IT Control Objectives for Sarbanes-Oxley

The Role of IT in the Deign and Implementation of Internal Control Over Financial Reporting

Feb.16.2009

조희준(Joseph)
(주)키삭 KISAC

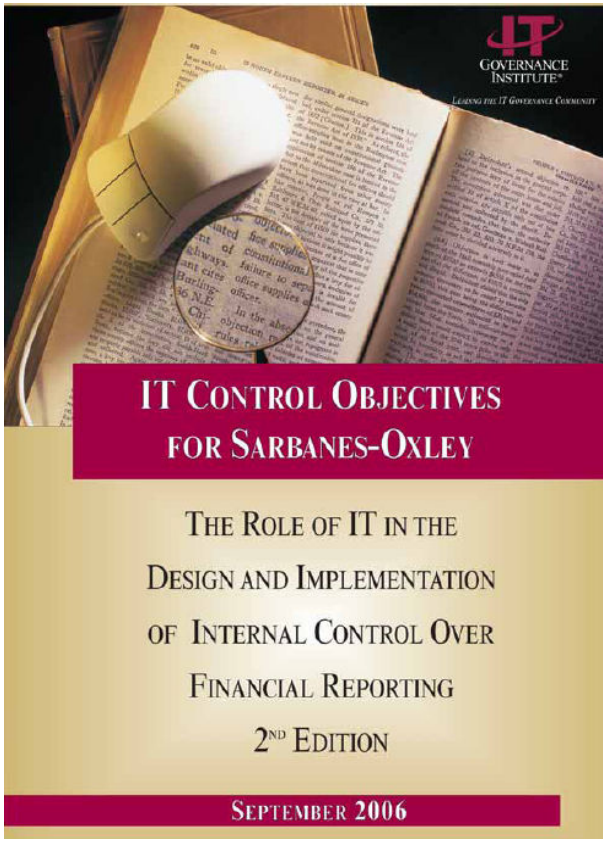
CIA, CISA, CISM, CGEIT, COBIT, CISSP, PMP, ITIL, IT-EAP, ISO 27001, IS Auditor

ISACA Korea GRA

Index

1. Sabanes-Oxley Act?
2. Executive Summary
3. 신뢰성 있는 재무보고의 기초
4. 변화에 적응하기 위한 인적자원관리
5. Ground Rule (기본규칙) 정하기
6. COSO
7. IT준수의 Road Map
8. SOX법의 기본서
9. COSO와의 접목

10. 맺는 말



Sabanes-Oxley Act?

먼저 Sabanes-Oxley Act(사베인-옥슬리 법안)이 무엇인가?

사베인 – 옥슬리소개

- SOX법은 기업 재무보고의 신뢰성을 위한 미국의 기업 개혁법.
- 2002년 에너지 대기업 엔론의 최고 경영자 케네스 레이가 저지른 회계 부정으로 하루아침에 몰락.
- 2002년 통신회사인 월드컴도 회계부정의 스캔들.

- 미국 의회가 기업에 대한 회계 및 재무보고의 투명성을 높이자는 취지로 엄격한 기업 개혁법안을 제정.
- 사베인과 옥슬리는 미국의회의 상,하원의원의 이름이며 2002년 7월 30일 부시 대통령에 의해 서명.

Sabanes-Oxley Act?

- SOX법의 핵심은 302조 및 404조에 명시.
- 회사의 최고경영자(CEO) 및 최고재무책임자(CFO)는 내부통제시스템에 대한 연대책임을 가지고 이를 구축, 운영 및 자발적 검증을 통해 그 결과를 미국 증권거래위원회(SEC)에 보고해야 한다.
- 또한 내부통제에 대한 중대한 문제점이 발견되면 즉시 해결해야 함은 물론 그 내용을 공시하여야 한다. 만일, 경영진이 허위사실을 알고 있었을 경우나 재무제표가 경영진에 의해 의도적으로 왜곡되었을 경우 민형사상의 책임을 지게 된다.
- 기업은 투명성이 전제되어야 외부 이해관계자와 상호 신뢰를 쌓고 발전적인 관계를 구축할 수 있다.
- 또한 내부 구성원들 사이의 신뢰도 강해져 업무 효율 상승 및 회사에 대한 충성도가 높아지게 된다.
- 즉, 기업의 투명성은 소비자를 위한 핵심 가치일 뿐만 아니라 경쟁 기업과 차별화할 수 있는 핵심 역량이다.

Executive Summary

준수(compliance)와 IT거버넌스

- 보다 정확하고 시기 적절한 재무보고를 위해서는 통제의 계획과 관리전반에 걸친 IT거버넌스의 결과로 달성.

- 단지 SOX를 준수한다는 것보다는 경영의 요구사항의 대응과 책임추적성에 기인한 강한 거버넌스 모델이 필요.

- IT와 효율적 내부통제의 효과
  - 조직 전반적 IT거버넌스 강화
  - 경쟁우위를 지키는 효과 효율적 운영
  - 위험관리로 경쟁우위 확보
  - 고위경영진의 IT에 대한 이해

Executive Summary

제 2판의 향상된 점

- Top-down 하향식 접근방법
- Risk Based 접근 – 완벽한 해결책이 아닌 위험을 기반한 접근방법 제시
- 통제의 우선수위
- COBIT 4.0과의 상호참조
- 직무분리(Segregation Of Duties; SOD) 강조

중소기업을 위한 고려사항

- COSO (Committee of Sponsoring Organizations of the Treadway Commission) 등장
- 위험평가의 필요성

Executive Summary

PCAOB 와 COIT의 연계

- PCAOB (Public Company Accounting Oversight Board) 미국 상장사 회계감사위원회의 등장과 COBIT의 연계

SOX법의 IT통제

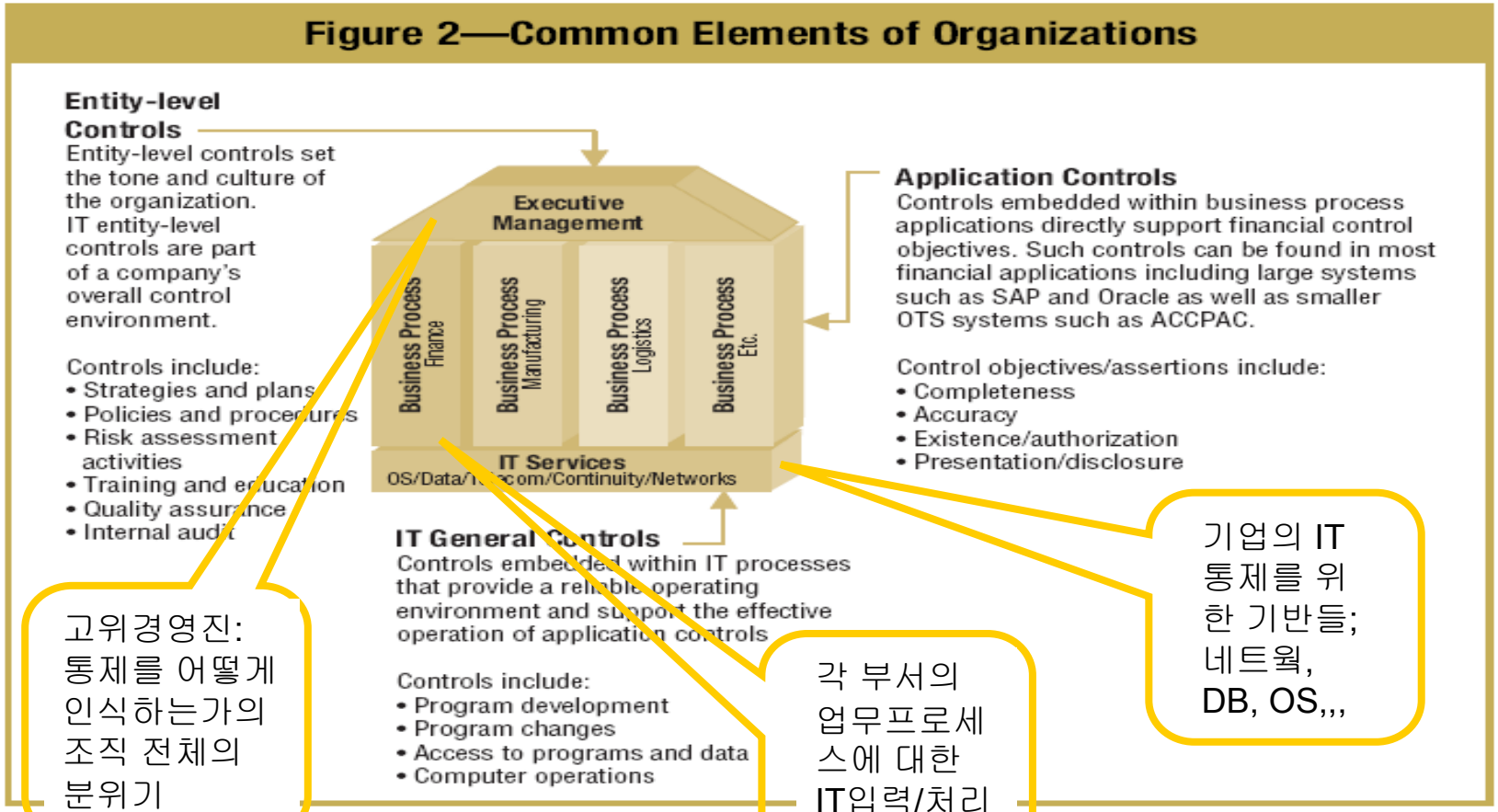
COBIT의 IT통제

Figure 1—Mapping to PCAOB and CobiT

IT Control Objectives for Sarbanes-Oxley	CobiT	PCAOB IT General Controls			
	Mapping to CobiT 4.0 Processes	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire and maintain application software.	AI2	●	●		●
2. Acquire and maintain technology infrastructure.	AI3	●		●	
3. Enable operations.	AI4	●	●	●	●
4. Install and accredit solutions and changes.	AI7	●	●	●	●
5. Manage changes.	AI6		●		●
6. Define and manage service levels.	DS1	●	●	●	●
7. Manage third-party services.	DS2	●	●	●	●
8. Ensure systems security.	DS5			●	●
9. Manage the configuration.	DS9			●	●

신뢰성 있는 재무보고의 기초

재무보고 기초를 위해서 IT통제를 적용하기 위해 조직의 3요소 이해하기



변화에 적응하기 위한 인적자원관리

변화에 대한 공약 획득

- 조직의 공약이 우선

지금 현 상태의 조직평가 – 다음 기준에 의해

- 조직문화
- 변화의 확장성
- 직원들의 변화 수용능력
- 조직의 변화 수용능력

장애물 극복

- 효과적인 의사소통
- 교육과 훈련
- 동기부여

Ground Rule (기본규칙) 정하기

COSO의 내재화

- 내부통제 framework에 기초
- SEC (Securities and Exchange Committee; 미국증권거래위원회)에서 COSO를 강조
- COSO는 AICPA, AAA, FEI, IIA, IMA의 기준을 포함

COSO를 IT에 적용하기 www.coso.org

- SOX의 IT 통제의 핵심

COSO

COSO Cube

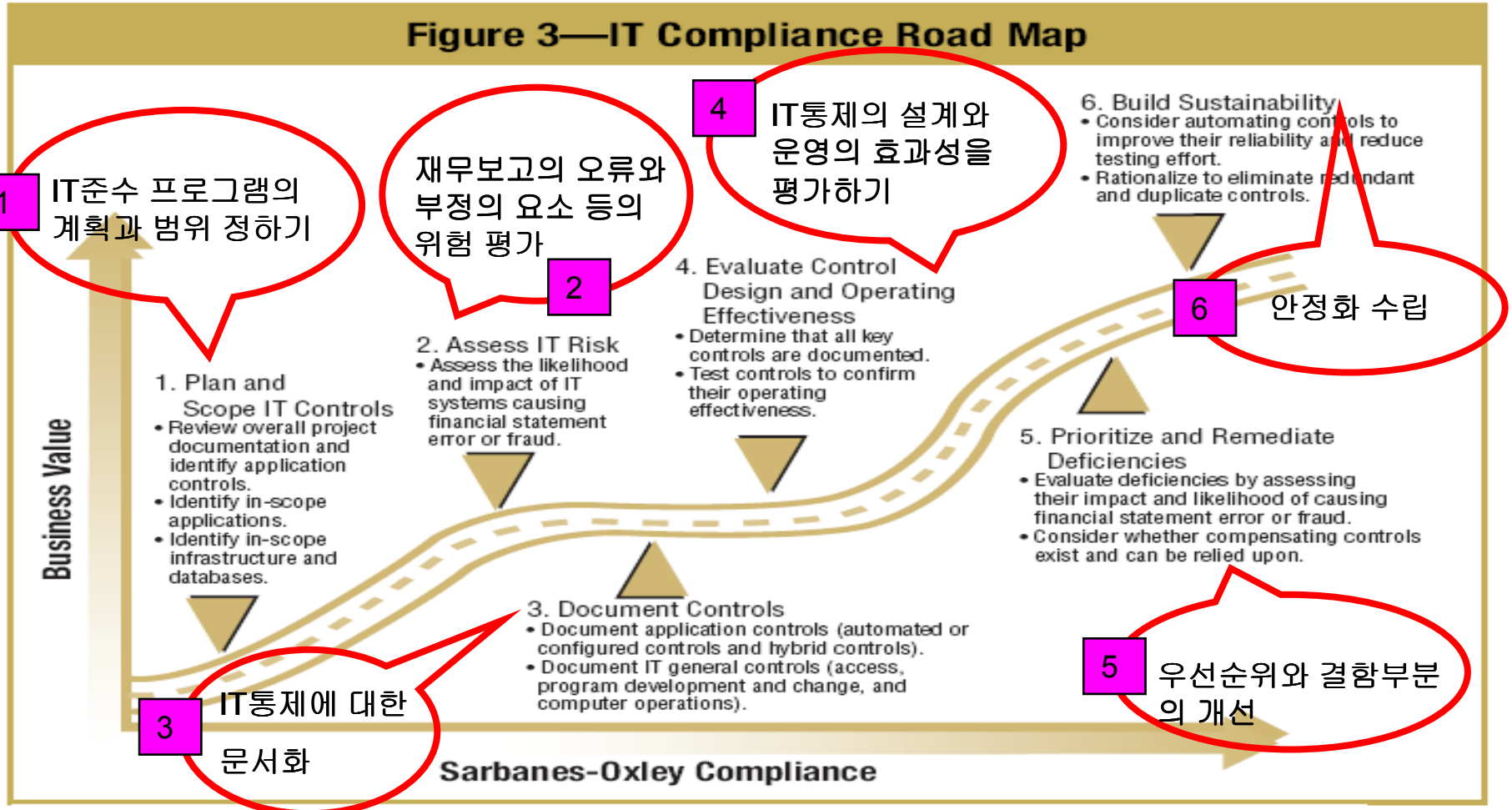
목적:
운영의 효율성
재무보고의 적정성
법, 규정의 준수

관리체계 5가지:
1.기업의 통제환경
2. 위험의 평가
3. 통제 수행활동
4.위험관리의 정보와 의사소통
5.지속적 감시

적용영역:
각 사업장

IT준수의 Road Map

SOX법 준수에 기초한 IT준수



SOX법의 기본서

SOX법 section 302, 404

302

최고경영자 , 최고재무책임자 및 임원들은 재무제표 및 그러한 보고를 관리하는 시스템을 포함한 분기별 보고의 정확성 및 완전성을 개인적으로 보증해야 합니다

404

경영진은 재무보고를 위한 충분한 내부통제구조 및 절차를 확립하고 유지할 책임이 있습니다

Figure 8—Sarbanes-Oxley Requirements Primer

	302	404
Who	A company's management, with the participation of the principal executive and financial officers (the certifying officers)	Corporate management, executives and financial officers ("management" has not been defined by the PCAOB)
What	1. Certifying officers are responsible for establishing and maintaining internal control over financial reporting. 2. Certifying officers have designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.* 3. Any changes in the company's internal control over financial	1. A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company 2. A statement identifying the framework used by management to conduct the required assessment of the effectiveness of the company's internal control over financial reporting 3. An assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including an explicit statement whether internal control over financial reporting is effective 4. A statement that the registered

COSO와의 접목

COSO와 내부통제, 그리고 국제공인 내부감사사(CIA)

맺는 말

감사합니다.
여러분 열심히 하셨습니다.

조 희 준 josephc@chol.com

CISM, CGEIT, CISA, COBIT, CIA, CISSP, PMP, ISO27001, ITIL, IT-EAP, 정보시스템감리원

IT감리,컨설팅법인 ㈜키삭 에서 IT 컨설팅 업무를 맡고 있으며 ISACA(정보시스템감사통제협회) GRA (정부 및 규제기관 대외협력부문)에서 IT Governance에 관한 활동을 하고 있다. IT감사를 확장하고 비즈니스에 연계하는 분야가 관심분야이며 이와 관련해서 원고기고 및 강의 활동도 하고 있으며 고려대학교 대학원 감사행정학과에서 열심히 공부 중이다.