情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

COBIT 프레임워크를 활용한 정보보호 성숙도 측정에 관한 연구 – 정보보호 거버넌스 관점을 중심으로 –

조 희 준*, 박 성 갑**, 민 대 환***

요 약

정보보호의 중요성으로 공공기관이나 일반 기업은 정보보호관리체계를 수립, 운영하고 있거나 정보보호 활동을 하고 있다. 하지만 정보보호관리체계나 정보보호 활동에 대한 성과측정이 불명확한 기준을 가지고 있거나 명확한 기준이 없는 것이 현실적인 문제점이다. 이러한 문제점으로 적절한 성과측정이 이루어지지 않기 때문에 현재의 정보보호 수준을 올바르게 측정할 수 없을 뿐만 아니라 그에 따른 성과개선을 하기에도 어려운 실정이다. COBIT 프레임워크의 정보보호 성숙도 모델을 활용하여 정보보호 거버넌스 관점과 연계함으로써 정보보호 성과에 대한 측정지표를 구체적으로 제시하고자 한다. 구체적인 정보보호 성과에 대한 측정지표를 활용함으로써 현재의 정보보호 수준을 파악하고 나아가서 정보보호 수준을 개선하고자 하는데 이 연구의 의미를 두고 있다.

Ⅰ. 서 론

정보자산에 대한 적절한 보호 여부는 조직의 목적달성에 상당한 영향을 끼치는 시대가 되었다. 2009년 7.7. 인터넷 대란, 2011년 5월 현대캐피탈 개인정보 유출, 2013년 3.20. 전산망 대란 등의 정보보호 사고로 인해 공공기관이나 일반 기업의 비즈니스에 막대한 악영향을 초래하는 것은 물론 국가안보의 안전 여부에도 심각한 지장을 불러오게 되었다. 이러한 정보보호에 대한 중요성으로 각 조직은 정보보호에 대한 관리적, 기술적, 물리적 보안적인 측면을 통합하여 정보보호관리체계를 수립, 운영하고 있거나 정보보호 활동을 하고 있다. 하지만 수립, 운영되고 있는 정보보호관리체계나 정보보호 활동의 성과에 대한 수준을 측정하는 지표가 존재하지 않거나 명확한 기준이 부족한 실정이다.

COBIT 프레임워크에서 제시하는 정보보호 프로세스에 대한 성숙도를 활용하여 정보보호 거버넌스의 3요소인 리더십, 조직구조, 프로세스 관점에서 정보보호 성숙도를 측정하는 연구 모형과 지표를 제시하고 이를 통하여 공공기관이나 일반 기업 조직의 성숙도 수준별 정보보호의 적절한 대응과 개선을 도모하고자 한다.

1.1 연구 배경

정보보호의 중요성으로 조직마다 해당 조직의 특성에 맞는 정보보호관리체계를 수립, 운영하고 있거나 정보보호 활동을 하고 있지만 어느 정도의 수준인지를 측정하는 기준이 존재하지 않거나 불명확한 기준에 의해서 정보보호 수준을 적절히 측정할 수 없다면 정보보호 관리체계나 정보보호 활동을 관리하거나 통제를 할 수 없을 뿐만 아니라 보다 나은 개선점을 찾을 수 없다. 그러므로 구체적인 정보보호에 대한 성숙도 측정 지표를 통해서 현재의 정보보호 수준을 파악하고 나아가서 정보보호 수준을 개선하고자 한다.

* (주)씨에이에스 / 고려대학교 일반대학원 디지털경영학과 박사과정 (cisspcho@gmail.com)
** 새마을금고 중앙회 / 고려대학교 일반대학원 디지털경영학과 박사과정 (xman8590@naver.com)
*** 고려대학교 디지털경영학과 교수 (mismdh@korea.ac.kr)

1.2 연구 목적 및 방법

COBIT 프레임워크에서 제시하는 정보보호 프로세스에 대한 성숙도 6단계(0 수준인 부재 단계에서 5 수준인 최적 단계까지)를 활용하여 정보보호 거버넌스의 3요소인 리더십, 조직구조, 프로세스 관점에서 각각 정보보호 성숙도를 측정하는 연구 모형과 지표를 제시함으로써 조직의 정보보호에 대한 성숙도의 수준을 측정하여 수준별 정보보호의 적절한 대응과 개선을 도모하고자 한다.

1.3 논문의 구성

본 논문은 다음과 같이 구성하였다. 제 1장에서는 연구의 배경 및 목적과 방법에 대해 설명을 하였다. 제 2장에서는 COBIT 프레임워크의 정보보호 프로세스에 따른 성숙도 모델과 정보보호 거버넌스의 의미 및 구성요소에 대하여 소개하였다. 제 3장에서는 정보보호 성숙도 측정지표를 도출하기 위해서 제 2장에서 논의한 내용들을 중심으로 정보보호 거버넌스 3요소와 COBIT 프레임워크 DS5 정보보호 프로세스의 성숙도 모델을 연계하여 측정지표 모델과 지표를 도출하였다. 제4장에서는 측정지표 모델과 지표에 대하여 결론을 맺었다.

II. 정보보호 성숙도에 대한 이론적 고찰

2.1 COBIT 프레임워크의 정보보호 프로세스

IT통제 및 거버넌스 프레임워크인 COBIT 4.1에서는 프로세스 도메인을 PO(Plan & Organize; 계획수립 및 조직화), AI(Acquire & Implement; 도입 및 구축), DS(Delivery & Support: 운영 및 지원), ME(Monitor & Evaluate: 모니터링 및 평가) 4가지로 분류하고 각각의 도메인에 프로세스를 분기하여 총 34개의 프로세스를 제시하고 있다. 이 중에서 DS5 프로세스는 정보보호에 대해 다음의 내용을 설명하고 있다.

DS5의 프로세스는 “시스템 보안성 확보”로써 정보의 무결성을 유지관리하고 IT 자산을 보호하기 위해서는 보안 관리 프로세스가 필요하며 이 프로세스에는 IT 보안에 대한 역할 및 책임, 정책, 표준, 절차 등을 수립하고 유지관리 하는 것이 포함된다. 또한 보안 관리에는 보안 모니터링 및 주기적인 테스트를 수행하고, 식별된 보안 취약점이나 인시던트에 대한 수정조치를 실행하는 것 등이 포함된다. 효과적인 보안 관리는 보안의 취약성 및 인시던트가 비즈니스에 미치는 파급효과를 최소화할 수 있도록 모든 IT 자산을 보호해야 한다는 것이다. 이 프로세스의 IT 목표는 정보 및 처리 인프라의 무결성을 유지관리하고, 보안 취약성 및 인시던트의 파급효과를 최소화한다는 것이다. 이 프로세스 목표는 IT 보안 정책, 절차, 표준 등을 정의하고, 보안 취약성 및 인시던트를 모니터링하고, 적발하고, 보고하고, 해결하는 것을 포함한다. 프로세스의 활동 목표로는 ● 보안에 대한 요구사항, 취약성, 위협 등을 파악하며 ● 사용자의 신원과 승인을 표준화된 방법으로 관리하며 ● 보안을 정기적으로 테스트하는 것이다. 핵심 메트릭으로는 ● 대중적인 물의를 일으킨 인시던트의 건수 ● 보안 요구사항들을 충족시킨 시스템의 수 ● 직무분리를 위배한 건수이다. [1]

2.2 COBIT 프레임워크의 정보보호 성숙도 모델

COBIT 프레임워크가 제시하는 성숙도 모델의 기본적인 표현은 다음과 같다.

0 부재 단계: 인식할 만한 프로세스가 전혀 존재하지 않는다. 조직은 해결해야 할 문제가 있다는 것조차 인식하지 못하고 있다.

1 초기/임기응변 단계: 문제가 존재하고 해결되어야 한다는 것을 조직이 인식하고 있다는 증거가 존재한다. 그러나 표준화된 프로세스가 존재하지 않고 개인별 혹은 사안별로 적용되는 임기응변적인 방법이 존재한다. 전반적인 관리 방법은 조직화되어 있지 않다.

2 반복/직관 단계: 동일한 작업을 수행하는 사람들이 서로 유사한 절차를 따르는 수준까지 프로세스가 발전되어있다. 공식적인 훈련이나 표준 절차에 대한 전파가 이루어지지 않고, 책임은 개인에게 맡겨져 있다. 개인의 지식에 대한 의존도가 높아서 오류가 발생할 가능성이 높다.

3 정의 단계: 절차가 표준화되고, 문서화되고, 훈련을 통해서 전파되고 있다. 그러나 이러한 프로세스를 따를 것인가의 여부는 개인의 재량에 맡겨져 있고,

프로세스를 준수하지 않는 행동이 감지될 수 있는 가능성이 낮다. 절차 자체는 정교하지 않지만, 현행 프랙티스를 공식화한 것이다.

4 관리/측정 단계: 절차의 준수 여부를 모니터링하고 측정하고, 프로세스가 효과적으로 수행되지 못하고 있다고 판단될 때 조치를 취하는 것이 가능하다. 프로세스는 지속적으로 개선되고 있고, 모범적인 프랙티스를 제시하고 있다. 자동화 및 도구는 제한적으로 혹은 부분적으로 활용되고 있다.

5 최적 단계: 프로세스는 지속적인 개선 및 다른 기업과의 성숙도 비교 등을 바탕으로 베스트 프랙티스의 수준으로 발전되어 있다. IT가 워크플로우를 자동화할 수 있도록 통합적인 방법으로 활용되어, 품질과 효과성을 향상시킬 수 있는 도구를 제공하고, 조직이 변화에 신속하게 대응하도록 하고 있다. [2]

DS5 프로세스 “시스템 보안성 확보”의 성숙도 모델은 정보 및 처리 인프라의 무결성을 유지관리하고, 보안 취약성 및 인시던트의 파급효과를 최소화한다는 IT에 대한 비즈니스 요구사항을 충족시키는 시스템 보안성 확보 프로세스의 관리를 기초로 하고 있다. 이 프로세스의 총 5개의 성숙도 모델은 다음과 같다. [3]

“성숙도 0 - 부재”는 다음과 같은 내용을 포함하고 있다. 조직은 IT 보안에 대한 필요성을 인식하지 못하고 있다. 보안에 대한 역할과 책임이 할당되어 있지 않은 상태이다. IT 보안의 관리를 위한 측정이 실행되고 있지 않고 있다. IT 보안 위반 행위나 취약점이 식별되면 보고절차와 그에 따른 대응이 이루어지지 않고 있다. 보안관리를 인식하는 프로세스가 전적으로 부족하다.

“성숙도 1 - 초기/임기응변”은 다음과 같은 내용을 포함하고 있다. 조직은 IT 보안에 대한 필요성을 인식하고 있다. 보안에 대한 의식은 개인에 따라 다르다. IT 보안은 사후 대응적으로 다루어지고 있고, 측정되지 않고 있다. IT 보안 위반 행위가 적발되면, 책임이 불분명하기 때문에 서로 책임을 미루는 현상이 발생하고 있다. IT 보안 위반 행위에 대한 대응은 예측 불가능하다.

“성숙도 - 2 반복/직관”은 다음과 같은 내용을 포함하고 있다. IT 보안에 대한 책임은 관리 권한이 제한적인 IT 보안 조정자에게 할당되어 있다. 보안의 필요성에 대한 인식은 단편적이고 제한적인 수준이다. 보안에 관련된 정보가 시스템에 의해서 생성되고 있지만, 분석되지 않고 있다. 외부업체의 서비스가 조직의 고유한 보안 필요성을 해결해 주지 못하고 있다. 보안 정책이 수립되고 있는 중이지만, 여전히 부적절한 스킬과 도구가 사용되고 있다. IT 보안에 관한 보고는 불완전하고, 사실을 정확하게 나타내지 못하거나 관련성이 없다. 보안에 대한 훈련이 가용하지만, 개인의 재량에 의해서 실시되고 있다. IT 보안은 IT 부문의 책임과 업무 영역으로 간주되고 있고, 비즈니스는 IT 보안이 자신들의 업무 영역으로 보지 않고 있다.

“성숙도 - 3 정의”는 다음과 같은 내용을 포함하고 있다. 보안 의식이 존재하고, 경영진이 보안 의식의 제고를 장려하고 있다. IT 보안 절차가 정의되어 있고, IT 보안 정책과 연계되어 있다. IT 보안에 대한 책임이 할당되어 있고 이해되고 있지만, 이러한 책임이 일관성 있게 집행되지 않고 있다. 위험 분석을 바탕으로 수립된 IT 보안 계획과 보안 솔루션이 존재한다. 보안에 관련된 보고는 명확한 비즈니스 측면의 초점을 포함하지 못하고 있다. 보안 테스트 (예: 침입 테스트)가 임기응변적으로 실시되고 있다. IT 및 현업을 대상으로 보안에 대한 훈련이 가용하지만, 비공식적으로 일정이 수립되고 관리되고 있다.

“성숙도 - 4 관리/측정”은 다음과 같은 내용을 포함하고 있다. IT 보안에 대한 책임이 명확하게 할당되고, 관리되고, 집행되고 있다. IT 보안 위험 및 영향 분석이 일관성 있게 수행되고 있다. 보안 정책 및 프랙티스가 구체적인 보안 기준선을 기반으로 하고 있다. 보안 의식을 제고하기 위한 방법을 의무적으로 공개하고 있다. 사용자의 식별, 인증 및 승인이 표준화되어 있다. 보안의 감사 및 관리 책임을 맡은 인력들에 대한 보안 인증을 추구하고 있다. 보안 테스트가 표준적이고, 공식화된 프로세스를 이용하여 완료되어, 보안 수준이 향상되고 있다. IT 보안 프로세스들은 조직의 전반적인 보안 기능과 조정되고 있다. IT 보안에 관한 보고는 경영 목적과 연계되어 있다. IT 보안에 대한 훈련이 현업과 IT 모두를 대상으로 실시되고 있다. IT 보안에 대한 훈련은 비즈니스의 필요성과 정의된 보안 위험 프로파일에 적합한 방법으로 계획되고, 관리되고 있다. 보안 관리에 대한 목표와 메트릭이 정의되어 있지만, 아직까지 측정되지 않고 있다.

"성숙도 - 5 최적"은 다음과 같은 내용을 포함하고 있다. IT 보안은 비즈니스 관리자와 IT 관리자의 공동 책임이고, 보안에 관련된 경영 목적에 통합되어 있다. IT 보안에 관련된 요구사항들은 명확하게 정의되고, 최적화 되고, 승인받은 보안 계획에 포함되어 있다. 사용자와 고객들이 점차 보안 요구사항을 정의하는데 최종적인 책임을 지고, 보안 기능은 설계 단계에서 애플리케이션에 통합되고 있다. 자동화 도구의 지원을 받는 공식화된 인시던트 대응 절차를 통해서 보안 인시던트가 즉각적으로 처리되고 있다. 정기적으로 수행되는 보안 평가에서는 보안 계획 실행의 효과성을 평가하고 있다. 새로운 위협과 취약성에 관한 정보가 체계적으로 수집되고, 분석되고 있다. 위험 경감을 위한 적절한 통제가 즉각적으로 전파되고 실행되고 있다. 보안 테스트, 보안 인시던트에 대한 근본원인 분석, 위험의 사전 예방적인 식별 등을 바탕으로 지속적인 개선이 이루어지고 있다. 보안 프로세스와 기술이 조직 전반적으로 통합되어 있다. 보안 관리에 대한 메트릭이 측정되고, 수집되고 전파되고 있다. 경영진은 이러한 지표를 활용하여 지속적인 개선 프로세스를 통해서 보안 계획을 조정하고 있다.

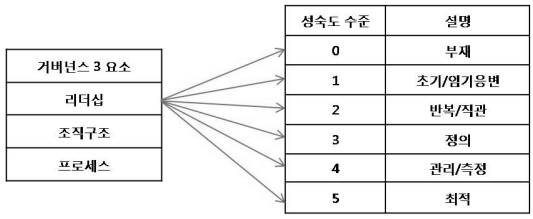
2.3 정보보호 거버넌스

정보보호 거버넌스는 정보에 대한 기밀성, 무결성, 가용성의 가치 지표에 초점을 맞춘 전반적인 활동으로서 조직을 둘러싼 환경변화가 글로벌 비즈니스로의 확장과 전 세계의 글로벌 네트워킹과 IT 의존성 증가와 이에 따른 정보 위협의 복잡성 증가로 다변화 되고 있다. 일반 대중과 규제기관에 부정확한 정보를 제공함으로써 발생되는 법적 책임과 사회적 책임은 물론 개인정보 보호에 대한 신의 성실의 실패와 규정과 준거에 대한 의무의 불이행은 조직에 심각한 결과를 초래할 수밖에 없는 조직의 생존과 직결되어 있다. 정보보호 거버넌스는 이사회와 고위 경영진의 책임으로 기업 거버넌스의 일부로서 통합되고 투명하여야 한다. 정보보호 거버넌스는 리더십, 조직구조, 정보보호 프로세스로 구성되어 있다.[4] 정보보호 거버넌스는 보안 프로그램의 수행을 구조화된 접근방법으로 이용하여 고위 경영진의 경영 및 의지가 조직의 보안 방침을 반영한다는 것을 보증한다. 정보보호 거버넌스의 결과는 전략적 연계(Strategic alignment), 리스크 관리(Risk management), 가치 전달(Value delivery), 자원 관리(Resource management), 성과관리(Performance measurement), 통합(Integration)으로 이루어져 있다.[5]

III. 정보보호 성숙도의 측정 모델

3.1 리더십 관점의 정보보호 성숙도 측정 모델 제시

COBIT DS5에서 제시하고 있는 성숙도 모델의 0~5 단계를 정보보호 거버넌스의 구성요소인 리더십 관점으로 연계성을 제시하였다 [그림 1]. 정보보호에 대한 정보보호관리체계는 전사적 차원의 경영관리체계의 일부이며 정보보호 활동은 조직의 경영관리 안에 통합되어야 하고 경영진의 의지와 지원이 필수 불가결한 요소라고 할 수 있다.



〔그림 1〕 리더십 관점과 정보보호 성숙도 연계

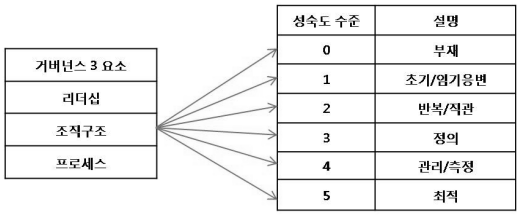
다음에 제시하는 [표 1]를 통해서 정보보호 거버넌스 리더십 관점에서 정보보호 성숙도의 측정지표를 제시하여 정보보호의 성과를 측정하게 된다.

〔표 1〕 리더십 관점의 정보보호 성숙도 지표

리더십 성숙도 지표	설명
0 부재	정보보호에 대한 경영진 리더십이 부재하다.
1 초기	정보보호에 대한 경영진 리더십의 필요성을 인식만 하고 있다.
2 반복	정보보호에 대한 경영진 리더십의 필요성을 인식하고 있지만, 부분적으로 리더십이 발휘되고 있다.
3 정의	정보보호에 대한 경영진 리더십의 필요성과 함께 경영진의 리더십만이 발휘되고 있고 일관성이 부족하다.
4 관리	정보보호에 대한 경영진 리더십의 필요성과 함께 경영진의 전사적인 리더십이 발휘되고, 리더십이 하위로 전달되고 있다.
5 최적	정보보호에 대한 경영진 리더십의 필요성과 함께 경영진의 전사적인 리더십이 발휘되고, 리더십이 하위로 전달되고 있으며 리더십에 대한 모니터링과 개선이 이루어지고 있다.

3.2 조직구조 관점의 정보보호 성숙도 측정 모델 제시

COBIT DS5에서 제시하고 있는 성숙도 모델의 0~5 단계를 정보보호 거버넌스의 구성요소인 조직구조 관점으로 연계성을 제시하였다 [그림 2]. 정보보호에 대한 정보보호관리체계는 역할, 책임, 해명책임성에 따른 조직구조에 포함되어 있어야 한다. 정보보호에 대한 명확한 역할이 각 조직구조의 구성원들에게 할당되어야 한다.



〔그림 2〕 조직구조 관점과 정보보호 성숙도 연계

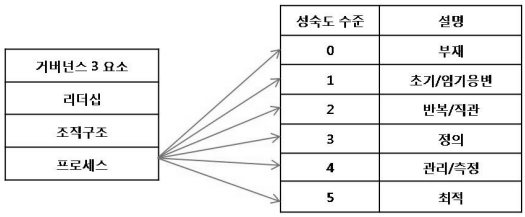
다음에 제시하는 [표 2]를 통해서 정보보호 거버넌스 조직구조 관점에서 정보보호 성숙도의 측정지표를 제시하여 정보보호의 성과를 측정하게 된다.

〔표 2〕 조직구조 관점의 정보보호 성숙도 지표

조직구조 성숙도 지표	설명
0 부재	정보보호 활동을 위한 역할, 책임, 해명책임성이 부재하다.
1 초기	정보보호 활동을 위한 역할, 책임, 해명책임성에 대해 필요성을 인식만 하고 있다.
2 반복	정보보호 활동을 위한 역할, 책임, 해명책임성에 대한 필요성을 인식하고 있지만, 한 사람이나 특정 부서에 한정되어 있다.
3 정의	정보보호 활동을 위한 역할, 책임, 해명책임성에 대한 필요성을 인식하고 전체 조직구조에 포함시키고 있으나 일관성이 부족하다.
4 관리	정보보호 활동을 위한 역할, 책임, 해명책임성에 대한 필요성을 인식하고 전체 조직구조에 포함시키고 있으며 전사적인 조직원의 정보보호 활동이 관리되고 측정된다.
5 최적	정보보호 활동을 위한 조직구조가 정의되고 관리되고 있으며 모니터링과 개선이 이루어지고 있다.

3.3 프로세스 관점의 정보보호 성숙도 측정 모델 제시

COBIT DS5에서 제시하고 있는 성숙도 모델의 0~5 단계를 정보보호 거버넌스의 구성요소인 프로세스 관점으로 연계성을 제시하였다 [그림 3]. 정보보호관리체계는 비즈니스 프로세스에 통합되어야 한다. 조직 내 비즈니스 프로세스와 정보보호 활동을 연결시키고 통합적으로 관리하여야 한다.



〔그림 3〕 프로세스 관점과 정보보호 성숙도 연계

다음에 제시하는 [표 3]을 통해서 정보보호 거버넌스 프로세스 관점에서 정보보호 성숙도의 측정지표를 제시하여 정보보호의 성과를 측정하게 된다.

〔표 3〕 프로세스 관점의 정보보호 성숙도 지표

조직구조 성숙도 지표	설명
0 부재	정보보호를 위한 프로세스가 부재하다.
1 초기	정보보호를 위한 프로세스에 대해 필요성을 인식만 하고 있다.
2 반복	정보보호를 위한 프로세스에 대해 필요성을 인식하고 있지만, 한 사람이나 특정 부서에 한정되어 있다.
3 정의	정보보호를 위한 프로세스에 대해 필요성을 인식하고 있고 전체 비즈니스 프로세스에 포함시키고 있으나 일관성이 부족하다.
4 관리	정보보호를 위한 프로세스에 대해 필요성을 인식하고 있고 전체 비즈니스 프로세스에 포함시키고 있다. 효과적이지 못한 프로세스는 조취를 취하고 있다.
5 최적	정보보호를 위한 프로세스에 대해 필요성을 인식하고 있고 전체 비즈니스 프로세스에 포함시키고 있으며 프로세스는 개선이 지속적으로 진행되고 있다.

IV. 결론

정보자산을 보호하기 위한 정보보호관리체계나 정보보호 활동은 정해진 기준에 의해 그 성과가 측정됨으로써 그 기준과 현재의 정보보호 수준과의 차이점을 파악할 수 있으며 이를 통해서 식별된 취약점을 보완하고

교정활동을 통해 보다 나은 개선활동으로 이어지는 선순환을 함으로써 정보자산의 보호에 대한 적정성을 보증할 수 있게 된다. COBIT 프레임워크 DS5 프로세스는 정보의 무결성을 유지관리하고 정보 자산을 보호하기 위해서는 보안 관리 프로세스가 필요하며 이 프로세스에는 정보 보안에 대한 역할 및 책임, 정책, 표준, 절차 등을 수립하고 유지관리 하는 것이 포함되어 있다. 또한 프로세스의 결과를 측정해서 그 수준을 정하는 성숙도 모델을 제시하고 있으며 성숙도의 수준은 인식할 만한 프로세스가 전혀 존재하지 않는 “0 부재” 단계, 표준화된 프로세스가 존재하지 않고 전반적인 관리 방법이 조직화되어 있지 않는 “1 초기/임기응변” 단계, 공식적인 훈련이나 표준 절차에 대한 전파가 이루어지지 않는 “2 반복/직관” 단계, 절차가 표준화되고 문서화되고 훈련을 통해서 전파되고 있는 “3 정의” 단계, 절차의 준수 여부를 모니터링하고 측정하며 프로세스가 효과적으로 수행되지 못하고 있다고 판단될 때 조치를 취하고 있는 “4 관리/측정” 단계, 프로세스는 지속적인 개선 및 다른 기업과의 성숙도 비교 등을 바탕으로 베스트 프랙티스의 수준으로 발전되는 “5 최적” 단계로 분류하고 있다. 이러한 성숙도 모델의 5단계를 정보보호 거버넌스의 3요소인 리더십, 조직구조, 프로세스 관점을 중심으로 하여 정보보호 성숙도 측정 지표를 제시하여 보았다.

정보보호 거버넌스에서의 리더십은 경영진의 의지와 지원이 필수 불가결한 요소이며 정보보호활동이나 정보보호관리체계는 전사적 차원의 경영관리체계의 일부이며 조직의 경영관리 안에 통합되어야 하는 것으로서 COBIT DS5에서 제시하고 있는 성숙도 모델의 0~5단계를 연계하여 정보보호 거버넌스 리더십 관점에서 정보보호 성숙도의 측정지표를 제시하였다. 정보보호 거버넌스의 조직구조 측면에서 정보보호관리체계는 역할, 책임, 해명책임성에 따른 조직구조에 포함되어 있어야 하며 정보보호에 대한 명확한 역할이 각 조직구조의 구성원들에게 할당되어야 하는 것으로 COBIT DS5에서 제시하고 있는 성숙도 모델의 0~5단계를 연계하여 정보보호 거버넌스 조직구조 관점에서 정보보호 성숙도의 측정지표를 제시하였다. 정보보호 거버넌스에서의 프로세스 측면에서 정보보호관리체계는 비즈니스 프로세스에 통합되어야 하며 조직 내 비즈니스 프로세스와 정보보호 활동을 연결시키고 통합적으로 관리하는 것으로 COBIT DS5에서 제시하고 있는 성숙도 모델의 0~5단계를 연계하여 정보보호 거버넌스 프로세스 관점에서 정보보호 성숙도의 측정지표를 제시하였다.

본 연구를 통해서 정보보호 거버넌스를 중심으로 하여 COBIT 프레임워크를 활용한 정보보호 성숙도 측정에 관한 연구로 공공기관 및 일반 기업의 정보보호 수준 향상에 다음과 같은 효과를 기대해 본다. 첫째, 제시한 측정지표를 이용하여 정보보호의 성과를 측정하고 이에 대한 성숙도 수준을 확인함으로써 현재의 정보보호 수준을 객관화 할 수 있다. 둘째, 객관화 된 정보보호 수준을 바탕으로 다음 수준(레벨)의 성숙도로 발전할 수 있는 개선의 방향을 제공할 수 있다. 셋째, 정보보호 성숙도 측정을 통해 조직의 성숙도 별 정보보호 수준 지표를 객관화함으로써 정보보호관리체계나 정보보호 활동에 대한 대내외적 인증 제시에 활용할 수 있다. 국가적으로 정보보호에 대한 인증을 장려하는 시대적 요구사항에서 한국인터넷진흥원(KISA)의 ISMS(정보보호관리체계) 인증제도에서 정보보호 성숙도 별 차등 인증 등에 도입하여 활용할 수 있는 계기를 마련할 수 있다. 넷째, 전사적이며 최고 경영진의 의지와 지원이 요구되는 정보보호 거버넌스의 필요성과 정보보호 거버넌스 수립에 성과측정 지표를 제시함으로써 정보보호 구현에 성과측정에 대한 구체적인 지표를 제시할 수 있다.

하지만 이 연구는 다음과 같은 한계를 가지고 있다. 정보보호 거버넌스의 3요소를 중심으로 범위를 한정지음으로써 정보보호 거버넌스 개념 정립이 부재하거나 아직 이른 조직에게는 타당한 지표를 제시할 수 없다는 것이며, IT 거버넌스와 통제의 프레임워크인 COBIT을 활용함으로써 IT 보안적인 요소에 치우쳐있는 한계점을 들 수 있다. 아울러 성숙도 지표가 계량적이고 정량적인 지표보다는 정성적인 지표에 한정적으로 제시한 것도 한계점이다.

따라서 향후에 이러한 한계점 등을 감안하여 공공기관과 일반 기업의 범용적인 정보보호 성숙도를 제시하고 IT 보안과 함께 정보보안을 포함시키며 정량적인 지표를 제공할 수 있는 연구가 지속되어야 할 것이다. 아울러 향후 국가적, 국제적 인증제도 등에서 정보보호 성숙도 모델과 성숙도 측정지표가 활용되어 정보보호 성숙도에 따른 차별화 된 인증제도가 국내와 국외에 소개되는 기회를 기대해본다.

참고문헌

[1] 황경태, “*COBIT 4.1*”, 사단법인 한국정보시스템감사통제협회, pp. 140, 2011.
[2] 황경태, “*COBIT 4.1*”, 사단법인 한국정보시스템감사통제협회, p. 31, 2011.
[3] 황경태, “*COBIT 4.1*”, 사단법인 한국정보시스템감사통제협회, pp. 145, 2011.
[4] (사)정보시스템감사통제협회, “*CISM Review Manual, 2012*”, 사단법인 한국정보시스템감사통제협회, pp. 43-44, 2012.
[5] (사)정보시스템감사통제협회, “*CISM Review Manual, 2012*”, 사단법인 한국정보시스템감사통제협회, pp. 44-45, 2012.

〈著者紹介〉

조 희 준 (Hee-Joon Cho)
2012년 2월 : 고려대학교 정책대학원 감사행정학 석사
2012년 3월~현재 : 고려대학교 일반대학원 디지털경영학과 박사과정
2010년 6월~현재 : (주)씨에이에스 컨설팅 이사
<관심분야> IT/정보보호 거버넌스, IT/정보보호 감사 및 감리

박 성 갑 (Sung-Kap Park)
2005년 8월 : 연세대학교 정경대학원 전산정보 석사
2013년 3월~현재 : 고려대학교 일반대학원 디지털경영학과 박사과정
2012년 3월~현재 : 새마을금고중앙회 전산정보부 정보보호팀 / 매니저
<관심분야> IT/정보보호 거버넌스, IT/정보보호 감사 및 감리

민 대 환 (Dae-Hwan Min)
1979년 서울대학교 경영 학사
1981년 KAIST 산업공학 석사
1991년 University of Michigan 경영정보학 박사
1991년 ~ 현재 고려대학교 경영정보학과/디지털 경영학과 교수
<관심분야> 정보기술 관리, 정보보호, BPM, 인터페이스 설계, 시스템 분석 및 설계, e-business 기술, e-business 전략, social media 등