정보보호관리 통제를 위한 프레임워크 개발

김정덕, 나태준

중앙대학교, 정보시스템학과

A Conceptual Framework for InfoSec Management Governance

Jungduk Kim, Taejoon Na

Department of Information Systems Chung-Ang Univ.

요 약

본 논문에서는 현재 그 중요성이 증가하고 있는 정보보호관리체계에 대하여 기존의 국내·외 정보보호관리체계 지침이나 표준 문서들이 단지 일반적인 가이드라인을 제공할 뿐, 평가나 측정, 혹은 인증을 위해 필요한 상세하고 객관적인 지표가 없다는 점을 파악하고, 이러한 주요 지표들을 개발하기 위한 프레임워크를 제시하고자 한다. 이 프레임워크는 정보보호관리 국제 표준인 ISO/IEC TR 13335 GMITS에서 정의하고 있는 정보보호관리 프로세스를 기준으로 적절한 정보보호관리 프로세스를 도출한 다음, 현재 정보기술 통제 기준으로 사용중인 COBIT의 각 주요 지표들을 위에서 도출된 프로세스별로 적용시키는 것이다. 즉 정보보호관리 프로세스별 주요목표지표(KGI - Key Goal Indicator), 주요성과지표(KPI - Key Performance Indicator), 그리고 핵심성공요소(CSF - Critical Success Factor)들을 개발하여 정보보호관리체계에 대한 상세하고 객관적인 평가와 측정을 가능하게 하고 이를 통해 총체적인 정보보호관리 통제 이룩하고자 한다.

I. 서론

증가하는 취약점과 위협으로부터 자산을 보호하기 위해서, 정부와 조직들은 서둘러 정보보호시스템을 구축하기에 이르렀다. 그러나 현재 대부분의 조직들이 채택하고 있는 각종 침입탐지시스템(IDS), 항 바이러스시스템(AVS), 방화벽(Firewall) 등의 정보보호시스템은 해당 영역에서만 그 역할을 수행할 뿐, 전체적인 입장에서의 정보보호 효과는 그리 두드러지고 있지는 않은 실정이다. 그 이유는 기존의 정보보호시스템이 관리적 차원에서의 문제점을 무시하고, 기술적 차원의 문제만 해결하려고 하며, 정보보호를 전담하고 있는 팀 구성이 취약하거나, 총체적이고 중앙 집중적인 정보보호관리가 부족하기 때문이다.

결국 조직은 자신의 정보보호관리체계를 수립하고 이것이 효과적이고 효율적이라는 것을 증명할 필요가 생기게 되었다. 또한 자신의 정보보호관리체계에 대한 효과성·효율성을 측정하고 평가하며, 개선하기 위해 노력하고 있다. 그러나 아직까지 이러한 정보보호관리체계를 평가하기 위한 상세하고 객관적인 기준은 나와있지 않은 실정이다. 비록 외국의 경우 정보보호관리체계에 대한 평가나 인증 작업은 현재 활발하게 진행중이며 제 3의 기관을 통한 공인 인증이 이미 시행되고 있지만, 대표적인 BS7799의 경우를 보더라도 정보보호관리시스템에 대한 보편적이고 일반적인 지침이나 기준을 제시하고 있다. 이는 정보보호관리를 위한 지침으로는 적합할 수 있지만 인증의 측면에서 볼 때에는, 기본적으로 합격/불합격 또는 만족/불만족의 이분법적 표현방식을 사용하기 때문에 그 결과로는 평가대상 조직의 정보보호관리체계 개선이나 향상이 쉽지 않다는 문제가 있다.

이에 본 논문에서는 정보보호관리체계에 대한 상세하고 객관적인 평가를 가능하게 하도록, 정보보호관리 프로세스별로 주요 지표들을 개발하기 위한 프레임워크를 제시하고자 한다. 주요 지표들은 현재 IT 통제의 기준인 COBIT(Control OBjectives for Information and related Technology)에서 제시하는 주요 지표들(핵심성공요소, 주요목표지표, 주요성과지표)이며 이 지표들

을 정보보호관리 프로세스에 적용시켜 개발함으로서 각 지표들을 통한 총체적인 정보보호관리 통제가 가능할 것이다.

II. 정보보호관리 프로세스에 관한 연구

1. ISO GMITS

현재 정보보호관리 국제 표준인 ISO/IEC TR 13335 GMITS(Guidelines for the Management of IT Security)에서 제시하는 정보보호관리 프로세스를 살펴보면 아래와 같다. [13]

우선 IT 보안목적과 전략 및 정책은 조직의 전체 수준에서 운영수준까지 계층구조별로 달성해야 할 보안목적, 목적을 달성하기 위한 방법으로서 전략, 그리고 목적을 달성하기 위한 규칙으로서 정책을 정하게 된다.

위험분석전략 선택은 조직의 환경에 적합한 위험관리 전략을 사용하기 위한 것으로, 이러한 위험분석에 대한 접근방법은 네 가지로 나뉘는데, 기본통제 접근방법(Baseline Approach), 상세 위험분석(Detailed Risk Analysis), 비공식적 접근방법(Informal Approach), 그리고 복합적 접근방법(Combined Approach)이 그것이다.

혼합적 접근방법은 현재 가장 권고되고 있는 위험분석 방법으로, 초기에 상위 수준의 위험분석 결과에 따라 조직의 사업목표에 중요하거나 위험으로 인한 영향이 크다고 판단되는 자산에는 상세 위험분석을, 그 외의 자산에는 기본통제 접근법을 수행하는 방법이다. 이러한 위험분석이 끝나면 해당 조직에 적합한 IT 보안계획을 확정하게 된다.

IT 보안계획의 구현은 확정된 IT 보안계획을 실행하는 것으로 여기서는 위험을 감소시키기 위한 모든 보안대책이 수행되며, 장치, 절차, 기법, 행위 등이 모두 포함된다. 여기서 대부분의 보안대책들은 조직적이고 관리적인 절차에 의해 실행되어야 한다. 더 나아가 보안인식의 제고 및 훈련 역시 반드시 수행되어야 하는 보안대책이다.

마지막으로 사후조치(Follow Up)는 조직이 채택한 보안대책들이 적절히 작용하고 있다는 것을 보증하기 위한 것이다. 이는 크게 보안 준거성 확인, 모니터링, 변화관리, 사고 처리 등의 활동들로 이루어져 있고, 이 외에 보안승인 검토, 운영환경의 검토, 로그 기록 검토 등의 활동들도 수행된다.

2. 정보보호관리 프로세스 도출

본 논문에서는 현재 국제표준인 GMITS의 정보보호관리 프로세스와, 위험분석 영역에서 권고되고 있는 프로세스들을 중심으로 다음과 같은 14개의 정보보호관리 프로세스를 제시한다.

표 1 : 정보보호관리 프로세스

영역	프로세스
IT 보안목적, 전략과 정책	IT 보안목적과 전략
	조직의 IT 보안 정책
위험 분석	상위수준 위험분석
	상세 위험분석 계획수립 및 승인
	자산식별 및 가치 평가
	위협 평가
	취약성 평가
	위험 평가
IT 보안의 구현	보안대책의 구현
	보안인식제고 교육 및 훈련
	IT 시스템 승인
사후조치	보안 준거성 확인
	모니터링
	사고처리
	변화통제

III. 정보보호관리 통제를 위한 프레임워크 개발

정보보호관리 통제를 위해서는 조직의 정보보호관리의 구축과 더불어, 현재 작동중인 정보보호관리체계에 대한 정확하고 지속적인 측정 및 평가 작업이 필요하다. 이러한 측정과 평가 작업을 통해서 조직은 현재 자신의 정보보호관리체계 수준과 필요한 요구사항들을 파악할 수 있고, 이를 바탕으로 조직의 정보보호관리체계에 대한 지속적인 개선이 가능하다. 또한 측정·평가는 객관적인 제3자에 의한 인증의 형태로 이루어질 수 있는데, 이 경우 조직은 자신의 정보보호관리체계의 수준을 알리고 조직의 경쟁력과 가치를 높일 수 있다.

영국 BS7799는 이러한 정보보호관리체계에 대한 인증의 대표적인 예로, BS779 Part II는 정보보호관리시스템(Information Security Management System : ISMS)에 대한 표준적인 명세서이다. 즉, 이는 ISMS에 대한 세부적인 규격으로 문서화에 대한 요구사항과 각 조직의 필요성에 따라 실행될 수 있는 정보보호관리 항목들을 규정하고 있다.

BS7799 Part II에 대한 인증에 대해 간단히 살펴보면, 해당 조직이 그들의 정보자산 관리를 설명하고 있는 개별 ISMS를 문서화를 통해서 수립하고, 이렇게 수립된 ISMS에 대해서 평가단이 판단하여 구체적인 인증 작업을 하게 된다. 이러한 인증은 일회적인 것이 아니라 지속적인 관리체계가 유지되고 있는가와 문서화가 영속적으로 이루어지고 있는가를 확인하는 절차를 거친다. [6][7]

다른 예로 미국의 FITSAF(Federal Information Technology Security Assessment Framework)를 들 수 있는데, 이는 미국 CIO 협의회에 의해 개발된 연방 정보기술 보안평가 프레임워크로 기관의 담당자들이 기존의 정책과 관련하여 그들의 보안 프로그램의 현재 상태를 결정하고, 필요한 경우 향상 목표를 수립하기 위한 방법을 제공한다. 연방 정보기술 보안평가 프레임워크는 정보기술 보안 프로그램의 효과성을 다섯 수준으로 구분하고 있는데, 각 수준에는 각 수준이 적절하게 구현되었는지를 확인하기 위한 기준들이 포함되고, 이를 사용하여 구체적인 관리적, 운영적 및 기술적 통제 목적들을 측정한다. 다섯 수준에 대해 살펴보면, 각각 문서화된 정책(수준 1), 문서화된 절차(수준 2), 구현된 절차와 통제(수준 3), 시험되고 검토된 절차와 통제(수준 4), 완전히 통합된 절차와 통제(수준 5)가 있다. [1]

그러나 이러한 대표적인 정보보호관리체계에 대한 평가나 인증제도 역시 현재로선 정보보호관리의 총체적인 통제를 위해서는 부족한 면이 없지 않다. BS7799의 경우 평가결과의 표현방식이 단일체제, 즉 만족/불만족의 방식으로 표현되기 때문에 평가 결과가 단순 명료하게 전달될 수 있다는 장점은 있으나 평가 대상의 개선이나 향상에 대한 상세한 기준을 제시하지 못한다는 단점이 있다. 또한 FITSAF의 경우 정보보호관리가 아닌 전체적인 보안 관점에서 평가를 수행한다. 게다가 그 대상이 현재는 정부기관에 한정되어 있기 때문에 이익을 최우선으로 하는 일반 기업들에게 적용하기엔 무리가 있을 수 있고, 일반 기업으로의 대상 전환이 아직 완료되지 않은 상황이라 어느 정도 시행착오의 기간이 필요할 것으로 본다.

이러한 한계점을 극복하는 방안으로, 정보보호관리체계의 기밀성, 가용성, 무결성 등을 확인할 수 있도록 주요 지표들을 개발할 것을 제시한다. 이를 위해서 본 논문에서는 대표적 IT관리도구인 COBIT에서 사용중인 세 가지의 주요 지표들(핵심성공요소, 주요목표지표, 주요성과지표)을 정의하고, 위에서 제시된 정보보호관리 프로세스별로 각 지표들을 적용할 것이다.

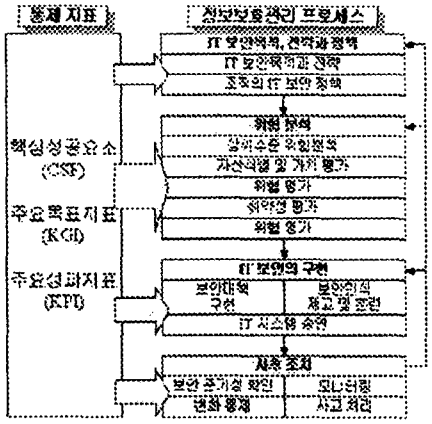

그림 1 : 정보보호관리 통제 프레임워크

적용하고자 하는 세 가지 주요 지표들에 대하여 살펴보면 다음과 같다.[15]

- 핵심성공요소(CSF : Critical Success Factor)는 프로세스의 성공을 위해 필요한 가장 중요한 전략적, 기술적, 조직적, 절차적 요소들을 의미한다. 이는 프로세스 또는 지원환경에 집중된 필수 실행동인으로 최적 성공, 또는 최적의 성공을 위해 권고된 활동을 위해 요구되는 일이나 조건을 나타낸다. 본질적으로 전략적, 기술적, 조직적, 절차적이고 사업관점이 아닌 프로세스 관점에서 표현된다.

- 주요목표지표(KGI : Key Goal Indicator)는 각 프로세스에서 "무엇이" 달성되어야 하는가를 측정하는 지표로, 해당 프로세스가 목표로 하는 것을 의미한다. 이는 프로세스 결과의 서술이며 따라서 후행 지표이다. 사업 중심적이고, 가능한 정확하고 측정 가능한 용어로 표현되어야 한다.

- 주요성과지표(KPI : Key Performance Indicator)는 프로세스가 "얼마나 잘" 달성되는가를 측정하는 지표로, 프로세스의 성공, 또는 실패의 정도를 표현한다. 이는 미래의 성공이나 실패의 확률을 예측하는 선행지수로 IT 중심적이고 정확히 측정 가능한 용어로 표현되어야 한다.

정보보호관리 프로세스별 주요 지표들을 개발하기 위해서 본 논문에서는 각 프로세스별로 모든 활동(Activities)들과 업무(Task)를 도출한다. 이 도출은 기존의 정보보호관리와 관련된 여러 가지 지침이나 표준들(예를 들어, BS7799, GMITS,

BSP등과 같은)을 기준으로 하며 중복된 것은 제외하게 된다.

이렇게 도출된 활동과 업무사항들을 중심으로 해당 프로세스에서 각각의 활동과 업무가 가져야 할 목표를 도출하고, 각 목표를 달성하기 위해 필요한 핵심성공요소들을 개발하게 된다. 또한 각 목표로부터 그 목표가 달성되었을 때 나오는 결과물들을 측정할 수 있는 지표의 형태로 도출하여 주요목표지표를 개발한다. 마지막으로 각 목표들에 대하여 이를 가능하게 하는 실행인자(Enabler)들이 무엇인지를 도출하고, 이 실행인자의 성과를 측정할 수 있는 지표의 형태로 주요성과지표를 개발하게 된다.

개발된 주요 지표들(핵심성공요소, 주요목표지표, 주요성과지표)은 현재 COBIT 경영자지침에서 제시하고 있는 각 지침들과 같은 프로세스의 범주 내에서 비교·참고할 수 있다. 또한 각 프로세스별 상세한 등급 분류를 통한 성숙도 모델을 개발할 때 그 기준으로 사용 가능하며, 이는 곧 정보보호관리체계 평가를 위한 공인된 객관적인 지표 개발의 기초로 작용 가능하다.

IV. 결론

조직의 정보보호관리체계가 중요한 만큼 이제는 그에 대한 평가나 측정이 더욱 중요시되고 있다. 이에 본 논문에서 정보보호관리 프로세스에 대한 평가나 측정을 통해 전체적인 통제가 가능하도록 주요 지표들을 개발할 것을 제시한다. 주요 지표들은 현재 IT 관리도구인 COBIT의 주요지침들을 따르며 정보보호관리 프로세스는 국제 표준인 GMITS의 정보보호관리 프로세스와 위험분석 영역에서 현재 권고되고 있는 프로세스들을 기준으로 하였다.

COBIT의 경영자지침에 제시된 각 주요 지표들의 경우 그 완성도를 더하기 위해 ISACA의 전문가들에 의해 여러 해에 걸쳐 시행착오를 겪으며 개발되었기 때문에, 정보보호관리 프로세스에 적용된 주요 지표들 역시 개발된 후에라도 얼마간의 시간 동안 지속적으로 검토·수정되어야 할 것이다.

참고문헌

[1] 김종기 외, "정보통신망 보호수준 측정방안 연구", 한국전자통신연구원, 2001

[2] 정보보호 21c, "IT보안관리 지침", 2001. 2 - 2001. 6

[3] 이경석 외, "정보보안시스템 구축에 관한 연구", 산업연구원, 1999

[4] 김정덕 외, "정보화지표 항목개발 및 계량화 연구". 1998

[5] BS7799 Part 1 "Information Security Management - Code of practice for information security management", BSI, 1999

[6] BS7799 Part 2 "Information Security Management - Specification for information security management", BSI, 1999

[7] PD3001 "Preparing for BS7799 Certification", BSI, 1999

[8] PD3002 "Guide to BS7799 Risk Assessment and Risk Management", BSI, 1999

[9] Guy King, "Best Security Practice : An Overview", Computer Sciences Corporation, 1999

[10]Government Process Classification Scheme : A Taxonomy of Common government Processes to use for Collection and Sharing "Best Practice", 1996

[11]ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 1 - Concepts and Model", 1997

[12]ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 2 - Managing and Planning IT Security", 1998

[13]ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 3 - Techniques for the Management of IT Security", 1998

[14]ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 4 - "Selection fo Safeguard", 1999

[15]Information Systems Audit and Control Association, "COBIT, Management Guideline, 3rd Edition", 2000