ISSN(Print): 2287-5891

http://dx.doi.org/10.3745/KTCCS.2012.1.2.103

Risk Management interaction model for Process of Information Security Governance

You-jin Song†

ABSTRACT

Recently, IT Governance has been applied to business management environment. In this paper, we study business model that can minimize information security risk using IT governance in cloud computing environment. Especially, we propose the interaction model that link risk management for subject of information security governance. In our model, synergy means the effective, strategic and secure business support. And interaction analysis of BMIS's 4 elements and 6 dynamic interconnections is required. Therefore we propose interaction model which can link risk management based on COSO ERM or COBIT Risk IT Framework.

Keywords : Information Security Governance, Risk Management, Interaction Model, ERM, BMIS, COBIT

정보보호 거버넌스 프로세스를 위한 위험관리 상호작용 모델

송 유 진†

요 약

최근 IT 거버넌스 개념이 기업경영 현장에 적용되고 있다. 본 논문에서는 클라우드 컴퓨팅 환경에서 IT 거버넌스를 기반으로 기업의 정보보호 위험을 최소화할 수 있는 비즈니스 모델에 대해 연구한다. 특히, 정보보호 거버넌스 세부 주제인 위험관리를 연계하는 상호작용 모델(IT 거버넌스 프레임워크인 COBIT과 연계하여 시너지를 높일 수 있는 구조)을 제안하고자 한다. 여기서, 시너지는 효과적, 전략적이고 안전한 비즈니스 지원을 의미하며, BMIS의 4가지 요소, 6가지 역동 연결자와의 상호작용성에 대해 분석이 요구된다. 따라서 COSO ERM이나 COBIT Risk IT Framework를 기반으로 위험관리와 연계될 수 있는 상호작용 모델을 제안한다.

키워드 : 정보보호 거버넌스, 위험관리, 상호작용 모델, ERM, BMIS, COBIT

1. 서 론

IT환경에서 클라우드 환경으로 트랜드가 변화하면서 그에 따른 많은 관심과 기술도 발전하고 있다. 또한, Smart&Mobile 환경으로 인한 비즈니스 프로세스의 변화가 모색되고 있으며 기업의 클라우드 서비스 도입에 따른 위험관리 프로세스가 중요시 되고 있다. 클라우드 컴퓨팅은 최소의 관리 노력으로 빠르게 준비되거나 배포될 수 있는 네트워크, 서버, 스토리지, 애플리케이션, 서비스와 같은 이용 가능한 컴퓨팅 자원의 공유된 풀(POOL)에 대한 주문형 네트워크 접속을 가능하게 하는 편리한 모델이다[1]. 또한, 인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 자원들을 서비스로 제공하는 컴퓨팅의 한 형태로 사용자는 IT 자원(애플리케이션, 스토리지, OS, 보안 등)을 필요한 만큼 빌려서 사용하고, 사용한 만큼만 비용을 지불하는 것이다.

기업의 입장으로는 수많은 정보기기를 구입하고 관리해야 할 조직을 갖추어야 하며, 이를 운영하는 데 소요되는 비용도 점차 증가하게 될 것이고, 이는 기업운영에 큰 부담으로 연결된다. 복잡하거나 값비싼 정보시스템들을 외부에서 싼 가격에 빌려 쓸 수 있다면 점차 아웃소싱을 선호하게 될 것이다.

개인의 입장에서도 전문성을 가지지 못한 다수의 소비자들은 외부의 공격에 무방비로 노출될 뿐만 아니라 해커들에게 좀비 PC로 악용될 수 있는 위험을 지니고 있다. 이러한 경우에 개인이 사용하는 소프트웨어를 직접 다운이 아닌 외부 클라우드 사업자의 서비스를 제공받으면 이러한 문제는 해결된다.

클라우드 컴퓨팅은 기업에게 비용절감, 시간단축, 생산성 및 비즈니스 성장 등의 재정적, 운영적 혜택을 제공하

† 정 회 원 : 동국대학교 정보경영학과 교수
논문접수 : 2012년 4월 12일
수 정 일 : 1차 2012년 9월 17일
심사완료 : 2012년 9월 18일
* Corresponding Author : You-jin Song(song@dongguk.ac.kr)

지만 정보유출 악성코드 감염, 서비스 장애 등 보안 위협에 대한 우려가 여전히 높기 때문에 보안 문제에 대한 보장이 없이 클라우드 서비스 확대에는 한계가 있을 수밖에 없다. 클라우드 서비스 특성상 정보가 한 곳으로 집중되고, 다양한 모바일 기기를 통한 접속이 가능하기 때문에, 향후 클라우드 서비스가 급속도로 활성화 될 경우 많은 해커들의 주 공격대상이 될 가능성이 크다. 이로 인한 피해 규모가 커질 것으로 예상되기 때문에 안전한 클라우드 서비스를 이용하기 위해서는 신규 보안위협 및 사고 발생에 대한 대응이 필요하다[2].

본 논문에서는 기업의 위험에 대하여 평가하고 대응하기 위해, 클라우드 환경을 기반으로 기업의 정보보호 위험을 최소화 할 수 있는 비즈니스 모델에 대해 연구한다. 특히, 클라우드 컴퓨팅의 요소를 관리적 차원과 운영적 차원으로 정의하고 위험관리에 대한 통제를 위해 BMIS 기반의 순환 프로세스 모델을 제시한다. 현재 클라우드 컴퓨팅 환경에서 비교 분석이 가능한 순환 프로세스를 표현하는 상호작용 관련 기존 모델은 제안되고 있지 않다. 그러므로 본 논문에서는 BMIS 기반 순환 프로세스라는 새로운 모델을 제시함으로써, 기존 기법의 비교 대신 BMIS를 이용한 모델을 제시하고자 한다. 즉, BMIS의 4개 요소 중 핵심요소라고 할 수 있는 프로세스 순환 측면에서 COSO ERM Framework, COBIT Cube 및 Risk IT Framework와의 상호작용을 통해 위험 거버넌스 실행체계 개념을 정립한다. 또한, 정보보호 거버넌스 세부 주제인 위험관리를 연계하는 아키텍처(IT 거버넌스 프레임워크인 COBIT과 연계하여 시너지를 높일 수 있는 구조)를 분석하고 제안한다. 한편, 시너지는 효과적, 전략적이고 안전한 비즈니스 지원을 의미하며, BMIS의 4가지 요소와 6가지 역동 연결자와의 상호관련성에 대해 분석이 요구된다. 따라서 COSO ERM이나 COBIT Risk IT Framework를 기반으로 위험관리가 연계될 수 있는 아키텍처를 제안한다.

본 논문의 2장에서는 관련 연구에 대해 기술하고 3장에서는 클라우드 서비스에 대한 위험관리, 4장에서는 위험 거버넌스 프로세스를 검토하고 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 기업의 중요한 정보자산을 관리하고 통제하는 대표적 모델인 COSO ERM과 COBIT Risk IT 프레임워크, COBIT Cube를 설명하고 정보보호 거버넌스의 위험관리와 연계하기 위해 BMIS를 분석한다.

2.1 COSO ERM

기존의 위험관리는 각 부서의 기능별로 위험을 인지하고 관리하는 것이었지만, ERM은 전사적 관점에서 각 부서의 내부 활동에 대한 위험관리가 통합된 활동이다.

COSO(The Committee of Sponsoring Organization of the Treadway Commission)는 경영윤리, 내부통제, 기업지배구조 등의 이슈를 연구하는 미국의 비정부 기구이며, ERM 의 모범 기준인 “Enterprise Risk Management Framework”를 2004년 9월 공개하였다(Fig. 1). 이후 기업에서 효과적인 업무수행을 위해 내부통제의 개념들을 통합한 COSO와 PwC(Price waterhouse Coopers; 미국의 시장조사 및 컨설팅 기관)가 합작하여 만든 Enterprise Risk Management Framework의 개념이 도입되었다[3].

Fig. 1. COSO ERM Framework

COSO ERM Framework는 기업의 내부 통제에 대한 비즈니스의 목표를 저해하는 위험들을 식별하고, 평가하여 이러한 위험들을 회피할 것인지, 대응할 것인지 판단하여 효과적으로 기업 가치를 극대화하는 것을 목표로 한다.

COSO ERM Framework의 8개의 구성요소(내부 환경, 목표 설정, 사건 인식, 위험 평가, 위험 대응, 통제 활동, 정보와 의사소통, 모니터링)들은 가로 행에 제시되어 있고, 4개의 목표 카테고리들(전략, 운영, 보고, 준수)은 세로 열에 제시되어 있다. 또한, 세부사항, 비즈니스 요소, 분배, 개체 등급은 매트릭스의 3번째 차원에 제시되어 있다(Fig. 1).

2.2 Risk IT 프레임워크

COBIT(Control Objectives for Information and related Technology)이나 Val IT(IT Value Delivery)와는 달리 위험관리 측면에서 부각된 Risk IT Framework는 2009년 11월 말 ISACA(Information Systems Audit and Control Association)에서 공식적으로 발표되었다.

10년이 넘게 버전 4.1까지 개정되면서 COBIT은 ISACA의 대표적인 IT 통제 및 거버넌스 프레임워크로 자리 잡았고, ISACA에서 다른 프레임워크의 개발은 필요로 하지 않는 것처럼 보였다. 그러나 최근 Val IT가 발표되었고, 공개 초안 발표로 전문가들의 의견을 수렴하는 과정을 거쳐 2009년 11월 Risk IT 프레임워크가 공식적으로 발표되었다[4].

Risk IT 프레임워크는 COBIT이 가진 위험 부분의 한계점과 이를 개선하기 위한 보완책으로 위험 기반의 접근 방법이다. 기업들은 위험 관리가 얼마나 중요한지 많은 IT 보

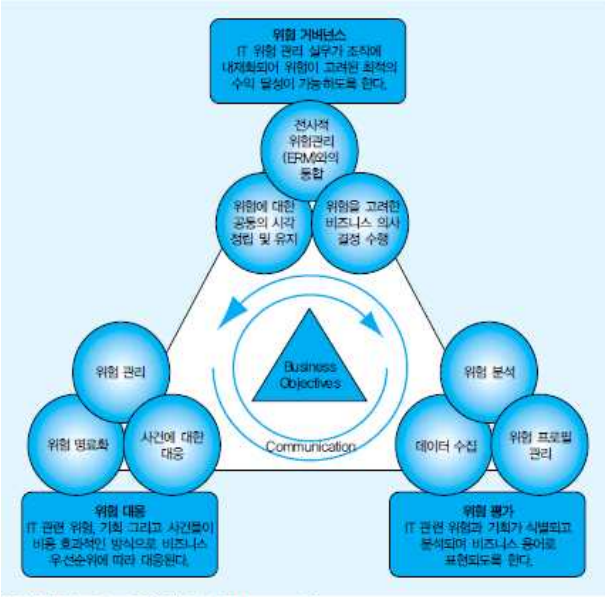

Fig. 2. Risk IT Framework

안 사고를 통해 그 중요성을 절감하게 되었다. 이러한 IT 위험들을 효과적으로 통제, 관리하기 위해 필요한 방법으로써 ISACA는 경영진이 채용해야 할 IT 위험 관리 프레임워크가 Risk IT 프레임워크이다(Fig. 2).

Risk IT 프레임워크의 구성은 COBIT이나 Val IT와의 일관성을 유지하기 위해 거의 동일한 형식을 취하고 있다. Risk IT 프레임워크는 3개의 도메인과 각각 3개의 서브 도메인으로 구성되어 있다(Fig. 2).

그리고 각각의 서브 도메인은 COBIT과 Val IT와 마찬가지로 7개 부분으로 구성되어 있다[5].

Table 1. Risk IT Framework Structure

위험 거버넌스(Risk Governance)	
A. RG1	위험에 대한 공통의 시각 정립 및 유지
B. RG2	전사적 위험관리(ERM)와의 통합
C. RG3	위험을 고려한 비즈니스 의사결정 수행
위험 평가(Risk Evaluation)	
A. RE1	데이터 수집
B. RE2	위험 분석
C. RE3	위험 프로필 관리
위험 대응(Risk Response)	
A. RR1	위험 명료화
B. RR2	위험관리
C. RR3	사건에 대한 대응

2.3 COBIT Cube

COBIT(Control OBjectives for Information related Technology)은 가장 권위 있는 IT 거버넌스 통제 프레임워크로서 국제적으로 인정받고 있다. COBIT은 IT 프로세스와 이들의 관리를 위한 프레임워크이며 기존의 다양한 표준과

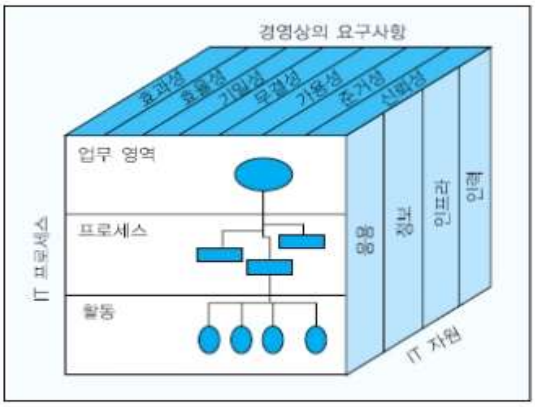

Fig. 3. COBIT Cube

실무를 참조하고 포괄하는 지식 베이스라고 할 수 있다.

COBIT의 프레임워크 원칙은 IT는 조직이 그 목적을 달성하기 위해 필요로 하는 정보를 제공해야 한다는 것이다. 이에 따라 COBIT 프레임워크는 세 가지 요소로 구성된다. 경영 요구사항, IT 프로세스, IT 자원이 그것이다. 경영 요구사항은 이해 관계자들이 IT에 기대하는 것으로, 정보 기준으로 나타난다. 즉, 경영 요구사항을 만족하는 정보기준을 달성할 수 있도록 IT 프로세스는 IT 자원을 관리한다. 정보 기준은 목적이며, IT 프로세스는 방법이며, IT 자원은 수단이 된다. Fig. 3은 COBIT 프레임워크의 구성을 보여주는 COBIT 큐브이다.

COBIT 프로세스 모델은 IT 자원을 관리하기 위한 업무 영역을 4개로 구분한다. 계획 수립 및 조직화, 도입 및 구축, 운영 및 지원, 모니터링 및 평가가 그것이다. 이 업무 영역은 IT 부문의 전통적인 책임 영역인 계획 수립, 구축, 운영, 모니터링에 매핑된다. COBIT은 이 업무 영역 내 총 34개의 IT 프로세스를 제시하고 있다[6].

2.4 BMIS

정보보호 거버넌스 프레임워크인 BMIS(Business Model for Information Security)는 4개의 요소와 6개의 동적연결자에 의해 외부 환경에 따라 밀어지거나 당겨짐으로써 힘의 균형을 유지한다(Fig. 4). BMIS의 핵심을 이루는 4개의 각 요소에 대한 설명은 다음과 같다.

① 조직 설계와 전략(Organization Design and Strategy)
- 설계는 조직이 전략을 구현하는 구체적인 방법을 말하며 전략은 또한 조직이 추구해야 할 가치와 임무를 말한다.

② 인적 자원(People)
- 조직 설계와 전략을 누가 수행할 것인가의 고민을 해결해야 하는 것이 인적자원이다. 그리고 인적 자원은 가치, 행동 양식, 편견과 같은 독특한 특성을 가지고 있음을 상기해야 한다.

③ 프로세스(Process)
- 프로세스는 6개의 동적연결자를 직접적으로 연결시키는 역할을 하므로 3차원의 피라미드 형태에서도 가장 가운데에 위치한다. 프로세스는 조직의 정책과 전략에 연계

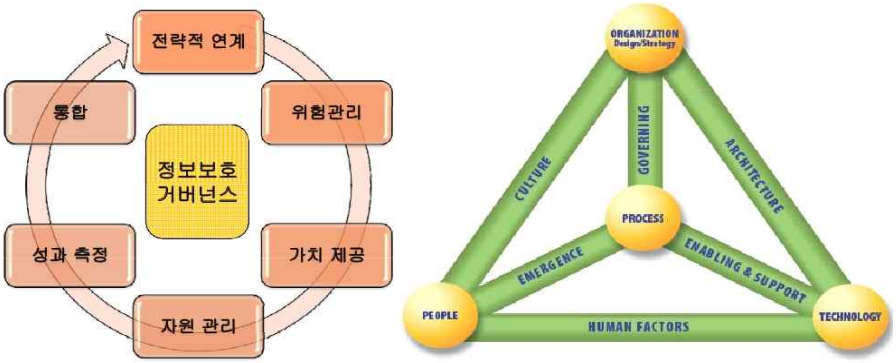

Fig. 4. Information Security Governance and BMIS

되어야 하며 조직의 요구사항에 유연해야 한다. 또한 프로세스는 반드시 측정 가능해야 하며 주기적으로 검토되어야 한다.

④ 기술(Technology)

- 툴이나 응용 프로그램(애플리케이션), 인프라 등으로 구성된 것이 기술이다. 기술의 속성은 동적이므로 위험이 높을 수 있다. 기술을 얼마만큼 신뢰하느냐에 따라 혹은 인적자원이 기술을 잘 사용하지 못하는 미숙함의 사용자에 따라 좌우되는 특성이 있다[7].

3. 클라우드 서비스에 대한 위험관리

본 논문에서는 CSA(Cloud Security Alliance)에서 발간한 “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0” 자료를 중심으로 보안관리 요구사항을 분석한다.

기업에서 클라우드 서비스를 안전하게 사용하려면 비즈니스 연속성을 보장해야 한다. 클라우드 컴퓨팅 12개의 보안영역 중 5개는 관리 도메인으로 7개는 운영 도메인으로 분류하였다[9]. 관리 도메인은 전략과 정책을 다루며, 운영 도메인은 전술적인 보안 고려사항과 아키텍처 상의 구현을 다룬다. 이는 향후 클라우드 컴퓨팅 서비스를 이용하는 기업이 SLA를 작성하고 업무연속성, 가용성 등을 보장하기 위해서이다[8].

본 장에서는 클라우드 서비스에 대한 위험관리를 위해 보안영역을 관리영역과 운영영역으로 구분하여 검토한다. Table 2는 클라우드 컴퓨팅 보안영역 중 관리에 대한 주요 도메인을 나타낸다.

Table 2. Management Area of Cloud Security

영 역	주 요 내 용
Domain1	거버넌스 및 전사적 위험관리
Domain2	법과 전자 증거
Domain3	감사와 준수
Domain4	정보 라이프사이클 관리
Domain5	이식성과 상호운영성

Table 3. Operation Area of Cloud Security

영 역	주 요 내 용
Domain1	전통적 보안, 사업연속성과 재해복구
Domain2	데이터센서 운영
Domain3	사고대응, 공지와 전파
Domain4	응용시스템 보안
Domain5	암호화와 키 관리
Domain6	식별과 접근관리
Domain7	가상화

관리영역에서 거버넌스와 전사적 위험관리는 클라우드 환경에 따른 전사적 위험을 측정하고 관리하는 조직의 능력이다. 아울러 클라우드 서비스에 대한 위험관리를 위해 보안관리 영역을 기반으로 적절한 정책이 수립되어야 하며 그에 따른 가이드라인을 정확히 명시해야 하며 보안 통제사항이 포함되어야 한다.

Table 3은 클라우드 컴퓨팅 보안영역 중 운영에 대한 주요 도메인을 나타낸다.

운영 도메인에서는 클라우드 환경에서 가상화 기술을 사용함에 따른 보안이슈 확인 및 대응방안을 식별해야 한다. 클라우드 서비스를 이용하는 제공자와 이용자는 운영 영역의 가상화를 기반으로 보안 이슈에 대한 대응방안 및 암호화와 키 관리가 이루어져야 한다. 한편, 운영 도메인의 전통적 보안, 사업연속성과 재해복구 도메인은 클라우드 환경에서 보안, 사업연속성, 재해복구를 구현하기 위해 사용하는 운영 프로세스와 절차의 확인이다[9].

CSA가 발표한 클라우드 보안의 운영 영역에서 사고대응, 고지와 전파 영역은 사고가 발생하였을 때, 신속한 대응이 있어야 추후에 발생할 수 있는 위험을 최소화시킬 수 있다. 이것은 BMIS 기반 순환 프로세스에서의 위험 대응과 위험 평가와 연결된다. 또한 식별과 접근관리는 어떤 프로젝트나 파트너십의 관계가 종료되었을 때 그 파트너는 회사 데이터의 액세스 허용이 금지되어야 한다. 하지만 권한이 그대로 이거나 추후에 다시 액세스하려 할 때 거부 없이 접근할 수 있다. 이것은 분명한 취약성으로 생각할 수 있으며 위험 거버넌스와 연결될 수 있다. 이와 같이 클라우드 보안 요구사

항과 BMIS의 순환 프로세스에서 연결하는 위험 거버넌스(RG)와 위험 평가(RE) 부분의 연계성을 충족할 수 있다. 특히, CSA 보안 요구사항에 따르면 거버넌스 측면과 운영 측면 중의 위험관리가 필수적인 요소로 부각되고 있다. 또한, 위험관리는 클라우드와 밀접한 관계가 있으며 이는 본 논문에서 제안하는 BMIS 기반 순환 프로세스와의 연관성을 갖게 된다.

4. 위험 거버넌스 프로세스

4.1 BMIS와 COBIT의 시너지

정보보호 활동에 대한 지시와 통제 행위를 포함하는 정보보호 거버넌스를 실행하기 위해서는 정보보호 체계를 단일화 된 관점에서 확인할 수 있는 청사진이 필요하다[10].

전사적 정보보호 아키텍처는 기업의 정보보호에 대한 청사진을 제공하여, 비즈니스와의 연계성, 정보보호 기능 및 조직들 간의 관계, 정보보호 기술 간의 연계성 등을 보장하므로 거버넌스 도구로서 활용 가능하다. 또한 EA (Enterprise Architecture)와의 관계를 제시하여 IT 영역과의 거버넌스 활동 간 교류에도 활용 가능하다[11].

또한, ERM은 전사적 위험관리와 정보보호 활동에 대한 위험을 측정하고 통제하는 것이 핵심으로서 ERM 아키텍처 설계의 기본 개념은 BMIS와 COBIT의 시너지를 통해 정보보호 거버넌스 실행 체계를 정의한다(Fig. 5).

BMIS의 4가지의 요소와 6가지의 역동 연결자는 COBIT과 연계 시너지가 높다. 예를 들어서 BMIS의 PEOPLE인 요소와 COBIT의 인력은 서로 연결되어 있는 것을 볼 수 있으며 Architecture는 활동과, ORGANIZATION과

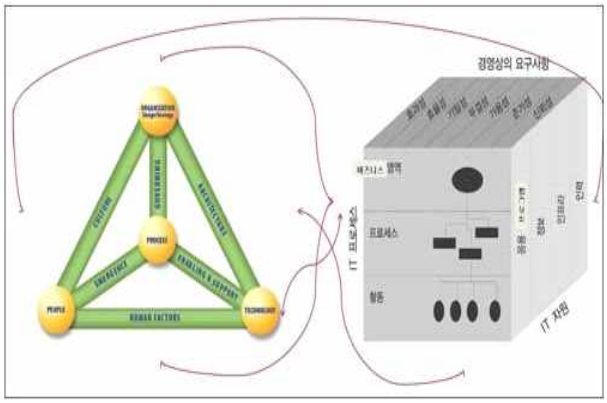

Fig. 5. Synergy of BMIS and COBIT[12]

HUMAN FACTORS는 비즈니스 영역과 연계되어 있는 것을 볼 수 있다.

이와 같이 본 논문에서는 비즈니스 지원(효과성, 효율성, 기밀성, 무결성, 가용성, 신뢰성, 준거성 등의 경영상의 요구사항)을 위해 COSO ERM, COBIT Risk IT Framework, BMIS를 검토하여 상호 연결된 모델을 제시한다.

4.2 위험 거버넌스 실행 체계

본 논문에서는 위험관리 상호작용 모델의 제안을 통해 위험 거버넌스 실행체계를 정립한다. 즉, BMIS의 4개의 요소 중 핵심요소인 프로세스의 순환 측면에서 COSO ERM Framework, COBIT Cube 및 Risk IT Framework와의 상호작용을 통해 위험 거버넌스의 실행체계를 정립한다(Fig. 6).

기존 BMIS 기반 프로세스 순환부분과 COBIT의 프로세스 부분은 상호연관성을 갖고 있으며 COBIT의 IT 프로

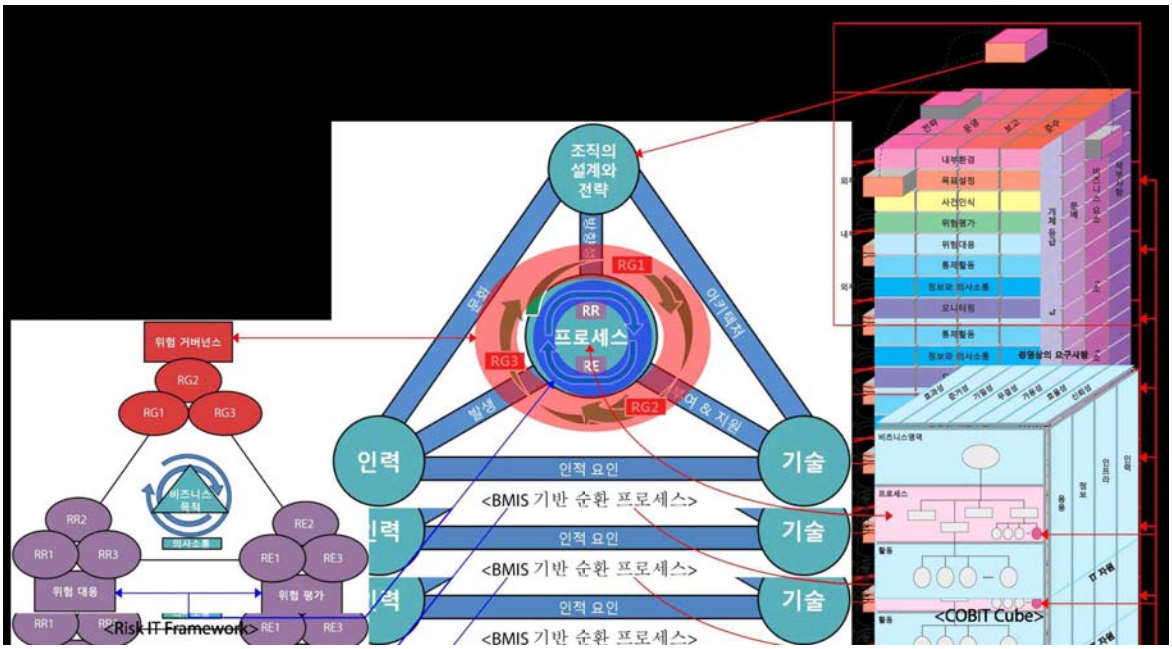

Fig. 6. Risk Management Interaction Model

세스는 4개의 도메인과 34개의 프로세스 중 위험과 관련된 프로세스 범위를 COSO ERM Framework와 상호연결시킬 수 있다.

예를 들면, COSO ERM Framework의 전략과 목표설정, 비즈니스 요소의 매핑 부분은 BMIS의 조직의 설계와 전략과 연결된다. 그리고 모니터링, 보고, 비즈니스 요소의 매핑 부분은 BMIS의 인력과 연결된다. 또한, 정보와 의사소통과 운영, 세부사항의 매핑 부분은 BMIS의 인력과 연결된다.

한편, COSO ERM Framework의 내부측면과 외부측면의 구성요소는 Risk IT와 상호작용하는데, 위험평가와 위험대응은 내부측면, 나머지 6가지의 구성요소는 외부측면과 상호작용될 수 있다.

Risk IT Framework에서 위험 거버넌스 RG1, RG2, RG3 부분은 BMIS의 순환 프로세스에서의 외부 구성요소로 순환되며 내부측면인 위험대응과 위험평가는 BMIS의 내부 구성요소로 순환된다.

기존 BMIS의 프로세스에서 변형된 BMIS 기반의 순환 프로세스는 위험 관리가 추가되면서 내·외부적으로 순환하여 효과적이고 전략적인 비즈니스 모델이 된다. 또한, 내부와 외부 구성요소의 분류는 위험 대응 및 평가가 전제로 되면서 위험 거버넌스 실행체계가 이루어지기 때문에 내부적인 RR, RE 프로세스 순환이 이루어지면서 위험 거버넌스 실행체계가 구축된다.

5. 결 론

본 논문에서는 클라우드 컴퓨팅을 위험 관리의 도구로서 거버넌스와 운영영역으로 나누어 검토하였으며 기업 IT 거버넌스 실행체계 정립을 위한 위험관리 상호작용 모델을 제안하였다. 제안 모델은 기존 BMIS의 프로세스 부분에 순환구조를 적용시킴으로써 위험관리의 체계적인 통제가 가능한 특성을 갖는다. 향후 연구과제로서 클라우드 컴퓨팅을 위험관리의 도구로서 검토하여 서비스 수준(SLA)을 향상시킴으로써 비즈니스 지원을 위한 경영상의 요구사항 도출과 이에 따른 위험 거버넌스 실행체계 구축에 대해 연구 예정이다.

참 고 문 헌

[1] P. Mell, T. Grance, “the Definition of Cloud Computing”, *Nist*, pp.23, 2009.

[2] H.Kim, H.Jung, Y.Won, “Mobile Cloud Security Issue and Technology Requirement”, Korea Information Processing Society Review, Vol.18, No.5, pp.37-44, 2011, 9.

[3] M. S. Richard, E.A. E. Miles, J. M. Frank and E. N. Lucy, “COSO, Enterprise Risk Management-Integrated Framework”, *COSO*, Internal Report, 2004, 9.

[4] ISACA, “The Risk IT Framework”, *ISACA*, Exposure Draft, 2009, 12.

[5] H.Choi, “IT Governance Framework 3. Risk IT Framework”, Korea Microsoftware, No.2, 2010, 2.

[6] K.Oh, “IT Governance Framework 1. COBIT Framework”, Korea Microsoftware, No.2, 2010, 2.

[7] H.Cho, “Information Security Governance Strategy V.3.0”, *ISACA*, 40th Concert Seminar, 2011, 5.

[8] J.Park, D.Lim, “Risk Management Countermeasure in Cloud Computing Environment”, Review of KIISC, pp.224-228, 2011, 12.

[9] CSA, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0”, *Cloud Service Alliance*, 2011.

[10] J.Kim, “Starting Standardization of Information Security Governance Framework in International Standardization Organization”, TTA, ICT Standard Weekly, 2009, 5.

[11] S.Lee, K.Hwang, “Study on Information Security Governance Framework Development”, Korea Database Society, Journal of Information Technology Applications & Management, Vol.18, No.2, July, pp.91-108, 2011.

[12] H.Cho, “Information Security Governance and BMIS-Overview”, Security News(http://www.boannews.com/media/view.asp?idx=27203), 2011, 8.

송 유 진

e-mail : song@dongguk.ac.kr

1982년 한국항공대학교(학사)

1987년 경북대학교(석사)

1995년 일본 Tokyo Institute of Technology (박사)

1988년~1996년 한국전자통신연구원 선임연구원

2003년~2005년 미국 University of North Carolina at Charlotte 연구교수

2006년~2006년 일본 정보보호대학원대학 객원교수

2005년~2012년 동국대학교 부설 전자상거래연구소장

1996년~현 재 동국대학교 정보경영학과 교수

1998년~현 재 한국정보보호학회 부회장(영남지부장)

2006년~현 재 국제 e-비즈니스학회 이사

2006년~현 재 한국사이버테러정보전학회 이사

2001년 ICISC2001 운영위원장

2003년 하계CISC2003 프로그램위원장

2006년 CISC-S2006 공동프로그램위원장

2007년 한국정보시스템학회 추계학술발표대회 공동조직위원장

관심분야 : Privacy Protection, Secret Sharing, 클라우드 보안 및 응용, Context Aware Security, 정보보호 거버넌스