정보보안 거버넌스 프레임워크에 관한 연구*

김민준** · 김귀남***

요 약

시대의 흐름에 따라 기업의 지속적인 비지니스 연계 보증을 위하여 IT의 비중이 높아지면서, IT가 조직의 하나의 부분으로서 작용하는 것이 아닌 전사적인 차원에서 정보화 사회의 경쟁 화두로서 인식되어가고 있다. 정보보안 거버넌스는 정보의 무결성, 서비스 연속성, 정보자산의 보호라는 3가지 목적으로 시작된다. 이는 기업 거버넌스에 필수적이며 투명한 부분이 되어야 하고, IT프레임워크와 연계되어야 한다. 기존의 정보보안 거버넌스 프레임워크는 그 범위가 넓어 소규모 기업 거버넌스와 이해관계를 가지지 못한 문제점이 있다. 따라서 본 논문은 단순화된 정보보안 거버넌스 프레임워크를 제안하여, 문제점을 해결하고, 제안하는 프레임워크의 안전성 분석과 효율성 분석을 통하여 제안 방법의 효율성에 관하여 알아보았다.

A Study on Information Security Governance Framework

Min Jun Kim** · Kuinam J. Kim***

ABSTRACT

The flow of time, depending on the company's ongoing business link to guarantee the proportion of much greater importance, it in the organization as part of an enterprise-wide level, rather than acting on the information society has been considered as the topic of race. Information Security Governance, the integrity of the information, service continuity, the three kinds of information asset protection purpose begins. It is essential for corporate governance, transparency should be part, must be aligned with the IT framework. Existing information security governance framework that small businesses a wide range of governance issues and interests have never had. Therefore, we simplified the information security governance framework is proposed, and solve problems, and propose a framework for analysis of the safety and efficiency through the analysis of the effectiveness of the proposed method were discussed.

Key words : Information Security, Governance, Framework

접수일 : 2010년 9월 28일; 채택일 : 2010년 12월 3일

* 본 과제는 경기도 기술개발사업의 사업비지원(과제번호A10101110)에 의해 수행되었습니다.

** 경기대학교 산업보안학과

*** 교신저자, 경기대학교 산업보안학과

1. 서 론

시대의 흐름에 따라 기업의 지속적인 비지니스 연계 보증을 위하여 IT의 비중이 높아지면서, IT가 조직의 하나의 부분으로서 작용하는 것이 아닌 전사적인 차원에서 정보화 사회의 경쟁 화두로서 인식되어가고 있다. 그로 인해 기업 거버넌스의 부분으로 IT 거버넌스가 도래하게 되었고, 이에 대한 많은 연구가 진행되어 왔다[1].

Earl[2]은 전략정보시스템 연구에서 IT 계획수립에 포함될 요소를 비즈니스 목표에 부합하는 정보시스템에 대한 연계된 투자, 경쟁우위를 위한 IT의 이용, IT자원의 효율적이고 효과적 관리에 대한 방향제시, 기술정책과 구조 개발과 같은 4가지 영역으로 분류하였으며, Van Gembergen[3]은 전략적 연계, IT를 통한 비즈니스 가치의 전달, 위험관리, 성과관리의 네 가지 요소들을 IT 거버넌스의 목적으로 정의하였다.

이와 같이, IT를 이용한 기업의 활동들이 상당한 노력에 의한 전략적 연계를 통해서 다루어져야 함에도 불구하고 해당 의사결정이 IT부서나 현장 사용자에 의해 수행하여야 할 역할로 인식되고 있다[4]. 또한 Carr(2003)은 IT가 기업 활동에 없어서는 안 될 필수 요소로 주장함에 있어, 필수 요소로 자리매김 했지만, IT의 전략적 가치는 예전에 비해 낮아지고 있으며, 기업은 IT에 대해 소극적이고 방어적인 투자를 제안하고 있어 논란이 되고 있다.

Bannister and Remenyi[5]는 IT가 기업 경쟁력의 점진적 증가에 기여하고 있으며, 기업 활동의 기초이자 생존의 필수 요소이고, 변화와 혁신의 플랫폼이기 때문에 IT는 전략적으로 여전히 중요한 가치를 지니고 있다고 주장했다. 계속되는 경제 악제로 인해, 기업들은 IT 투자에 대한 직접적으로 보여 질 수 있는 성과를 요구하고 있다[6].

국내 대기업들은 IT 거버넌스에 관심을 가지고 IT조직체계 및 IT 관련 의사결정 체계와 과정을 가지기 시작했지만 여전히 중소기업의 경우는 IT 거버넌스에 대하여 소극적인 입장을 가지고 있다. 본 연구에서는, 정보보안 거버넌스의 필요성을 조사 및 분석하고, 중소기업을 위한 정보보안 거버넌스 프레임워크를 제안할 것이다. 급변하고 불확실해지는 상황 속에서 효과적이고 체계적인 정보보안 거버넌스 프레임워크 구축을 통해, IT의 전략적 가치를 극대화하여 근간에는 시장의 경쟁력에 기여할 수 있다.

본 제안 방법을 설명하기 위해서 본 논문의 구성은 다음과 같다. 제 2장에서는 IT 거버넌스와 정보보안거버넌스 관련 연구에 대해서 설명하고, 제 3장에서는 본 논문에서 제안하는 정보보안 거버넌스 프레임워크에 대해서 설명을 한다. 제 4장에서는 본 논문에 제안하는 방법의 안정성과 효율성을 알아보고, 제 5장에서 결론을 맺는다.

2. 관련 연구

2.1 IT 거버넌스

IT 거버넌스란 기업 지배에 통합된 부분이며, 조직의 IT가 조직의 전략과 목적을 지원하고 확장하는 것을 보증하기 위한 리더십, 조직구조 및 프로세스로 구성되어 있다[7]. IT 거버넌스의 가장 대표적인 선두주자는 ISACA(Information Systems Audit and Control Association)로 알려진 협회이며, 대표적인 모델로는 (그림 1)의 Cobit(Control OBjectives for Information and realted Technology)으로 IT 거버넌스를 실현하기 위해 업계표준과 Best Practice에 바탕을 둔 통제 프레임워크이다[8].

IT거버넌스의 취지(Purpose)는 IT노력(Endeavors)을 지휘하고, IT 성과가 기업과 IT를 연계시키고 약속한 효익을 실현한다는 전략적 연계(Strategic Alignment)와 성과측정(Performance Mea-

surement), 기회를 이용하고 이익을 극대화할 수 있도록 IT를 사용한다는 가치제공(Value Delivery), IT자원을 책임감 있게 사용하는 자원관리(Resource Management), IT관련 위험을 적절히 관리하는 위험관리(Risk Management)에 있다[10].

(그림 1) COBIT 모델[9]

기업의 IT의존성은 IT를 고려하지 않고서는 기업 지배 문제를 해결할 수 없게 만들어졌다. IT는 기업의 전략적 활동에 영향을 주며 전략 계획을 수립할 때도 중요한 요소로 작용하고 있다. 또한 IT지배는 기업지배에 통합되어야 하며 IT 거버넌스가 기업지배의 통합적 일부가 됨에 따라, IT 거버넌스는 최고 경영진, 이사회의 책임사항이 되었다[11].

이와 같이 IT 거버넌스는 조직 내 바람직한 IT 사용을 유도하기 위한 의사결정의 책임과 권한을 정립하는 체계이며, 이러한 의사결정이 올바르게 구현될 수 있도록 하는 개념이라 할 수 있다. IT 거버넌스는 정책적으로 기업지배의 전략과 목표달성에 맞추어 IT의 전략적 가치를 극대화하는데 기여해야 하며, 이는 기업의 시장 경쟁력 강화에 기여하게 될 것이다[12].

2.2 정보보안 거버넌스

정보보안 거버넌스는 정보의 무결성, 서비스 연속성, 정보자산의 보호라는 3가지 목적으로 시작된다. 이는 기업 거버넌스에 필수적이며 투명한 부분이 되어야 하고, IT프레임워크와 연계되어야 한다. 정보보안 거버넌스는 정보를 보호하는 리더쉽, 조직 구조 그리고 프로세스들로 구성되며, 정보의 수명주기에 걸쳐 정보의 보호, 기밀성, 무결성 그리고 가용성과 조직내 정보의 사용을 다룬다[13].

정보보안 거버넌스는 기업 거버넌스의 부분집합으로서 전략적 방향을 제시하며, 목적 달성, 적절한 위험관리, 조직자산의 책임있는 사용, 기업보안 프로그램의 성공과 실패가 모니터링 됨을 보장한다[14].

정보보안 거버넌스는 조직의 목적을 지원하기 위한 정보보안과 사업전략 연계, 조직의 목적을 지원함에 있어서 최적화된 정보보안투자, 정보보안 지식과 인프라스트럭처를 효율적이고 효과적으로 이용, 정보자산에 대한 위험 관리/완화, 잠재적 영향을 용인 가능한 레벨로 감소시키기 위한 적절한 측정, SMART(Specific, Measurable, Achievable, Relevant, Time-bound)한 목표가 달성됨을 보장하는 정보보안 프로세스 측정, 모니터링과 보고 외에도 프로세스 통합, 보증이라는 부분을 가진다. 이는 보안을 위한 조직 내 관리 보증 프로세스들의 통합으로 산재한 보안관련 활동을 통합 관리한다는 의미를 가진다[14].

이와 같이 정보보안 거버넌스는 기업의 한 부분이며, IT 거버넌스와 같은 맥락에서 구분된다. 정보보안이 포화상태에 치닫고 있는 현시점에서, 여전히 기업기밀 유출사고는 보이지 않는 곳에서 일어나고 있다. 이는 정보보안 거버넌스를 통해 전사적 차원의 관리가 시급하다. 기업이 용인하는 보안 비용에 비해 위험 비용이 월등히 높은 정보보안은 아직도 기업의 경영진들은 소극적으로 대

처하고 있다. 이에 정보보안 거버넌스 프레임워크를 통해 대기업이 아닌 수많은 중소기업의 정보보안에 기여할 수 있다. 또한 이는 기업의 시장경쟁력 강화에 기여하게 된다.

3. 제안방법

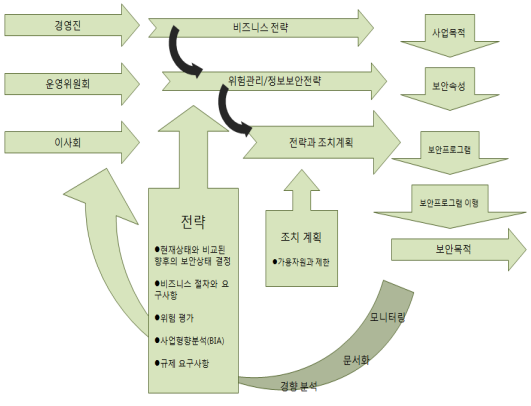
본 제안하는 정보보안 거버넌스 프레임워크는 기존의 대기업을 위해 ISACA에서 공개한 Information Security Governance Conceptual Framework에 착안하여 개발하였다[14]. 중소기업의 경우 개발팀, 운영팀, 경영진으로 구성되어 있기 때문에 역할의 따른 승인절차가 제대로 이루어지지 않으며, 기존 프레임워크와 상충되지 못하는 문제점이 있었다. 또한 의사결정이 규모의 다양성, 산업 및 지역차이와 같은 상황요인으로 기업의 전략목표와 다르게 진행되었으며 보완할 정보보안 거버넌스 프레임워크도 존재하지 않았다.

3.1 비즈니스 전략과 정보보안 거버넌스

기업의 비즈니스 전략은 연계를 촉진하기 위하여 위험관리와 정보보안 전략으로 입력의 하나가 된다. 이는 경영진의 판단으로 결정하며, 위험관리와 정보보안전략은 운영위원회에서 결정하여 보안속성을 정하게 된다. 하지만 소규모 기업의 경우는 운영위원회를 따로 구성하기엔 기업의 목적에 적합하게 경영될 수 없으며, 보안과 관련된 모든 사항은 보안팀에서 관리하게 된다. 이에 위험관리, 정보보안전략, 보안전략, 조치계획은 보안팀에서 담당처리하게 된다.

(그림 1)은 기존의 정보보안 거버넌스 프레임워크를 나타낸 것으로 전략적 연계의 범주에서 위험관리와 정보보안 전략이 운영위원회로 위임된 것을 확인할 수 있다. 또한 전략에서 볼 수 있듯이 입력의 균형은 기존 또는 현재 상태와 비교된 향후의 보안상태 결정에 기초하게 된다.

(그림 2)는 제안하는 정보보안 거버넌스 프레임워크이며, 제한적인 인원의 관리를 위하여 운영팀장에 의해서 비즈니스 전략과 사업목적을 나타내며 이는 위험관리와 정보보안전략 뿐만 하니라 구체적 전략과 조치계획도 포함하게 된다.

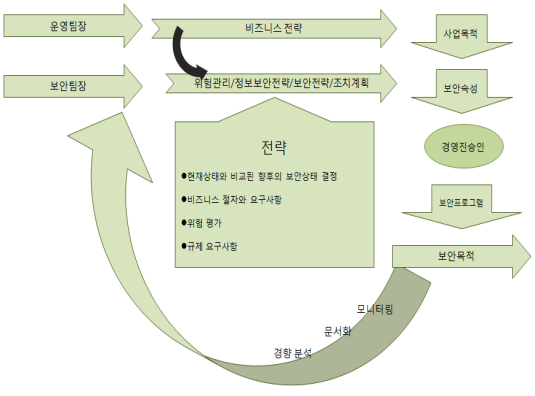


(그림 1) 기존의 정보보안 프레임워크[14]

3.2 승인절차와 정보보안 거버넌스

본 논문에서 제안하는 정보보안 거버넌스 프레임워크는 소규모 기업에 맞게 승인 절차를 제안한다. 기존의 정보보안 프레임워크는 (그림 1)에서와 같이 경영진, 운영위원회, 이사회를 통한 종합적인 승인절차를 요구하며, 빠른 의사 결정에 어려움이 있다. 이는 절차 상 이해관계에서 반복되는 요구사항 정의 및 단계말 검토를 거치게 되어 거버넌스 비용증대와 정보보안의 적합한 시기의 대응에 어려움을 앉고 있다. 이에 재안하는 프레임워크(그림 2)에서는 보안속성에 위험관리, 정보보안전략, 조치계획을 통합하여 한 번의 승인으로 업무 순환이 가능하게 된다. 거대 기업의 경우 변화가 다양하기 때문에 가용자원과 제한에 의한 조치계획의 변화가 빈번하게 발생할 수 있지만, 중소기업의 경우는 보통 하나 혹은 두개의 서버와 단순한 문서화 정책으로 이루어져 있기 때문에 조치 계획의

구성을 제거하며, 변화에 가장 잘 대응 할 수 있는 보안팀에서 계획하게 된다.



(그림 2) 제안하는 정보보안 프레임워크

3.3 보안목적 변화의 보고 체계

기존의 프레임워크는 가장 높은 이사회에서 모든 사항의 분석 결과를 성과측정의 일면으로 BSC (Balanced Scorecard)[15]를 통해서 의사결정을 하게 된다. 이는 자산 평가 방법으로, 재무성과에 미래의 경쟁력 향상을 위한 지표로 고객, 내부 프로세스, 학습 등을 추가하여 균형 있게 평가하는 모델이다. 또한 사업영향분석(Balanced Impact Analysis)를 통해서 보안 전략을 명시하게 된다. 하지만 소규모 기업의 경우 사업 영향이 직접적으로 보여지기 때문에, 이를 제외하며, 성과 측정을 실무진인 보안팀에서 완료하고 모든 사항을 경영진에게 승인 받도록 한다.

4. 제안 프레임워크 효율성 연구

본 논문이 제안하는 정보보안 거버넌스 프레임워크의 효율성 분석을 위하여, 정보보안 거버넌스의 효익과 필수 구성요소 관점에서 분석한다.

4.1 정보보안 거버넌스의 효율성 연구

정보보안 거버넌스는 고객과의 관계에서의 신뢰성을 향상시키며, 조직의 명성 보호와 프라이버시 침해 가능성 감소의 기능을 갖는다. 또한 정보보안 거버넌스의 목적은 기업 거버넌스와 연계하여 더 적은 비용으로 기업의 보안이 향상될 것이라는 보증을 토대로 한다. 이는 기존의 프레임워크보다 진화된 모델로, 기업의 위험 감내의 범위를 벗어나지 않았으며, 용인 가능한 위험 수준을 유지하도록 하였다. 또한 정보보안 프레임워크에 개발팀을 분리하여 직무 분리를 통한 기업의 지속적인 존속 가능성을 높일 수 있다.

4.2 정보보안 거버넌스의 안정성 연구

본 제안하는 프레임 워크는 기존의 여러 단계에 걸쳐서 일어나는 승인 절차를 실제 보안 프로그램이 시작되기 직전의 단일 승인을 통해서 유지하였다. 기업의 계속적인 존속 여부는 경영진이 책임지게 되며, 이는 기업의 안전성을 가져올 수 있다. 이는 높은 집권형, 높은 분권형, 중간점, 집권적, 분권적, 결합적 구조와 같은 여러 가지 거버넌스 구조[1]를 하나의 거버넌스로 강제하여 IT의 개발, 운영, 관리 뿐만 아니라 보안 업무도 안정적으로 운영될 수 있다.

5. 결 론

본 논문은 소규모 기업을 위한 정보보안 거버넌스 프레임워크에 관한 연구로써 기존의 프레임워크의 복잡한 구조를 중소기업에 맞게 변화하였으며, 기존의 목적을 유지한 상태에서 비즈니스 전략과의 연계, 성과측정과 승인, 그에 따른 보고 체계의 기준에서 살펴보았다.

본 논문에서는 단순화된 프레임 워크를 통해서 효율성을 극대화 하여 소규모 기업의 거버넌스와 이해 상충되도록 효과적으로 개선하였으며, 안정성을 유지하는 방안을 모색하였다.

향후 본 논문이 제안하는 방법을 통하여 소규모 기업의 정보보안 거버넌스 구조를 변경 및 유지해 보고 변화된 기업과 기존의 기업을 비교 분석하여 그 효율성과 안전성을 입증하는 것이 필요하다.

참 고 문 헌

[1] Kimon Sung, "A study on IT Governance of small and medium sized enterproses in korea : with multiple contingencies perspective", 2008.

[2] J. G. Rockart, "The Line Takes the Leadership-IS Management in a Wired Society", Sloan Management Review, pp. 57-64, Summer, 1998.

[3] M. H. Olson and N. L. Chervany, "The Relationship Between Organizational Characteristics and the Structure of the Information Services Function", MIS Quarterly, Vol. 2, pp. 57-68.

[4] W. Van Grembergen, S. De Haes, and E. Guldentops, "Structures, Processes and Relational Mechanisms for IT Governance, in Strategies for Information Technology Governance", Idea Group, pp. 1-36, 2004.

[5] Bobbister, F. and Remenyi, D., "Why IT Continues to Matter : Reflections on the Strategic Value of IT", Electronics Journal of Information Systems Evaluation, Vol. 8, No. 3, pp. 159-168, 2005.

[6] H. Zo, C. Song, H. kang, and D. Lim, "IT Governance of the Korean Conglomerates: A Comparative Case Study", June, 2009.

[7] IT 거버넌스, Wim Van Grembergen, 안중호, 서한준 옮김, 네모, 2005.

[8] Cobit 4.1(www.isaca.org).

[9] ISACA Serving IT Governance Professionals Transforming EnterprIse IT(www.isaca.org/knowledge-Center/cobit/).

[10] J. Lee, "IT Governance Mediated the Effect of Human Resource Capability on Information Systems Outsourcing Success", 2009.

[11] 이자영, 이정훈, "국내서비스 업체의 IT지배구조 의사결정체계 분석에 관한 사례연구 : 'A', 'B'사 비교분석", 한국IT서비스학회지, 제5권, 제2호, pp. 93-105, 2006.

[12] 이창진, 이정훈, 장덕화, "IT지배구조 기반의 IT전략 및 운영관리 : 문헌연구와 미래연구 방향", 한국경영정보학회 2006 춘계학술대회 논문집, pp. 853-863, 2006.

[13] CobiT_Security_Baseline_2ndEd(www.isaca.org).

[14] Information Security Governance : Guidance for Information Secrity Managers(www.isaca.org).

[15] S. Kang, A Study on the application of Balanced Scorecard in Small Business: A case of development of a Human Resource Evaluation System.

김 커 남

미국 캔자스대학(학사)
미국 콜로라도주립대학(석사)
미국 콜로라도주립대학(박사)
현재 경기대학교 산업보안학과
교수

김 민 준

경기대학교 산업보안학과
2010년 안양대학교 전기전자공학과
현재 경기대학교 산업보안학과
석사과정