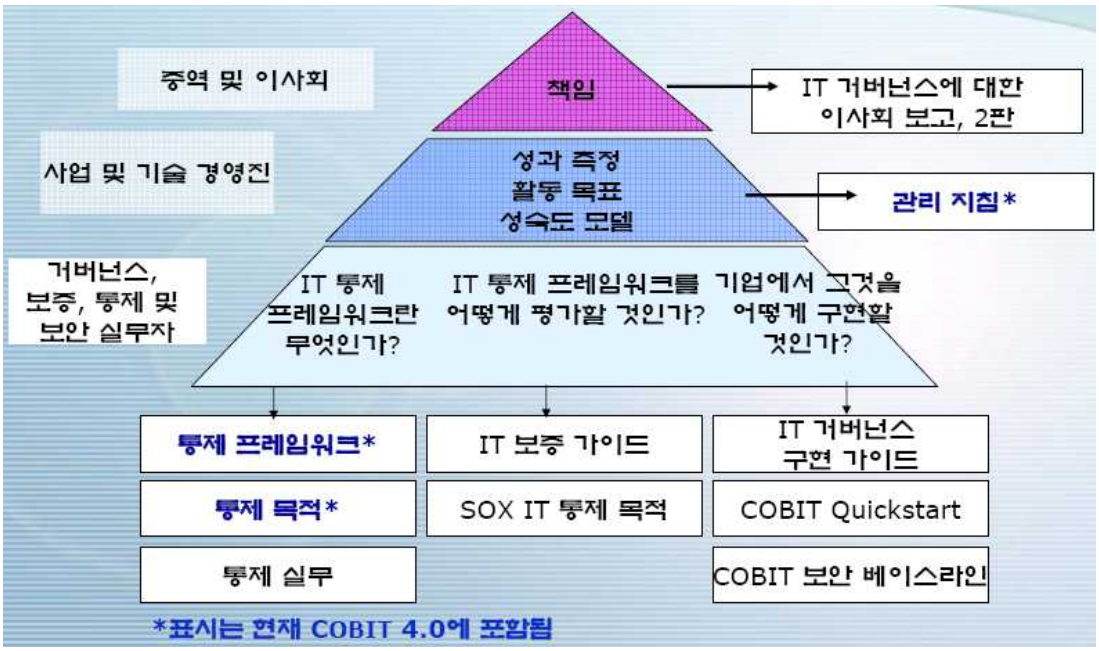
COBIT

1. COBIT의 정의
   - ○ ISACA가 개발한 IT 통제 및 감사를 위한 프레임워크
     ▷ 감사 도구에서 IT 경영진이 사용하는 IT 거버넌스 프레임워크로 진화
   - ○ 효과적인 IT Governance와 통제를 구현하기 위한 실무차원의 베스트 프랙티스를 제공하는 공개표준 프레임워크
   - ○ IT Governance의 이점을 최대화하고, 자산을 보호하며, 규제를 준수하며, IT 투자효과를 높이기 위한 IT Governance 구현 모델로 사용

2. COBIT의 구성



   - ○ 책임 : 고위 경영진들이 IT 거버넌스가 왜 중요하고, 관련된 이슈에는 어떤 것들이 있으며, IT 관리에 있어 그들의 책임이 무엇인지를 이해할 수 있도록 고안
   - ○ 관리 지침(서) : 책임을 할당하고, 성과를 측정하며, 역량을 벤치마킹해 격차를 해소하는 것을 도와주는 도구
   - ○ 프레임워크 : COBIT가 IT 거버넌스의 목적과 베스트 프랙티스들을 IT 도메인과 프로세스로 조직화하고, 이들을 비즈니스 요구사항과 연계하는 방법을 설명
   - ○ 통제 목적 : 모든 IT 활동에 대한 일반적인 베스트 프랙티스 관리 목적을 제시

3. COBIT의 특성

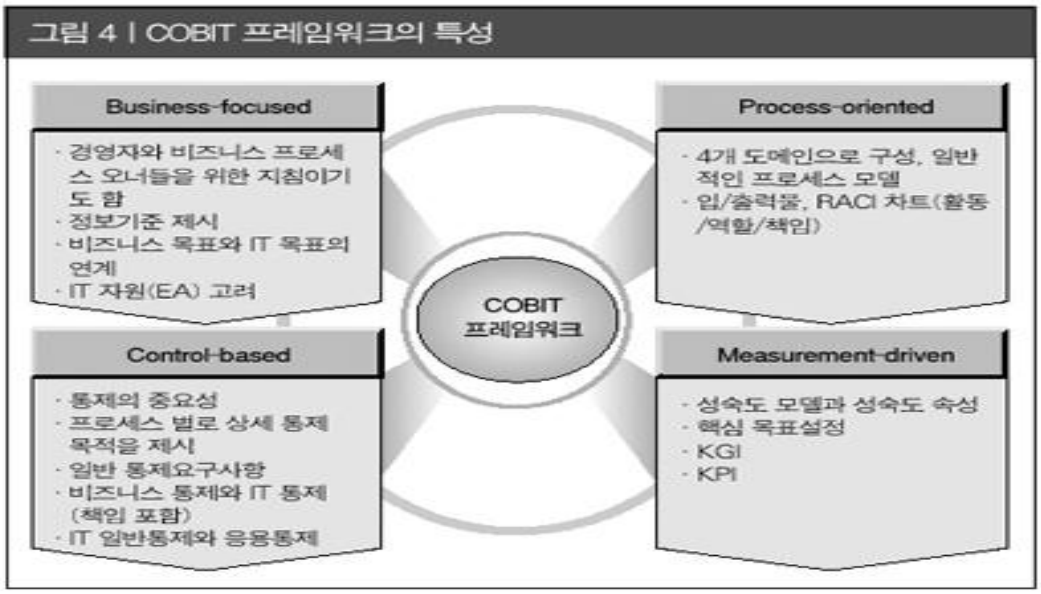
① 비즈니스 요구를 IT 목표와 연계시키는데 초점을 맞추고,

② 효과적인 IT 프로세스의 구현을 지향하고,

③ 프로세스와 어플리케이션 측면에서 IT 위험을 통제하며

④ 프로세스별로 IT 성과를 모니터링하고 측정하기 위한 도구를 제공

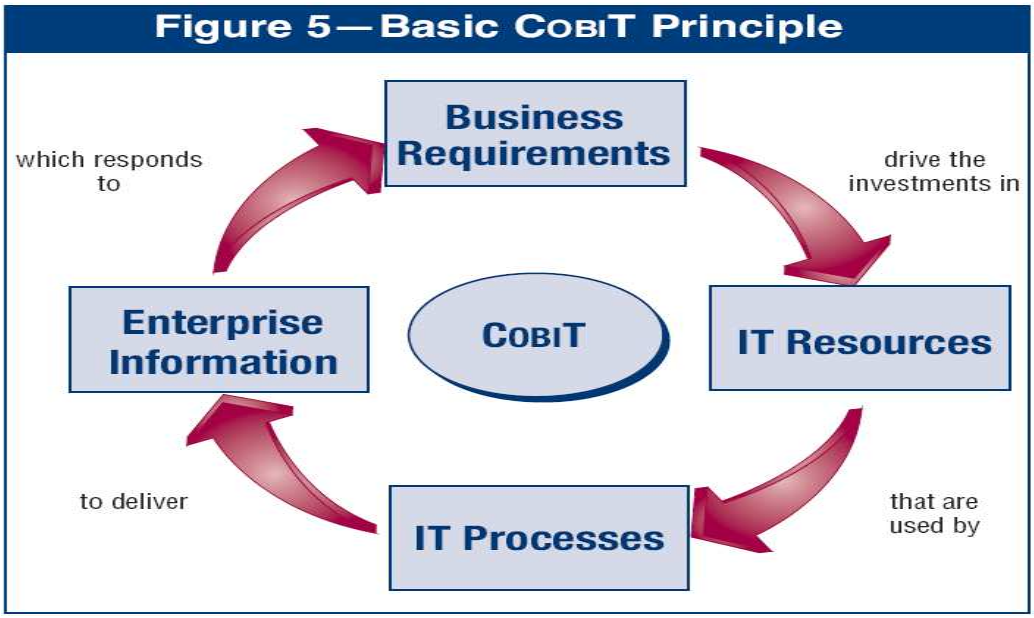
그림 4 | COBIT 프레임워크의 특성



3.1 비즈니스에 초점

○ COBIT는 서비스 제공자와 사용자, 감사인 뿐만 아니라 보다 중요한 대상인 경영진과 비즈니스 프로세스 책임자들을 위한 종합적인 지침이 될 수 있도록 고안되었음

○ 조직이 그 목적을 달성하는데 필요로 하는 정보를 제공하기 위해서는, 요구되는 정보 서비스를 제공하기 위한 일련의 구조적인 프로세스를 이용해 IT 자원을 관리하고 통제할 필요가 있음



○ COBIT의 정보기준(Information Criteria)

▷ 비즈니스 목적을 만족시키기 위해서 정보는 일련의 통제 기준을 준수해야 함 COBIT는 이를 [정보에 대한 비즈니스 요구사항]이라 부름

▷ 품질 요구사항, 주주에 대한 수탁책임, 보안 요구사항을 기반으로

품질 요구사항	품질, 비용, 서비스 제공
주주에 대한 수탁책임	운영의 효과성 및 효율성, 정보의 신뢰성, 법률과 규정의 준거성
보안 요구사항	기밀성, 무결성, 가용성

▷ 7개의 정보기준을 정의함

효과성	적시에 정확하고 일관성 있으며, 사용 가능한 방식으로 정보 제공
효율성	최적의(가장 생산적이며 경제적인) 자원 활용을 통한 정보 제공
기밀성	민감한 정보를 불법적인 유출로부터 보호
무결성	비즈니스 가치와 기대에 합당한 것뿐만 아니라 정보의 정확성과 완전성 제공
가용성	현재와 미래에 비즈니스 프로세스가 요구할 때 이용 가능한 정보
준거성	내부정책과 외부에서 부과된 비즈니스 기준 충족
신뢰성	경영진이 조직을 운영하고 주주에 대한 수탁책임과 거버넌스 책임을 수행하기 위한 적절한 정보의 제공

○ 비즈니스 목표와 IT 목표

▷ 정보 기준은 비즈니스 요구사항들을 정의하기 위한 일반적인 방법을 제시

▷ 일련의 일반적인 비즈니스나 IT 목표를 정의하는 것은 비즈니스 요구사항을 수립하고, 이런 목표 대비 측정 기준을 개발하기 위한 비즈니스 지향적이고, 정교한 기반을 제공

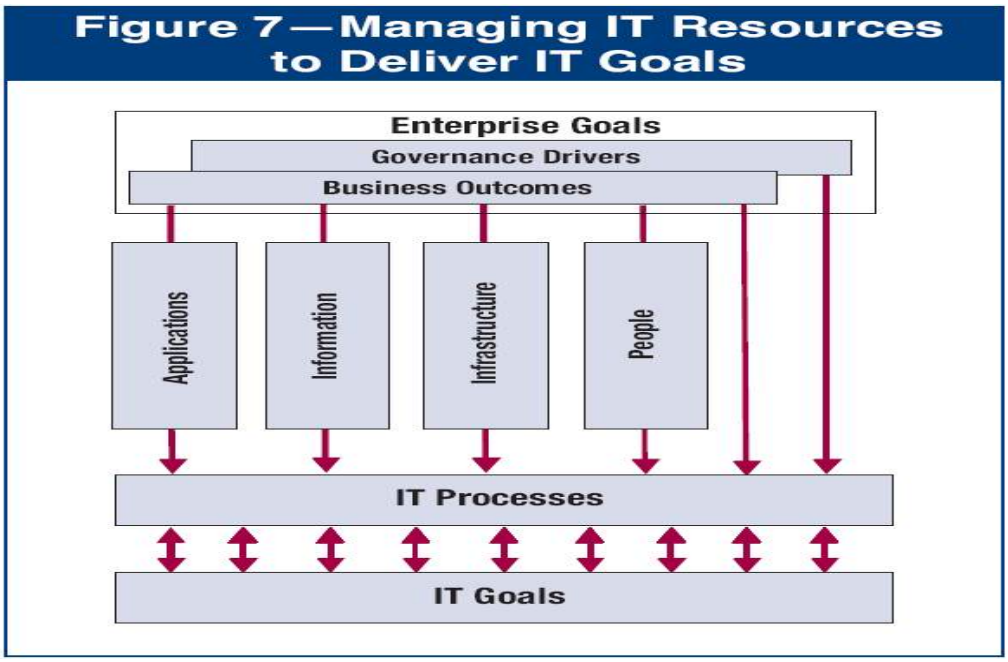
LINKING BUSINESS GOALS TO IT GOALS

		Business Goals	IT Goals								COBIT Information Criteria						
											Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24														
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22							
	3	Improve corporate governance and transparency.	2	18													
Customer Perspective	4	Improve customer orientation and service.	3	23													
	5	Offer competitive products and services.	5	24													
	6	Establish service continuity and availability.	10	16	22	23											
	7	Create agility in responding to changing business requirements.	1	5	25												
	8	Achieve cost optimisation of service delivery.	7	8	10	24											
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26										
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11												
	11	Lower process costs.	7	8	13	15	24										
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27								
	13	Provide compliance with internal policies.	2	13													
	14	Manage business change.	1	5	6	11	28										
	15	Improve and maintain operational and staff productivity.	7	8	11	13											
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28												
	17	Acquire and maintain skilled and motivated people.	9														

○ IT 자원

▷ COBIT에서는 IT 자원을 다음과 같이 정의하고 있음

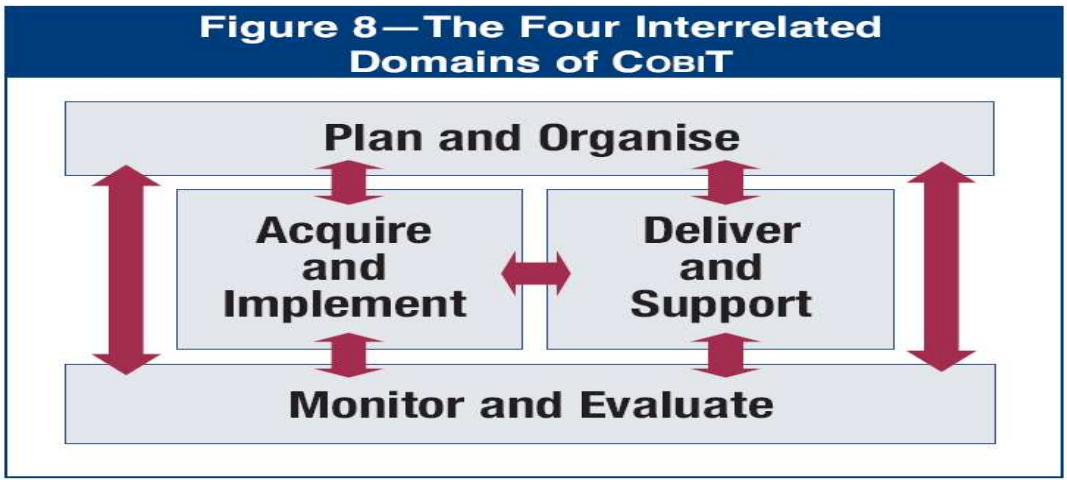
애플리케이션	정보를 처리하는 자동화된 사용자 시스템과 수작업 절차
정보	비즈니스 부문에 의해 사용되는 모든 형태의 데이터로, 정보시스템에 의해 입력이나 처리, 출력되는 모든 형식의 데이터
인프라	애플리케이션의 처리를 가능하게 해주는 기술과 시설
인력	정보시스템이나 서비스에 대한 계획 수립과



3.2 프로세스 지향적

○ COBIT은 IT 활동을 4개의 도메인을 갖춘 하나의 일반적인 프로세스 모델로 정의 (① Plan and Organise, ② Acquire and Implement, ③ Deliver and Support, ④ Monitor and Evaluate)

○ 이 도메인은 IT 부문의 전통적인 책임 영역인 계획 수립, 구축, 운영, 모니터링에 매핑



○ 이 도메인은 운영 모델을 정립하고, 연관된 비즈니스 인력들과의 커뮤니케이션에 활용할 수 있으며, IT를 모니터링하고 측정하기 위한 기반이 됨

3.2.1 PLAN AND ORGANISE (PO)

○ 비즈니스 목표를 달성하기 위해서 IT 전략과 전술을 다루는 도메인
○ 전략적 비전의 구현에 관해서 여러 관점에서 계획하고 의사소통하며, 관리하기 위한 활동이 필요함
○ 다음과 같은 질문에 대응할 수 있어야 한다.
  ▷ IT와 비즈니스 전략이 연계되었는가?
  ▷ 전사차원에서 자원의 최적사용을 하고 있는가?
  ▷ 조직이 IT 목표를 이해하고 있는가?
  ▷ IT 리스크를 이해하며 관리하고 있는가?
  ▷ IT 시스템의 품질이 비즈니스의 요구에 적합한가?

3.2.2 ACQUIRE AND IMPLEMENT (AI)

○ IT전략을 실현하기 위해서 IT 솔루션을 식별, 개발, 획득, 통합하고 구현하는 도메인
○ 다음과 같은 질문에 대응할 수 있어야 한다.
  ▷ 신규 프로젝트가 비즈니스의 요구를 만족시키는 솔루션을 공급할 수 있는가?
  ▷ 신규 프로젝트가 예산 범위 내에서 적시에 솔루션을 공급할 수 있는가?
  ▷ 신규 시스템이 구현 시에 적합하게 동작할 수 있는가?
  ▷ 현재의 비즈니스 운영에 혼란을 최소화하고 변화가 가능한가?

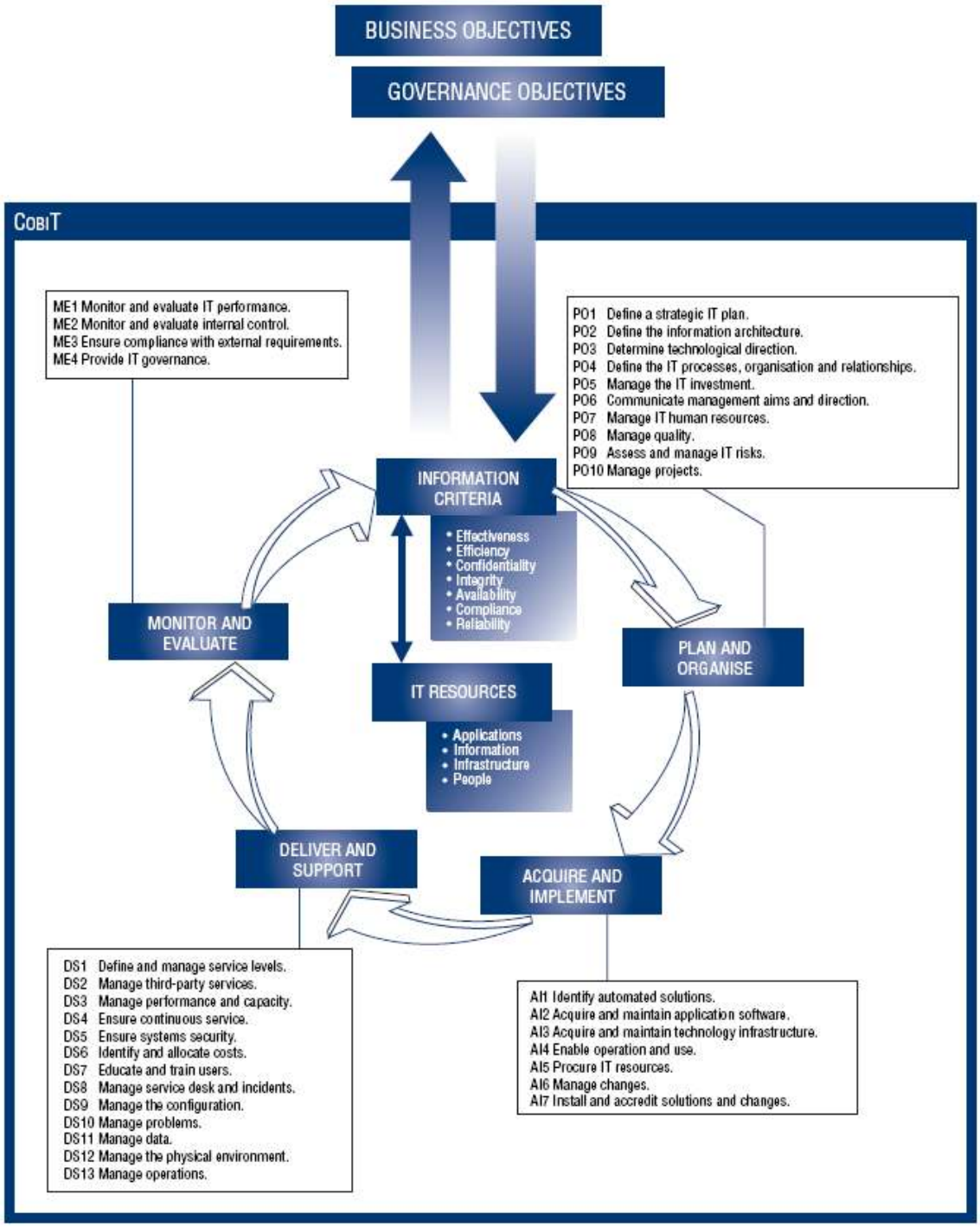
3.2.3 DELIVER AND SUPPORT (DS)

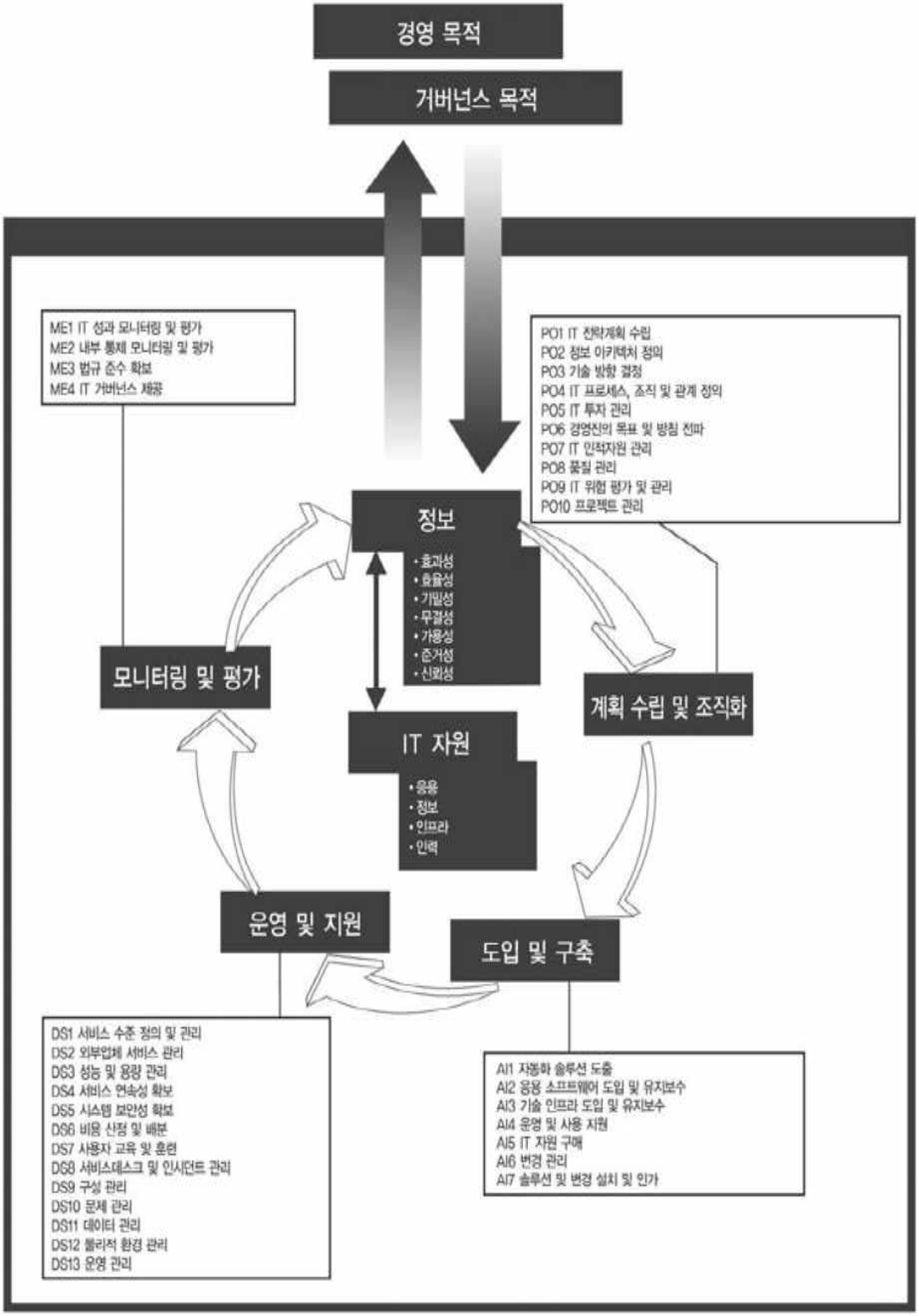
○ 요구된 서비스를 실제적으로 공급하기 위한 도메인
○ 서비스 공급, 재난 및 보안 관리, 사용자 서비스 지원, 데이터 관리, 운영 및 설비 관리 등을 포함
○ 다음과 같은 질문에 대응할 수 있어야 한다.
  ▷ IT 서비스가 비즈니스 우선순위와 부합하게 제공되는가?
  ▷ IT 비용은 최적화 되었는가?
  ▷ 직원들이 IT 시스템을 생산적으로, 안전하게 사용할 수 있는가?
  ▷ 적정한 보안성, 무결성, 가용성이 적소에 위치 하는가?

3.2.4 MONITOR AND EVALUATE (ME)

○ 정기적으로 IT Process의 품질과 통제요건준수의 수준을 측정하고 평가하는 도메인
○ 다음과 같은 질문에 대응할 수 있어야 한다.
  ▷ 사전에 문제를 탐지하기 위해 IT 성과를 측정하는가?
  ▷ 관리진이 내부 통제가 효과적이고 효율적이라는 것을 보장하는가?
  ▷ IT 성과로부터 비즈니스 목표로의 연계가 가능한가?
  ▷ 리스크, 통제, 준수, 성과를 측정하고 리포트하고 있는가?

Figure 23—Overall CobiT Framework




경영 목적
거버넌스 목적
ME1 IT 성과 모니터링 및 평가
ME2 내부 통제 모니터링 및 평가
ME3 법규 준수 확보
ME4 IT 거버넌스 제공
PO1 IT 전략계획 수립
PO2 정보 아키텍처 정의
PO3 기술 방향 결정
PO4 IT 프로세스, 조직 및 관계 정의
PO5 IT 투자 관리
PO6 경영진의 목표 및 방침 전파
PO7 IT 인적자원 관리
PO8 품질 관리
PO9 IT 위험 평가 및 관리
PO10 프로젝트 관리
정보
• 효과성
• 효율성
• 기밀성
• 무결성
• 가용성
• 준거성
• 신뢰성
모니터링 및 평가
계획 수립 및 조직화
IT 자원
• 응용
• 정보
• 인프라
• 인력
운영 및 지원
도입 및 구축
DS1 서비스 수준 정의 및 관리
DS2 외부업체 서비스 관리
DS3 성능 및 용량 관리
DS4 서비스 연속성 확보
DS5 시스템 보안성 확보
DS6 비용 산정 및 배분
DS7 사용자 교육 및 훈련
DS8 서비스데스크 및 인시던트 관리
DS9 구성 관리
DS10 문제 관리
DS11 데이터 관리
DS12 물리적 환경 관리
DS13 운영 관리
AI1 자동화 솔루션 도출
AI2 응용 소프트웨어 도입 및 유지보수
AI3 기술 인프라 도입 및 유지보수
AI4 운영 및 사용 지원
AI5 IT 자원 구매
AI6 변경 관리
AI7 솔루션 및 변경 설치 및 인가

○ IT 목표와 IP Process 연계

▷ Business 목표를 IT 목표로 변환하고, 이렇게 변환된 IT 목표를 전개할 수 있도록 하기 위해서 IT 목표를 필요한 IP Process와 정보요건에 매핑시킴

LINKING IT GOALS TO IT PROCESSES

	IT Goals	Processes										COBIT Information Criteria						
												Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4						P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimise the use of information.	PO2	DS11										S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3							P	P		S			
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6								P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5								P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5									S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5									P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2										P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7								P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4				P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8						P	S					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2						S	S	P	P	P	S	S
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9						S	P					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10						P	P		S	S		
17	Protect the achievement of IT objectives.	PO9	DS10	ME2								P	P	S	S	S	S	S
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9										S	S	P	P	P	S	S
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12									P	P	S	S	S
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5								P			P	S	S	
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2				P	S		S	P		
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12							P	S		S	P		
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13							P	P			P		
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6									S	P					S
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10									P	P		S			S
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5									P	P		P	P		S
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4									S	S		P	S
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4							P	P					P

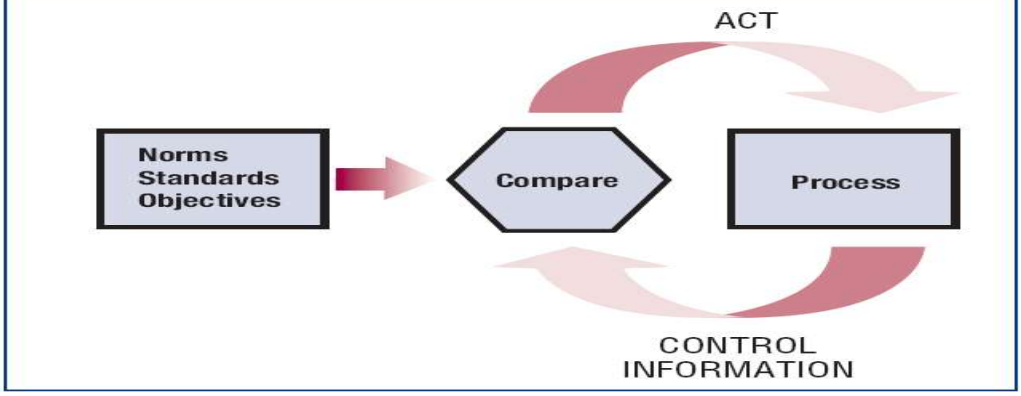
3.3 통제 기반

○ 통제는 비즈니스 목적을 달성하고 바람직하지 못한 사건들의 예방과 탐지, 수정을 적절하게 보증하기 위한 정책이나 절차, 사례, 조직구조 등으로 정의됨

○ IT 통제 목적이란 특정한 IT 활동에 통제 절차를 구현함으로써 달성하려는 결과나 목적을 선언한 것임

○ IT 통제 목적은 각각의 IT 프로세스의 효율적인 통제를 위해 경영진에의해 고려된 높은 수준의 완전한 요구사항의 집합을 제공함

Figure 9—Control Model



○ IT 일반통제와 애플리케이션통제

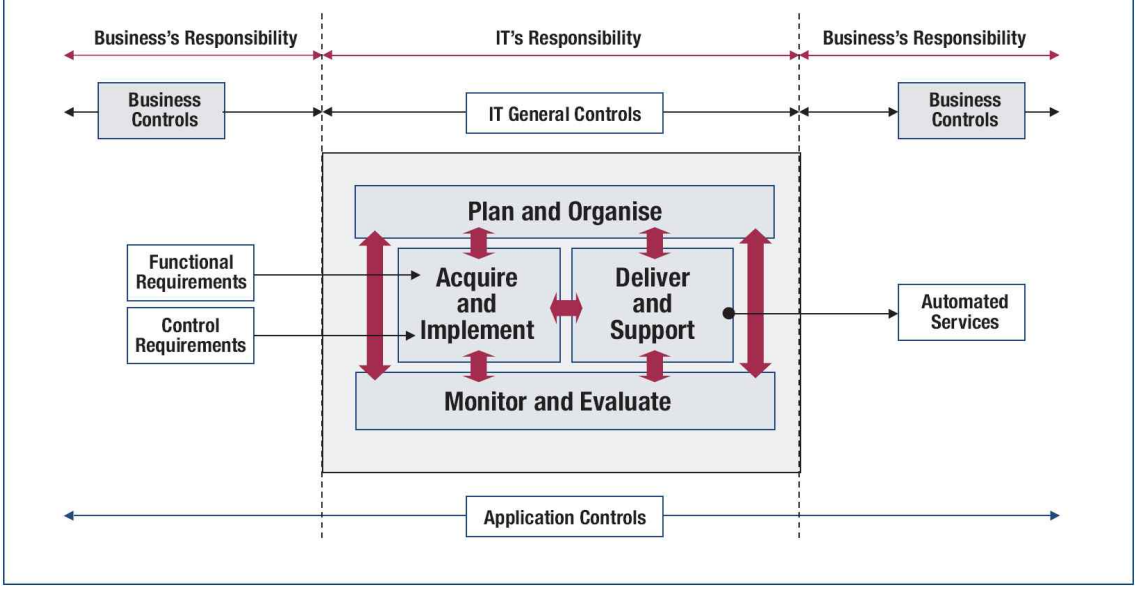
▷ 일반 통제 : IT 프로세스나 서비스에 내제된 통제를 말하는 것으로, 시스템 개발, 변경관리, 보안, 컴퓨터 운영 등을 포함

▷ 애플리케이션 통제 : 비즈니스 프로세스 애플리케이션에 내제된 통제를 의미하며, 완전성, 정확성, 타당성, 승인, 직무 분리 등이 이에 속함

▷ COBIT는 자동화된 애플리케이션 통제의 설계와 구현은 IT의 책임이고, 애플리케이션 통제의 운영적인 관리와 통제 책임은 비즈니스 프로세스 부분임

▷ COBIT의 IT 프로세스들은 애필리케이션 통제가 아닌 IT 일반통제를 담당

Figure 10—Boundaries of Business, General and Application Controls



3.4 측정 주도

○ 모든 조직의 기본적인 요구는 자신들의 IT 시스템 현황을 이해하고, 조직이 제공해야 할 관리나 통제 수준을 결정하는 것

○ 하지만 조직의 성과 수준에 대한 객관적인 시각을 확보하는 것이 용이한 일은 아님

▷ 무엇을 측정하고 어떻게 측정해야 하는지

▷ 현재 자신들의 위치가 어디쯤이며 어느 부문에 개선이 필요한지를 측정하고, 이런 개선을 모니터링하기 위한 관리 도구들을 구현해야 함

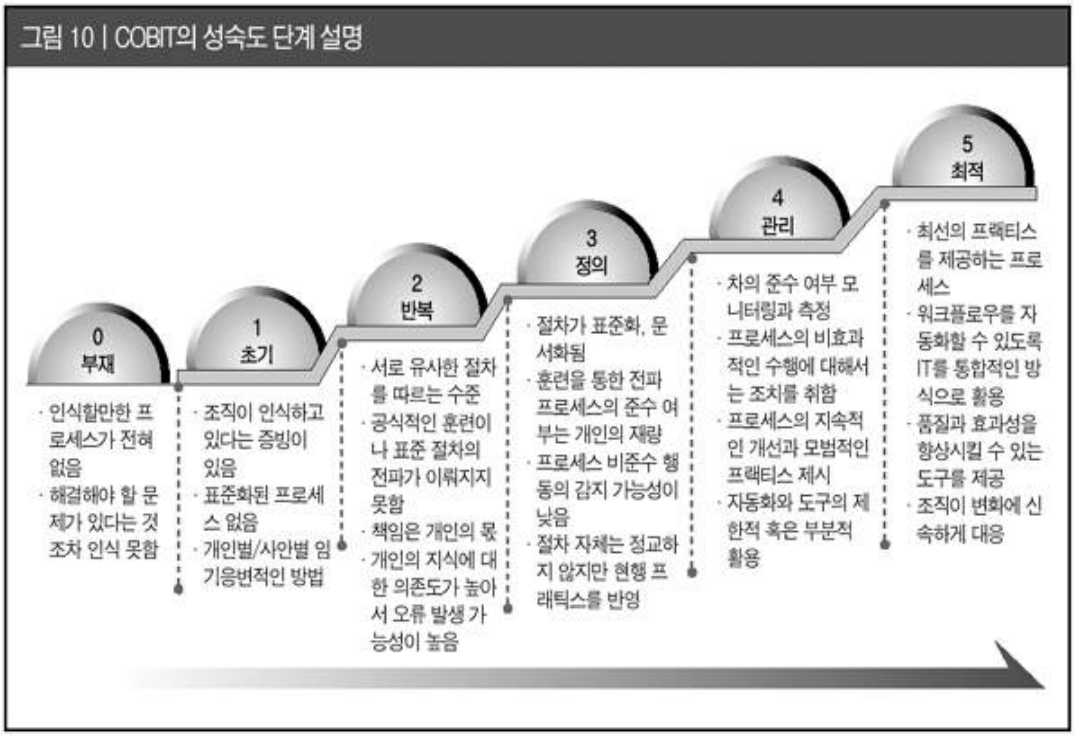
○ 이런 질문에 대한 답을 제시하기 위해 COBIT는 성숙도 모델(Maturity Model)과 성과목표와 측정 기준(Performance goals and metrics), 활동 목표(Activity goals) 등을 제공함

3.4.1 성숙도 모델

○ 조직은 비용 대비 효과를 고려해 적절한 수준의 관리와 통제를 수행해야 함

○ COBIT는 SEI의 성숙도 모델(CMMI)을 기반으로 성숙도 모델을 작성했음

그림 10 | COBIT의 성숙도 단계 설명



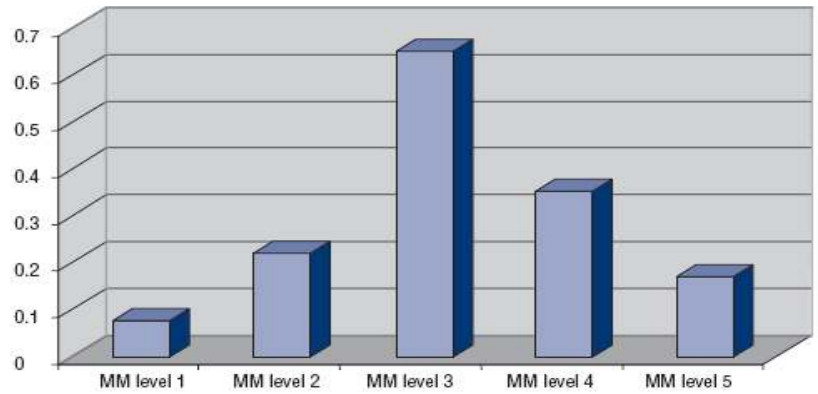
○ 성숙도 모델을 이용하여 조직 내 실제 성과조직의 현재 위치나 업계의 현황, 조직의 개선 목표나 조직이 원하는 위치 등과 같은 사항을 파악할 수 있음

○ 성숙 단계는 현재는 물론 미래의 상태에 대한 설명으로 인식할 수 있는 IT 프로세스의 프로파일로 작성됨

○ 이 성숙 단계는 하위 단계의 모든 조건들을 총족시키지 않고는 다음 단계로 발전할 수 없는 임계치 모델로 개발된 것은 아님

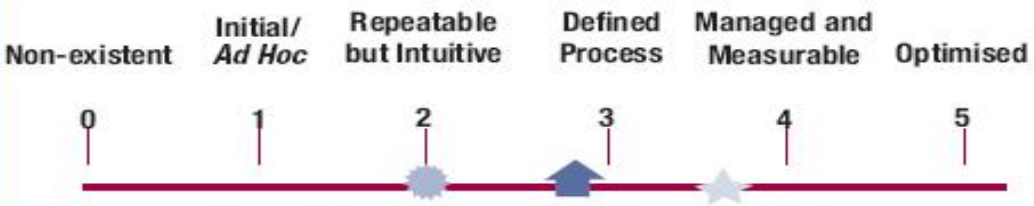
○ COBIT의 성숙도 모델은 역량에 초점을 맞춘 것이며, 성과에 중점을 둔 것은 아님
역량의 달성 정도는 비용 대비 효과에 입각한 의사결정에 따름
(예. 높은 수준의 보안관리는 조직에서 가장 중요한 시스템에만 초점을 맞춘다)

Figure 11—Possible Maturity Level of an IT Process



Possible maturity level of an IT process: The example illustrates a process that is largely at level 3 but still has some compliance issues with lower level requirements whilst already investing in performance measurement (level 4) and optimisation (level 5)

Figure 12—Graphic Representation of Maturity Models



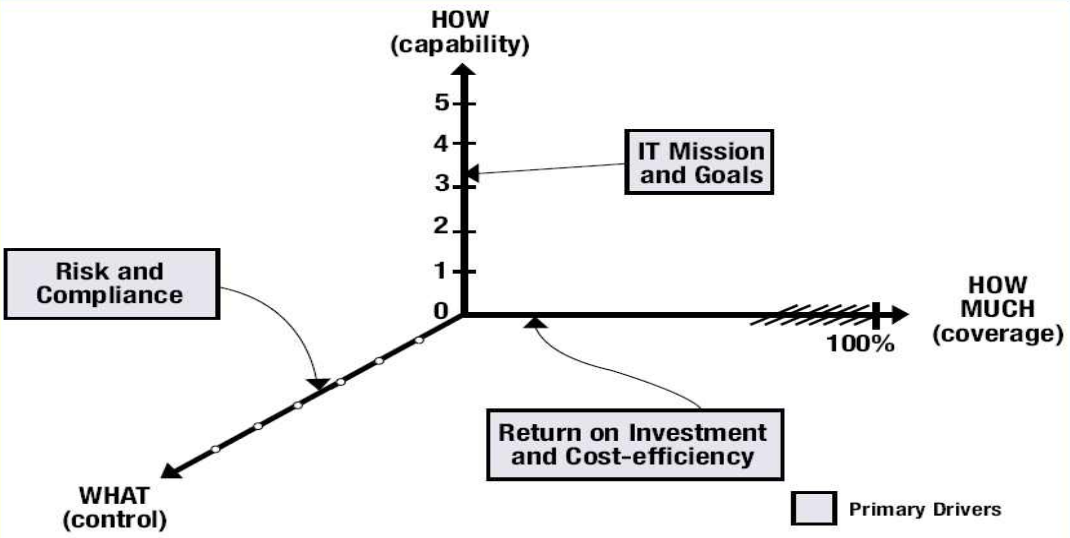
LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Figure 14—The Three Dimensions of Maturity



3.4.2 성과 측정

○ COBIT에서 목표와 측정 기준은 세가지 수준으로 정의

▷ IT 목표와 측정 기준 : 비즈니스가 IT로부터 기대하는 것을 정의하고 그것을 측정하는 것

▷ 프로세스 목표와 측정기준 : IT 프로세스가 IT 목적을 지원하기 위해서 제공해야 하는 것을 정의하고 그것을 측정하는 것

▷ 활동 목표와 측정기준 : 요구되는 성과를 달성하는 프로세스 내부에서 발생하는 필요성을 수립하고 그것을 측정하는 것

Figure 16—Example of Goal Relationships

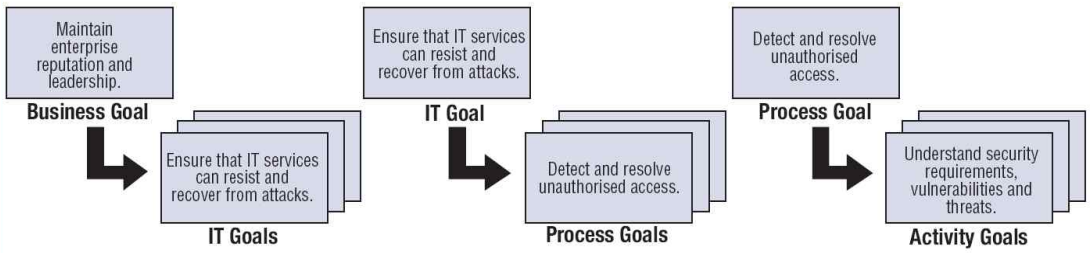


Figure 17—Possible Outcome Measures for the Example in Figure 16

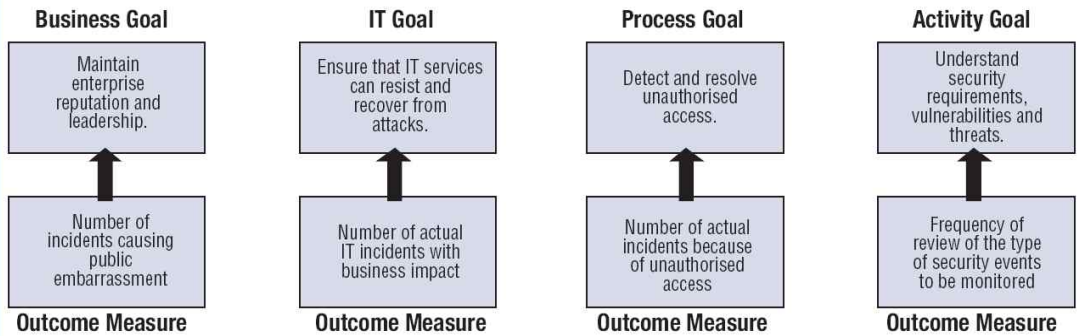
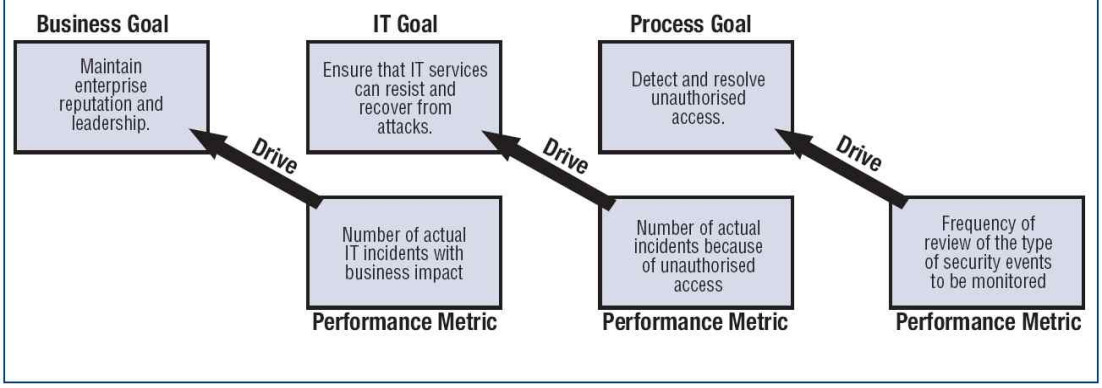
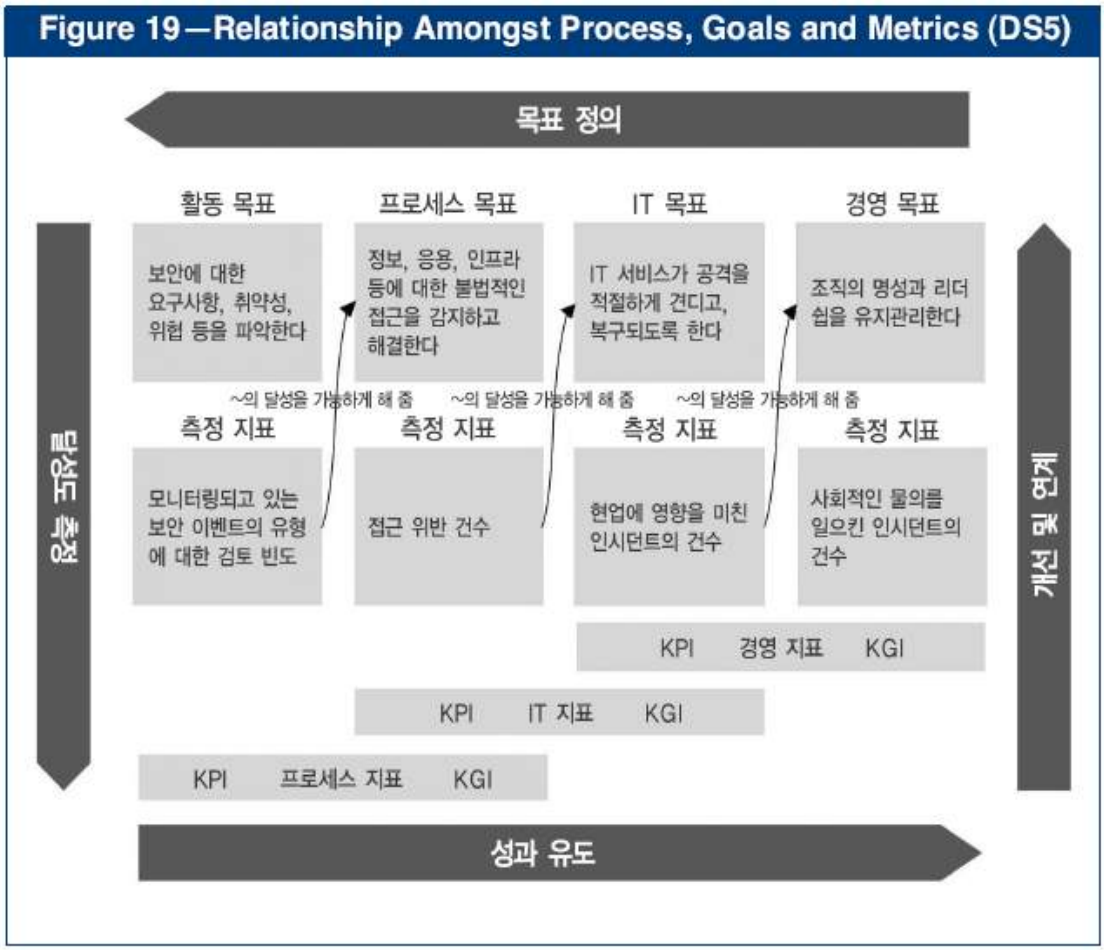


Figure 18—Possible Performance Drivers for the Example in Figure 16





○ COBIT는 목표지표와 성과지표 두 가지 종류의 측정 기준을 사용
하위 수준에서의 목표지표들은 상위 수준에서의 성과지표가 됨

○ 핵심목표지표(KGI : Key Goal Indicator) : IT 프로세스가 비즈니스 요구사항을 달성했는지를 사후적으로 말해주는 지표로, 보통 정보기준 용어로 표현

○ 핵심성과지표(KPI : Key Performance Indicator) : IT 프로세스가 목표를 달성할 수 있도록 얼마나 잘 수행되고 있는지를 파악하는 지표로, 목표의 달성 가능성을 나타내는 선행지표로, 역량이나 사례, 스킬 등을 잘 나타낸다

○ KGI는 목표 수준을 정하기 위한 정성적 지표이며, KPI는 목표 달성 수준을 측정하기 위한 구체적이고 정량적인 지표이다.

4. Governance 영역과 IT 프로세스 연계

○ COBIT의 Best Practice는 중요한 Governance 수단을 제공함

○ COBIT 구성요소와 IT 거버넌스의 연관성

	목표	측정기준	실행	성숙도 모델
전략적 정렬	P	P		
가치 전달		P	S	P
위험 관리		S	P	S
자원 관리		S	P	P
성과 측정	P	P		S

○ COBIT은 IT 프로세스를 4개의 도메인, 34개의 프로세스로 구성하고 있는데, 이를 IT Governance Focus Area와 매핑키실 수 있다.

		IT Governance Focus Areas					COSO					COBIT IT Resources				COBIT Information Criteria						
	IMPORTANCE	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring	Application	Information	Infrastructure	People	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Plan and Organise																						
PO1 Define a strategic IT plan.	H	P		S	S			P		S	S					P	S					
PO2 Define the information architecture.	L	P	S	P	S				P	P						S	P	S	P			
PO3 Determine technological direction.	M	S	S	P	S			S	P	S						P	P					
PO4 Define the IT processes, organisation and relationships.	L	S		P	P		P			S	S					P	P					
PO5 Manage the IT investment.	M	S	P	S		S		S	P							P	P					S
PO6 Communicate management aims and direction.	M	P			P		P			P						P					S	
PO7 Manage IT human resources.	L	P		P	S	S	P			S						P	P					
PO8 Manage quality.	M	P	S		S		P		P	S	P					P	P		S			S
PO9 Assess and manage IT risks.	H	P			P			P								S	S	P	P	P	S	S
PO10 Manage projects.	H	P	S	S	S	S	S	S	P		S					P	P					
Acquire and Implement																						
AI1 Identify automated solutions.	M	P	P	S	S				P							P	S					
AI2 Acquire and maintain application software.	M	P	P		S				P							P	P		S			S
AI3 Acquire and maintain technology infrastructure.	L			P					P							S	P		S	S		
AI4 Enable operation and use.	L	S	P	S	S				P	S						P	P		S	S	S	S
AI5 Procure IT resources.	M		S	P					P							S	P				S	
AI6 Manage changes.	H		P	S				S	P		S					P	P		P	P		S
AI7 Install and accredit solutions and changes.	M	S	P	S	S	S			P	S	S					P	S		S	S		
Deliver and Support																						
DS1 Define and manage service levels.	M	P	P	P		P	S		P	S	S					P	P	S	S	S	S	S
DS2 Manage third-party services.	L		P	S	P	S	P	S	P		S					P	P	S	S	S	S	S
DS3 Manage performance and capacity.	L	S	S	P	S	S			P		S					P	P			S		
DS4 Ensure continuous service.	M	S	P	S	P	S	S		P	S						P	S			P		
DS5 Ensure systems security.	H				P				P	S	S							P	P	S	S	S
DS6 Identify and allocate costs.	L		S	P		S			P								P					P
DS7 Educate and train users.	L	S	P	S	S		P			S						P	S					
DS8 Manage service desk and incidents.	L		P			S	S			P	P					P	P					
DS9 Manage the configuration.	M		P	P	S				P							P	S			S		S
DS10 Manage problems.	M		P		S	S			P	S	S					P	P			S		
DS11 Manage data.	H		P	P	P				P										P			P
DS12 Manage the physical environment.	L			S	P			S	P										P	P		
DS13 Manage operations.	L			P					P	S						P	P		S	S		
Monitor and Evaluate																						
ME1 Monitor and evaluate IT performance.	H	S	S	S	S	P				S	P					P	P	S	S	S	S	S
ME2 Monitor and evaluate internal control.	M		P		P						P					P	P	S	S	S	S	S
ME3 Ensure compliance with external requirements.	H	P			P				P	S	S										P	S
ME4 Provide IT governance.	H	P	P	P	P	P	P	S		S	P					P	P	S	S	S	S	S

Note: The COSO mapping is based on the original COSO framework. The mapping also applies generally to the later COSO *Enterprise Risk Management—Integrated Framework*, which expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. Whilst it is not intended to and does not replace the original COSO internal control framework, but rather incorporates the internal control framework within it, users of COBIT may choose to refer to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.

5. 구현계획 수립시 주의사항

○ 구현에 앞서 관련당사자들의 참여를 통해 조직의 프레임워크를 수립하고, 명백한 책임과 역할을 부여한다.

○ IT 전략과 비즈니스 목표를 정렬한다. IT가 현재의 비즈니스 목표 달성에 충분한 공헌을 하고 있는지 검토한다. 비즈니스 환경과 위험에 대한 선호도, 비즈니스 전략을 이해하고 IT에 연계시킨다. COBIT의 관리가이드라인과 프레임워크 정보기준을 활용하여 IT 목표를 정의한다. ITIL과 함께 사용할 때는 서비스와 SLA를 최종사용자 용어로 정의한다.

○ 리스크를 이해하고 정의한다. 비즈니스 목표가 주어지면 IT가 이들 목표를 달성하기 위해 필요한 역량과 관련된 리스크가 무엇인지 확인한다.

○ 목표영역을 정의하고, 리스크 영역을 관리하기 위한 핵심프로세스 영역을 식별한다. COBIT 프로세스 프레임워크를 기본으로 사용하고, ITIL의 핵심 서비스공급 프로세스의 정의와 ISO 27001의 보안 목표를 보조수단으로 사용할 수 있다.

○ 현재의 역량을 분석하고 갭을 식별한다. 성숙도 및 역량 진단을 수행하고 가장 개선이 필요한 부문을 찾아낸다. COBIT 관리가이드라인을 기본으로 하고, 상세사항은 ITIL과 ISO27001의 베스트 프랙티스를 참고할 수 있다.

○ 개선 전략을 수립하고, 핵심영역의 관리와 Governance를 개선하기 위한 프로젝트들 중에서 가장 우선순위가 높은 프로젝트를 선정한다. 선정기준은 잠재적 효과와 구현의 용이성에 토대를 두도록 한다.

○ 현재 성과를 측정하고, 개선결과를 모니터링하기 위해 스코어카드 메커니즘을 구축한다. 이때 전략구현을 지원할 수 있는 조직구조 등 주요 이슈를 고려하고, 리스크 관리의 책임이 조직 내부에 구현되어 있는지 확인한다. 또한 전략과 목표를 알 필요가 있는 모든 사람과 효과적으로 의사소통할 수 있도록 한다. COBIT 관리 가이드라인 중 "KGI와 정렬된 KPI'을 참고하여 스코어카드 메커니즘을 구현한다.

○ 상기 과정을 정기적으로 반복하여 수행한다.