최고경영자를 위한 기업 정보보호 거버넌스 모델에 대한 연구

김 도 형*

요 약

기존의 기업 정보보호 활동은 정보보호 조직 중심이 이었으며, 최고경영자는 정보보호와 기업경영은 별개의 것이라고 생각한다. 하지만 각종 보안사고가 끊임없이 발생하고 있으며, 이에 대응하기 위해서는 정보보호 조직만의 활동이 아니라 기업경영 측면에서의 정보보호 활동이 필요하다. 본 연구에서는 기존에 제시된 기업 거버넌스 및 IT거버넌스 등을 살펴보고 기업의 정보보호 활동에 기업의 비즈니스 목표와 경영진의 목표를 반영할 수 있는 정보보호 거버넌스 모델을 제시하고자 한다. 본 논문에서 제시하는 정보보호 거버넌스 모델은 계획 단계에서부터 최고경영자의 참여를 유도하여 정보보호 목표를 수립한다. 정보보호 목표에 따라 정보보호 계획 수립, 정보보호체계를 구축 및 운영하고, 컴플라이언스 감사, 취약점 분석 및 리스크 관리 등을 통해 그 결과를 최고경영자에게 보고함으로써 기업의 정보보호 활동을 강화할 수 있다.

The Study on Corporate Information Security Governance Model for CEO

Kim Do Hyeong*

ABSTRACT

The existing enterprise information security activities were centered on the information security organization, and the top management considers information security and enterprise management to be separate. However, various kinds of security incidents are constantly occurring. In order to cope with such incidents, it is necessary to protect information in terms of business management, not just information security organization. In this study, we examine the existing corporate governance and IT governance, and present an information security governance model that can reflect the business goals of the enterprise and the goals of the management. The information security governance model proposed in this paper induces the participation of top management from the planning stage and establishes information security goals. We can strengthen information security activities by establishing an information security plan, establishing and operating an information security system, and reporting the results to top management through compliance audit, vulnerability analysis and risk management.

Key words : Information Security Governance(정보보호 거버넌스), Information Security Management(정보보호관리체계), Security Management(보안관리)

접수일(2017년 3월 4일), 수정일(1차: 2017년 3월 30일), 게재확정일(2017년 3월 31일)

* (주)대구은행 정보보호부

1. 서 론

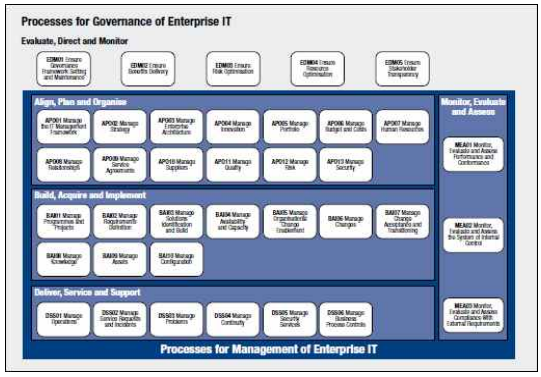
기업들은 정보기술의 발전과 더불어 정보자산을 보호하기 위해 다양한 정보보호시스템 구축과 정보보호관리체계를 마련하고 있다. 하지만 최근 발생한 3.20 사이버테러, KT 고객정보 유출, 카드사 고객정보 유출, 한수원 해킹 사태, 2016년 국방부 해킹 사태 등 다양한 보안사고가 지속으로 발생하고 있다. 또한 계속적인 보안사고 발생에 대응하기 위해 국가적인 차원에서 법률도 강화되고 있어 기업의 정보보호 활동이 더욱 어려워지고 있다. 하지만 최고경영자(CEO)는 정보보호를 정보보호 조직만의 업무로 대부분 생각하고 있다. 정보보호 강화를 위해서는 최고경영자(CEO)가 정보보호의 중요성을 인식하고 정보보호 활동에 대한 의지가 중요하다.

본 연구에서는 최고경영자(CEO)가 비즈니스 목표에 따라 정보보호 목표를 수립하고 정보보호 활동에 적극 참여 할 수 있는 정보보호 거버넌스 모델을 제시하고자 한다. 제2장 관련연구에서는 거버넌스, 기업 거버넌스, IT 거버넌스, 정보보안 거버넌스, 정보보호관리체계 등을 살펴보고, 제3장에서는 최고경영자를 위한 기업 정보보안 거버넌스 모델을 제시한다. 제4장에서는 본 모델의 효과성을 분석하고, 제5장에서는 결론을 맺는다.

2. 관련연구

2.1 거버넌스

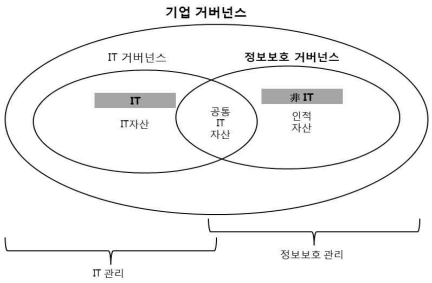
거버넌스란 사전적인 의미로 통치, 관리, 통치 방식을 의미한다. 거버넌스 개념의 핵심요소인 개념요건으로는 책임성, 관리와의 구분, 조직통제 등이 있으며, 실행요건으로는 의사결정권한, 지시, 성과모니터링이 있다[1]. 기업 거버넌스란 거버넌스의 개념을 기업에 적용한 것으로 개념요건으로는 이해관계자가 있으며, 목표요건으로 전략목표 연계, 책임성이 있으며, 실행요건으로 목표달성방법, 성과모니터링, 위험관리, 자원관리가 있다[1]. IT 거버넌스란 조직의 이사회 및 최고경영층이 IT가 효율적이고 효과적이며 책임성 있게 활용될 수 있도록 평가, 지시, 감독하는 체계이다[2]. IT 거버넌스의 대표적은 프레임워크로 Cobit(Control OBject for Information and related Technology)을 예를 들수 있수 있다. Cobit은 ISACA(Information Systems Audit and Control Association)에서 연구하여 IT 거버넌스를 실현하기 위하여 업계표준과 Best Practice에 바탕을 둔 통제 프레임워크이다. 현재 Cobit 5.0 버전까지 출시 되었으며 주요 프로세스는 다음(그림1)과 같다. 평가/지시/모니터링(EDM: Evaluate, Direct and Monitor), 연계/계획수립/조직화(APO: Align, Plan and Organize), 개발/도입/구축(BAI: Build, Acquire and Implement), 운영/서비스/지원(DSS: Deliver, Service and Support), 모니터링/평가/감사(MEA: Monitor, Evaluate and Assess) 그리고 Cobit 5.0에서 새로 추가된 거버넌스 관리 영역으로 평가/지시/모니터링(EDM: Evaluate, Direct and Monitor) 5가지 도메인이 유기적으로 연계되어 운영된다[3][4].



(그림 1) Cobit 5.0 Process Reference Model

정보보호 거버넌스란 위험관리 노력의 일환으로, 정보보호 전략이 비즈니스 목표와 연계되고 이의 달성을 지원하며, 정책과 내부통제를 통해 관련 법규와 규정을 준수하는 것을 보장하고, 책임을 할당하기 위한 프레임워크와 이를 위한 경영구조 및 프로세스를 수립하는 과정이다.[1] 정보보호 거버넌스는 정보의 기밀성, 무결성, 가용성이라는 3가지 목적으로 시작된다. 이는 기업 거버넌스에 포함이 되어야 하고 IT거버넌스와도 연계가

되어야 된다.[5] 기업 거버넌스, IT거버넌스, 정보보호 거버넌스의 관계를 살펴보면 아래 (그림2)와 같다.

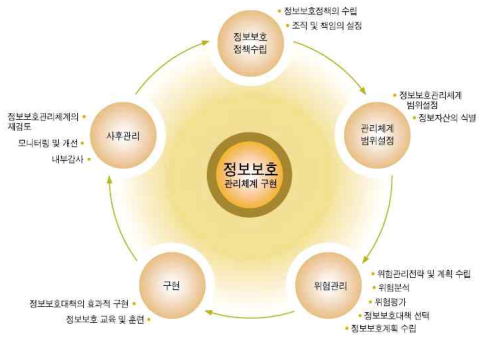


(그림 2) 기업, IT, 정보보호 거버넌스의 관계

첫째, 기업 거버넌스의 틀 안에서 정보보호 거버넌스가 작동되어야 한다. 둘째, 정보보호 거버넌스의 목표를 명시해야 한다. 정보보호 거버넌스는 IT와 비IT를 구분하지 않으므로 IT거버넌스와의 중복 이슈 등이 있으며 이를 해결하기 위해서는 정보보호 거버넌스의 목표를 명확히 해야 한다[1].

2.2 정보보호 관리체계

정보보호관리체계(ISMS: Information Security Management System)란 “정보자산의 무결성, 비밀성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리, 운영하는 체계로” 정의 내리고 있다“[6]. 대표적인 정보보호관리체계 모델에는 ISO27001과 한국인터넷진흥원(KISA) ISMS가 있다. ISO27001은 BS7799로 영국에서 처음으로 제정 되었으며 2005년 국제표준모델인 ISO27001로 개정되었다. ISO27001은 2013년 ISO27001:2013으로 개정되었으며, 114개 통제항목으로 구성되어 있다[7]. KISA ISMS에는 2002년 한국정보보호진흥원에서 국내 사정에 맞게 개발한 정보보호관리체계 인증 제도이다.[6] KISA ISMS 관리과정 요구사항는 크게 5개의 영역으로 구성되어 있다. (그림3)과 같이 정보보호 정책수립 및 범위설정, 경영진 책임 및 조직구성, 위험관리, 정보보호 대책 구현, 사후관리 등으로 구성된다[8].



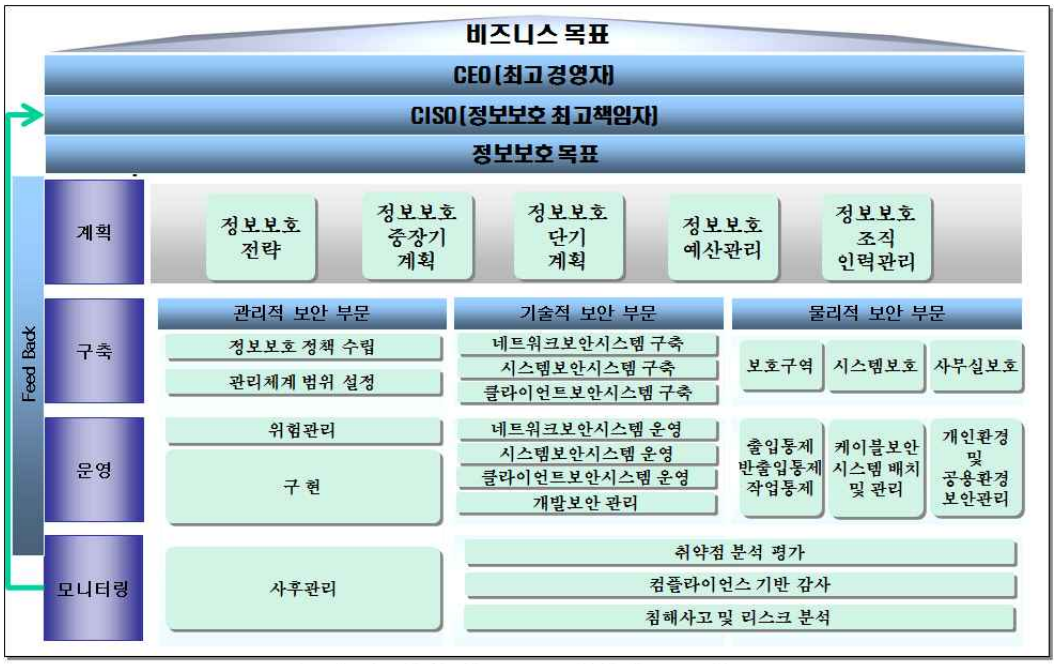
(그림 3) KISA ISMS 관리과정

KISA 정보보호관리체계 인증은 다음<표1>과 같이 관리과정 요구사항 5개 항목, 정보보호대책 통제사항 13개 항목으로 구성되어 있다[9].

<표 1> KISA ISMS 인증 항목

ISMS 인증 관리과정 요구사항
1. 정보보호 정책 수립 및 범위설정
2. 경영진 책임 및 조직구성
3. 위험관리
4. 정보보호 대책 구현
5. 사후관리
ISMS 인증 정보보호대책 통제사항
1. 정보보호 정책
2. 정보보호 조직
3. 외부자 보안
4. 정보자산 분류
5. 정보보호 교육
6. 인적보안
7. 물리적 보안
8. 시스템 개발보안
9. 암호통제
10. 접근통제
11. 운영보안
12. 침해사고관리
13. IT 재해복구

3. 최고경영자를 위한 기업 정보보호 거버넌스 모델



(그림 4) 기업 정보보호 거버넌스 모델

기업 정보보호 거버넌스는 최고경영자(CEO)의 비즈니스 목표에 따라 정보보호 목표를 수립하고 운영되어야 한다. 물리적, 기술적, 관리적 보안이 유기적으로 연동된 융합보안체계를 통해 정보보호 프로세스 운영 및 통제를 하고[10], 지속적 모니터링을 통해 비즈니스 목표에 맞는 정보보호 활동을 수행한다.

지금까지 살펴 본 거버넌스, 기업 거버넌스, IT 거버넌스, 정보보호 거버넌스 및 정보보호관리체계 연구를 바탕으로 최고경영자(CEO)를 위한 기업 정보보호 거버넌스 모델을 제시하고자 한다.

본 논문에서 제시하는 기업 정보보호 거버넌스 모델은 기존의 정보보호 조직 기반으로 이루어지던 정보보호 활동을 최고경영자(CEO)가 바라보는 측면에서 비즈니스 목표에 맞게 정보보호활동을 추진함으로써 기업의 정보보호를 효과적으로 강화할 수 있다. 본 논문에서 제시하는 기업 정보보호 거버넌스 모델은 (그림4)와 같다.

3.1 정보보호 목표

정보보호 목표는 기업 정보보호 활동의 방향성으로 비즈니스 목표를 기반으로 한다. 정보보호의 목표는 기업 비즈니스의 목표를 달성할 수 있도록 기업의 자산을 안전하게 보호해야 한다. 정보보호 활동이 잘 이루어지고 있는지 정보보호최고책임자(CISO)는 모니터링 활동을 통해 점검을 하고, 그 결과를 최고경영자(CEO)에게 보고한다. 정보보호최고책임자(CISO)는 모니터링 활동을 통해 정보보호 목표를 달성할 수 있도록 계획, 구축, 운영 업무를 추진한다.

3.2 계획 단계

계획 단계는 정보보호 목표에 따라 정보호보 활동 추진계획을 수립하는 단계로 정보보호 전략 수립, 정보보호 중장기 계획 수립, 정보보호 단기 계획 수립, 정보보호 예산관리, 정보보호 조직관리가 이에 속한다. 정보보호최고책임자(CISO)는 정보보호 목표에 따라 정보보호 전략을 수립하고, 이에 따른 정보보호 중장기 계획, 단기 계획을 세운다. 그리고, 중장기 및 단

기 계획에 따른 정보보호 예산 수립 및 정보보호 조직 인력 운영방안에 대해 계획을 수립하게 된다.

3.3 구축 단계

구축 단계는 정보보호 계획에 따라 구축하는 단계로 크게 관리적, 기술적, 물리적 보안부문으로 나누어진다. 관리적 보안부문에서는 정보보호 관리체계(ISMS) 관리과정 기준에 따라 정보보호정책 수립 및 범위설정을 한다. 기술적 보안부문은 정보보호관리체계(ISMS)보호대책 통제사항 기준에 따라 정보보안시스템을 구축한다. 기술적 보안부문은 네트워크보안, 시스템보안, 클라이언트보안으로 구분할 수 있으며, 기술적 보안을 적용하기 위한 해당 정보보안시스템을 구축한다. 물리적 보안부문은 정보보호관리체계(ISMS) 보호대책 통제사항 기준에 따라 보호구역 지정, 시스템 보호, 사무실 보호 등으로 범위를 정할 수 있다.

3.4 운영 단계

운영 단계는 구축 후 운영하는 단계로 관리적 보안부문에서는 정보보호관리체계(ISMS) 관리과정 기준에 따라 관리적, 기술적, 물리적 보안 전 분야에 대해 위험관리를 하고, 정보보호대책을 구현한다. 기술적 보안부문에서는 정보보호대책에 따라 네트워크보안시스템, 시스템보안시스템, 클라이언트보안시스템의 정책을 적용하고 운영한다. 추가적으로 개발에 대한 보안관리를 통해 소프트웨어 분석, 설계, 구현, 이관 각 단계별 안전한 소프트웨어 개발이 되도록 운영한다. 물리적 보안부문에서는 지정된 보호구역에 대해서는 물리적 접근통제, 각종 재난에 대한 보호대책, 전산기기 반출입 통제를 하고, 지정된 보호구역내에서 작업시에는 계획된 작업절차에 따라 안전하게 진행할 수 있도록 하며, 시스템에 대해서는 케이블보호, 시스템 배치 등에 대해 검토하여 보호할 수 있도록 운영한다. 사무실에서는 중요문서 및 매체가 노출되지 않도록 하고, 공동환경에서는 중요정보가 노출되지 않도록 보호대책을 수립한다.

3.5 모니터링 단계

모니터링은 사후관리 단계로 정보보호 활동이 잘 이루어지고 있는지 모니터링 하고, 그 결과를 정보보호최고책임자(CISO)에게 피드백(Feed Back)을 하여 정보보호 목표를 수립할 수 있도록 한다. 모니터링은 관리적 보안 사후관리, 취약점 분석 평가, 감사활동, 리스크 분석 활동이 있다. 우선 취약점 분석 평가는 기업 자산에 대해 취약점 여부를 점검하는 활동으로 정보보호관리체계 점검을 하는 관리적 보안부문 취약점 점검과 서버, 네트워크, DB, 웹, 앱 등 기술적 보안부문 취약점 점검 등이 있다. 취약점 분석 평가를 통해 정보보호 운영에 취약한 부문을 도출하고 정보보호최고책임자(CISO)에게 보고함으로써 정보보호 목표에 반영한다. 감사활동에서는 컴플라이언스를 잘 준수하고 있는지 점검함으로써 법적 위반사항이 없는지 검토하고 새로운 법률에 대해 모니터링함으로써 컴플라이언스를 준수할 수 있도록 관리한다. 마지막으로 침해사고 분석 및 리스크 분석에서는 각종 보안사고 사례 및 침해위협을 분석하고 그 결과를 정보보호최고책임자(CISO)에게 보고한다. 정보보호최고책임자(CISO)는 최고경영자(CEO)에게 보고하고 피드백 받음으로써 비즈니스 목표에 맞는 정보보호 목표를 수립할 수 있도록 한다.

4. 제안논문 분석

본 논문에서 제안한 방식은 기존의 정보보호 조직 기반의 활동에 비해 많은 장점을 얻을 수 있다. 기존의 정보보호 활동은 정보보호 조직만의 활동이었으며 최고경영자(CEO)는 정보보호는 비즈니스와 별개의 항목으로 인식하고 있었다면 본 논문에서 제시하는 기업 정보보호 거버넌스 모델은 최고경영자(CEO)는 기업의 정보보호 현황을 직관적으로 인식을 하게 됨으로써 최고경영자(CEO)가 기업경영의 하나로써 정보보호 활동에 적극 참여할 수 있도록 한다. 이를 통해 최고경영자(CEO)는 비즈니스 목표에 맞는 정보보호 목표를 수립하고 운영함으로써 기업 입장에서는 실질적이고 현실적인 정보보호 활동을 수행 할 수 있다. 본 모델을 통해 최고경영자(CEO)는 기업에 맞는 정보보호 전략 및 운영계획을 세울 수 있으며, 비즈니스 목표에 맞는 정보보호 예산수립, 정보보호 인

력을 운영 할 수가 있다.

5. 결 론

본 논문은 기업 최고경영자(CEO)가 비즈니스 목표에 맞는 정보보호 활동을 위한 정보보호 거버넌스 모델에 대한 연구로써 각종 거버넌스 모델과 정보보호 관리체계 분석을 통해 최고경영자(CEO)를 위한 정보보호 거버넌스 모델을 제시하였다. 본 논문에서 제시한 기업 정보보호 거버넌스는 비즈니스 목표에 맞는 정보보호 목표를 세우고 정보보호 활동에 대한 모니터링 및 피드백을 최고경영자에게 전달함으로써 정보보호에 대한 최고경영자(CEO)의 관심을 이끌어 낼 수 있다. 본 논문에서 제안하는 모델에 대해 실질적인 효과를 얻기 위해서는 해당 모델을 시스템화하는 연구가 필요하다. Dash board(대시보드:현황판) 형태의 정보보호 포털사이트를 통해 정보보호목표, 정보보호 운영현황, 모니터링 결과, 정보보호 수준 등을 실시간으로 최고경영자(CEO)에게 보여줌으로써 정보보호 활동을 강화하고 정보보호를 기업경영에 반영할 수 있을 것이다.

참고문헌

[1] 이성일, “정보보호 거버넌스 프레임워크에 관한 연구”, 동국대학교 대학원 경영정보학과, 2011.

[2] ISO/IEC 38500, “Corporate Governance of Information Technology", 2008.

[3] ISACA, “COBIT 5 Framework", 2012.

[4] 조희준, “COBIT 5와 거버넌스 프레임워크”, 한국정보시스템감사통제협회, 2012.

[5] 김귀남, 김민준, “정보보안 거버넌스 프레임워크에 관한 연구”, 융합보안논문지, 제10권, 제4호, pp. 14-19, 2010.

[6] 한국정보보호진흥원, 정보보호관리체계, 2002.

[7] ISO, ISO27001:2013, 2013.

[8] 정대령, “전자정부 정보보호관리체계(G-ISMS)를 활용한 공공기관 정보보호 거버넌스 수립방안에 관한 연구”, 배재대학교 대학원 컴퓨터공학과, 2012.

[9] 한국인터넷진흥원, 정보보호관리체계 인증, 2016.

[10] 이창훈, 하옥현, “기밀유출방지를 위한 융합보안 관리 체계”, 융합보안논문지, 제10권, 제4호, pp. 61-67, 2010.

[저 자 소 개]

김 도 형 (Do-hyeong Kim)

2003년 2월 경기대학교 정보보안전공 공학석사
2008년 8월 경기대학교 정보보호학 이학박사
현재, (주)대구은행 정보보호부 차장

email : pccop@daum.net