韓國 컴퓨터情報學會 論文誌
第12卷 第6號, 2007. 12.

2007-12-6-1-18

ISO 27001의 ISMS 보안성숙도 측정 모델링에 관한 연구 (ISO 27004 정보보호관리 측정 및 척도 체계)

김 태 달*

The ISO the research also the ISMS security maturity of 27001 regarding a measurement modeling (ISO 27004 information security management measurement and metric system)

tai-dal kim*

요 약

국내에서도 이제 정보시스템을 운영하고 있는 기업이나 기관들에서 체계적인 위험분석 및 보안관리에 대한 요구가 늘어나고 있다. 본 논문에서는 국제적인 정보보호관리시스템의 표준화 동향에 대해 조사. 분석하여 정보자산에 대해 통합적으로 위험을 관리 할 수 있는 정보보호관리시스템을 모델링하여 제안하였다. 제안시스템과 관련된 국제적인 표준에 대해 보안측정모델의 성숙도를 비교 분석한 결과, 개별 관리되던 각종 정보기술자원에 대한 보안관리를 전사차원에서 통합적으로 관리할 수 있게 되었고, ISO 27001, ISO 9000, ISO 14000 인증지원 및 인증수준 유지를 자동화 관리하게 함으로서 인적, 물적 자원의 효율적 운영이 가능한 것을 보여주고 있다.

Abstract

Recently the demand against the system risk analysis and security management from the enterprises or the agencies which operate a information system is increasing even from domestic. The international against the standardization trend of information protection management system it investigates from the dissertation which it sees. It analyzed and against information property information protection management system integrated it will be able to manage a danger modeling it did it proposed. Having analyzed as well as compared the matureness of security-measurement models in regard to the global standard of proposal system, the administrative presentation for various IT technology resources, which have been managed singly so far, is now well applied under the united control of the company itself, and enabled the automated management of authentication

• 제1저자 : 김태달
• 접수일 : 2007.11.5, 심사일 : 2007.11.10, 심사완료일 : 2007.11.19.
* 청운대학교 컴퓨터학과 교수
※ 본 연구는 청운대학교 교내 연구비 지원으로 이루어졌음.

support and renewal for ISO 27001, ISO 9000, ISO 14000, resulting in much advanced operation for both material and human resources.

▸ Keyword : ISMS (Information Security Management System), SSE-CMM, COBIT (ISACA Control OBjectives for Information and related Technology), ISFSoGP (Information Security Forum, Standard of Good Practice), IBM-ISF (IBM Information Security Frame- work)

Ⅰ. 서 론

현 시대에 있어 정보의 가치는 기업의 발전 및 연속성을 결정하는 중요한 요소로 대두되었다. 정보자산의 보호, 경쟁력 유지, 법규 준수, 상업적 이미지의 제고, 리스크 감소가 이제는 기업의 생존을 좌우하게 되었다. 정보 취약부분에 대한 보안을 위해서는 정보보호관리체계의 조직 내 정착 및 유지. 관리가 중요하며 조직 내부에서 정보보호관리체계의 독립적인 검토를 수행할 수 있고, 취약부분을 식별하고 개선할 수 있도록 기획하고 관리하는 관리자는 최신정보를 보유하고 위험에 따른 정보의 손실을 최소화할 수 있어야 한다.

국내에서도 이제 정보시스템을 운영하고 있는 기업이나 기관들에서 체계적인 위험분석 및 보안관리에 대한 요구가 늘어나고 있으며, 보안서비스업체의 컨설팅분야 (정보보호관리체계 수립)에서도 지속적으로 변화하고 있다. 이를 위해 사회와 일반조직에서도 정보보호관리시스템(Information Security Management System: ISMS)에 관심을 갖고 시스템 도입을 추진하고 있다.

ISMS란 조직의 통합관리시스템의 일부로 비즈니스 위험에 기반하여 정보보호를 위한 계획, 구현, 운영, 검토 및 개선시키기 위해 조직체계 및 정책, 정보보호 프로세스 및 절차, 정보보호통제 등으로 구성된 관리체계이다. [5,6]

국제표준인 ISO27001 ISMS인증은 국제표준화기구(ISO)에서 제정한 국제규격으로 BS7799 영국 표준에서 2005년 11월 ISO 국제표준으로 승격된 것으로 (그림 1)과 같이 PDCA(Plan-〉 Do-〉Check-〉 Act)사이클에 따른 ISMS 효과성 측정, 인적보안 강화, 외부업체 보안강화 등을 특징으로 한다.[5,6,7]

ISMS와 관련된 ISO 2700X에 대해 정의함에 있어, 해당분야를 분석해 보면 ISO 27001은 과거 BS7799-2를 수정하고 있으며, ISMS에 대해 기술하고 있으며, ISO 27002는 보통 BS7799-1로 알려져 있는 기존의 ISO 17799 표준의 잠재적인 새로운 표준이라고 할 수 있다.

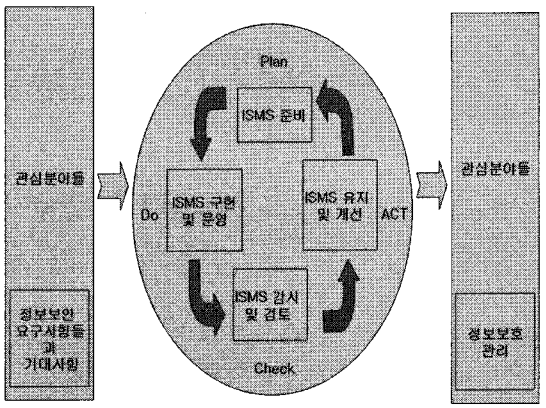

그림 1. ISMS 프로세서에 적용된 PDCA모델
Fig 1. The ISMS the PDCA model which is applied in the processor

ISO 27003은 ISMS 구현을 위한 새로운 안내 지침서라고 할 수 있고, ISO 27004는 정보보호체계 관리 측정 및 지표에 관한 새로운 표준을 제시하며, ISO 27005는 정보보호 위험관리 표준을 위해 할당 되었으며, ISO 27006은 인증조직에 관한 지침을 마련하고 있다.[8] 이와 관련 기존의 정보보호 성숙도 모델들에 대해 살펴보면, 프로세스 목표로 끌고 가는 시스템 보호엔지니어링을 위한 능력성숙도 모델인 SSE-CMM (Systems Security Engineering-Capability Maturity Model)과, 통합과 성숙도에 치중한 COBIT(ISACA Control OBjectives for Information and related Technology)과 프로세스 통합에 중점을 두고 있는 ISM3(Information Security Management Maturity Model)과 이상적인 사례를 정의하고 직접 비교하는 ISFSoGP(Information Security Forum, Standard of Good Practice), 기업에 따라서 능력에 대해 로드맵을 제시하는 IBM-ISF(IBM Information Security Frame-work) 등이 있다.

국가의 정보보호 수준을 결정하기 위해서는 개인, 기업 등 이용자를 중심으로 한 정보보호 기반시설, 정보보호 예산, 인력 등으로 구성된 정보보호 환경과 같은 보호활동 즉, 정보보호 수준과 보호활동에 원인을 제공하는 위협, 즉 정보화 역기능 수준을 종합적으로 고려하고 국가의 구성요소인 정부, 개인, 기업 차원에서 측정이 포함되어야 할 것이다.

(그림 2)는 국가정보보호수준 평가체계의 프레임워크를 그림으로 나타내고 있다.[1,3]

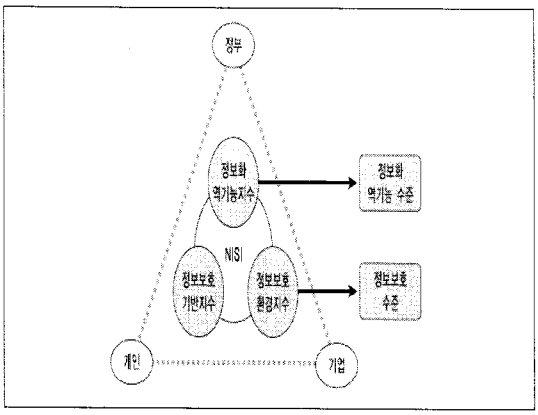

그림 2 국가 정보보호지수 프레임워크
Fig 2. National information protection quotient framework

II. 관련 연구

2.1 정보보호관리 국외 표준화 동향 [2]

2.1.1 BS7799

BS7799는 영국 BSI(British Standard Institute)에서 정보보호 관리를 위한 표준화된 실무규약(code of practice for information security management)으로서 1995년 처음 개발되었다. 1998년에는 이 기준에 따른 인증 요건을 개발하여 본래의 표준인 실무규약은 Part 1, 인증요건은 Part 2로 만들어졌다. 1999년 정보처리 기술의 발전을 반영하여 개정되었으며, 이 개정판에 기반하여 2000년에는 Part 1이 ISO/IEC JTC 1/SC27 WG1을 통하여 ISO 17799로 제정되었다. 현재는 Part 2를 ISO 표준으로 제정하기 위한 작업을 진행 중이다. BS7799 Part 1에서는 10개의 관리 통제 영역과 36개 통제 목적, 127개의 통제 항목으로 나누고 Part 2에서는 이에 따라 구현된 ISMS를 수립, 구현, 유지하기 위한 프로세스를 설명한다. BS7799 Part 1과 2는 호주/뉴질랜드, 브라질, 핀란드 공화국, 아이슬란드, 아일랜드, 네덜란드, 노르웨이, 스웨덴 등에서 국가표준으로 사용하고 있다.

2.1.2 ISO/IEC TR 13335 (GMITS)

국제 표준기구인 ISO/IEC JTC1 SC27 WG1에서 작성된 표준문서로, ISO/IEC TR 13335, "Guidelines for the Management of IT Security"의 5부로 구성되어 있다. 1부와 2부에서는 보안관리의 개념, 과정모델 및 위험관리와 기획 프로세스에 대한 내용들을 포함하고 있다. 이에 기초하여 3부에서는 보안관리 과정에서의 구체적인 기법들을 제시하고 있다. 4부에서는 보안요구사항과 조직의 특정 환경에 따라 보안대책을 어떻게 선정하는 과정을 기술하고 있으며 적절한 보호수준을 달성하기 위한 방법과 기본적 보안대책을 어떻게 적용할 수 있는가를 설명하고 있다. 5부에서는 인터넷과 같은 외부 네트워크와 연결된 상황에서의 보안대책을 선정하는 방법을 기술하고 있다.

2.1.3 IT Baseline Protection Manual

독일의 BSI(Bundesamt Für Sicherheit in der Information stechnik)에서 개발한 BSI IT Baseline Protection Manual은 IT시스템 차원에서 접근하고 있으며, 조직구조, 인력, 기반구조와 기술적인 차원을 적절하게 조화시켜 IT시스템에 대하여 정보보호 수준을 3단계로 분류하여 선택할 수 있도록 구성되어 있다.

이 매뉴얼은 자산별로 세부적인 설명을 하고 자산별로 가능한 위협들의 명세를 나열하였으며, 이러한 위협에 따른 위험을 줄이기 위한 가능한 통제사항들을 3단계 수준별로 구분하여 목록을 제시하고 있다.

2.1.4 일본(ISMS)

통산성은 기존의 정보시스템 안전대책 인증제도의 개선을 공표하고, 일본 정보처리 개발협회(JIPDEC)를 인정기관으로 지정하여, 2001년 4월 6일 정보시스템 안전대책 인증제도를 ISMS 인증 제도로 개정 시행 공표하였다. ISMS 위원회에서 인증심사기준 및 인증기관 지정기준을 마련하였고, 2001년 5월 22일부터 6월 4일까지 심사등록기관(인증기관) 지정 및 시범 인증사업을 시행한 후 본격적인 사업을 시행하였다.

일본의 ISMS 인증기준은 2002년 4월 1일부터 일본 산업 현황을 반영한 독자적인 인증기준(version 1.0)을 시행하다가 2003년 4월 1일부터는 BS 7799-2:2002 에 기반을 둔 version 2.0 을 시행해 오고 있다.

ISMS 통합 생명주기 측정 프로세스는 프로젝트나 조직 내에서 ISMS 사이클 안에서 통합되어야만 한다. 그리고 프로

젝트나 조직 안에서 보안과 관련된 프로세스들과 결과를 계속적으로 개선시키는데 효율적으로 사용되어 진다. (그림 3)은 ISMS 사이클 안에서 어떻게 측정 프로세스를 맞추어 갈 것인지를 나타내고 있다.[10]

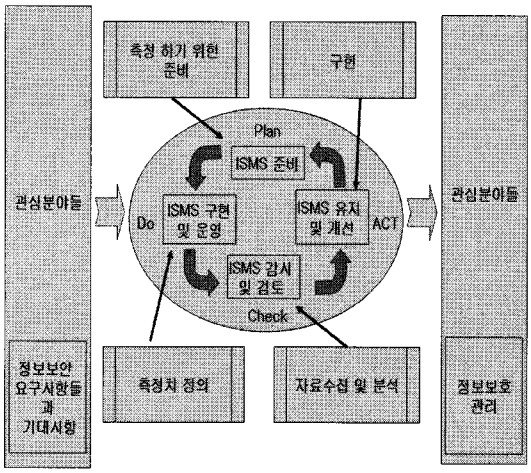

그림 3 ISMS 사이클 내에서의 측정
Fig 3. Measurement within ISMS cycle.

위 그림에서 계획단계(Plan)에서는 ISMS를 설치하는데, 이는 보안측정을 위한 준비 단계로 사업요구사항들, 보안정책, 위험관리, 통제 선택을 하게 된다.

수행단계(Do)에서는 측정항목 정의 단계로 측정을 위한 사업 요구사항들을 나타내고, 선택한 통제들에 대해 요구되는 효율성에 대해 정의한다.

점검 단계(Check)에는 통제 측정치, 인식, 운영에 관한 자료를 수집하고 분석하며, 모니터와 감리 및 측정에 관한 결과에 대해 평가하고 보고서를 작성한다.

실행단계(Act)는 구현단계로서 개선되었는지 확인하고, 통제방법을 개선하고 측정치를 수정하게 된다.

2.1.5 ISIZA Management Framework

남아프리카 공화국의 정보보호기구(ISIZA : Information Security Institute of South Africa)에서는 2000년 9월에 BS7799를 기반으로 한 정보보호 성숙도 평가 프레임워크를 제시하고 이를 기반으로 인증활동을 시행하고 있다.

남아프리카 공화국의 인증제도는 단계적 접근법을 택한 것이 특징이다. ISIZA는 기존의 BS7799가 정보보호관리체계 목적을 달성하는 데는 바람직한 도구이지만 단기간에 전체 요구사항을 충족하기는 어렵다는데 착안하여 점진적인 방법론을 제시하였고, ISIZA는 개발한 Management Framework를 국제 표준화하기 위해 활동 중이다.

2.2 정보보호지수 및 측정지표

정보보호지수의 구성 및 측정지표를 만들기 위한 연구는 (표 1)과 같이 세부지표에 사용되는 통계데이터는 한국정보보호진흥원의 『정보보호 실태조사』, 한국전산원의 『정보화통계집』에 의존하고 보안서버 보급률에 있어서는 OECD의 Communication Outlook을 참조하여 연구한 사례가 있다.[3] 그 외에도 국내, 외적으로 TTA, NIST(National Institute of Standards and Technology 등과 국내 한국정보통신기술협회(TTA) 한국전자통신연구원(ETRI), 정보통신정책연구원(KISDI), 한국표준협회(KSA)등에서 연구중이다.

각 지수의 성격을 보면, 정보보호 기반지수는 개인과 기업의 정보보호를 위한 시스템의 구축 정도나 데이터에 대한 정보보호 활동의 정도를 나타낸다. 이러한 정보보호 기반지수는 직접적인 정보보호 활동 수준을 나타낸다.

정보보호 환경지수는 정보보호에 대한 국민의 의식수준, 정보보호 활동을 위한 전문 인력의 확보 정도,

표 1 정보보호지수의 구성 및 측정 지표
table 1..Composition of information protection quotient and measurement index

구분	분류	세부지표
정보보호 수준지수	정보보호 기반	백신 보급률
		패치 보급률
		PKI 보급률
		Firewall 보급률
		IDS 보급률
		보안서버 보급률
	정보보호 환경	정보보호 관련 예산 비율
		정보보호 전문인력 비율
		국민의 보안의식 수준 비율
정보화 역기능 수준	정보화역기능	해킹.바이러스 신고비율
		개인정보 침해 신고비율
		스팸메일 수신비율

정보보호 환경지수는 정보보호에 대한 국민의 의식수준, 정보보호 활동을 위한 전문 인력의 확보 정도, 정보보호를 위한 연구개발의 적극성 등으로 구성되어 있다. 정보보호 환경지수는 간접적인 정보보호 수준을 나타낸다.

정보화역기능지수는 기반과 환경 부족으로 정보보호의 취약점 결과로서 나타난다. 시스템 침해 정도, 데이터 침해정도, 스팸메일의 수신정도를 나타낸다. 즉, 정보화 역기능지수가 높을수록 정보보호 활동 수준은 낮은 것으로 나타난다.

2.3 ISO/1EC WD 27004 측정 프로세스

현재 사용되고 있는 위험평가 접근이 효율성 있게 평가되고, 구현된 보안 통제들과 통제 목적들이 효율성 있게 평가되고 있는가, ISMS가 지속적인 개선 사이클을 갖고 있는지에 대한 효율성 평가, 관리관점에서 지원하기 위해 보안 측정항목이 준비되어 있는가, 정보보안을 위한 개선시설을 확보하고 있는가, 보안감사를 위한 입력사항이 준비되어 있는가, 조직내에서 정보보안의 가치에 대해 소통이 이루어지고 있는가, 보안측정이 가능토록 준비되고 있는가, 위험관리 절차에 따라 입력되고 지원되고 있는가에 대해 측정하는데 목적을 두고 있다. 그리고 측정 프로세스에는 개발척도와 운영을 측정할 수 있는 활동들, 분석과 보고서에 대한 측정, 결과에 대한 척도의 사용여부, 측정 프로세스에 대한 지속적인 개선책을 갖고 있는지를 검토하게 된다.

ISO/IEC 27004는 정보보호관리 측정을 위한 ISO의 새로운 표준이다. 이 표준은 현재 2008년을 목표로 각국에서 조언하고 있으며, 연구되고 있다. 이 표준은 기존의 보호관리 프로세스에 대해 다루고 있는 정의부분인 ISO/IEC 27001과 통제부분인 ISO/IEC 27002를 커버하며, 정보보호관리 시스템들의 효율성에 대해 조직들을 측정하고 보고하는데 도움을 줄 것으로 기대된다. 또한 이 표준은 ISMS에서 적용되는 정보보호 프로세스들과 정보보호 통제의 효율성을 결정하기 위한 측정절차와 기법에 대해 안내하고 있다. 이 표준에서 정의되고 있는 정보보호관리측정과 프로세스에 대한 구현과 개발의 목적은 ISMS 프로세스들과 관련되는 수집되고 분석 및 통신된 자료에 대해 각 조직을 위해 기본 자료로 활용된다. 이 자료는 궁극적으로 ISMS 구현을 개선하고 ISMS와 관련된 의사결정에 있어 기본으로 사용된다.

III. 정보기술 위험관리 시스템 모델 분석 및 제안

3.1 개괄적인 정보보안 측정 모형

개인들에 대한 통제에 있어 효율성에 관한 정보는 수집되고, 통합되고, 분석되어, 제 3자에게 (그림 4)과 같이 제공되게 된다.[10]

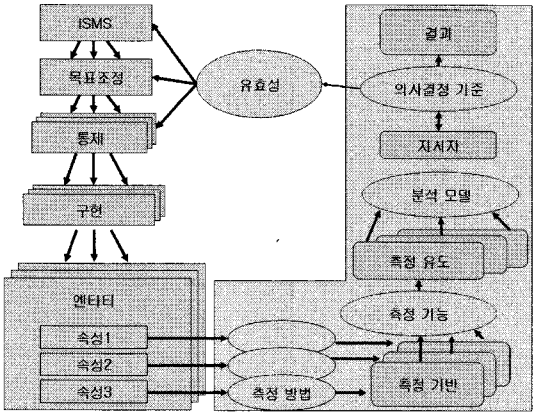

그림 4 정보보안 일반측정 모형
Fig 4. Information security general measurement model

3.2 정보기술위험관리시스템 모델링 제안

본 논문에서 제안 하는 정보기술 위험관리 시스템에 제한 시스템 구성도는 (그림 5)와 같다. [4]

제안시스템은 ISO27001에서 정의하고 있는 ISMS의 요건(Requirements)을 바탕으로 위험관리를 하기위한 시스템의 구성 예를 보여주고 있다. 구성요소로는 통제마스터 DB, 정책관리부, 위험시나리오 관리부, 수준관리부, 위험처리부 및 통제작업관리부를 포함하고 있다.

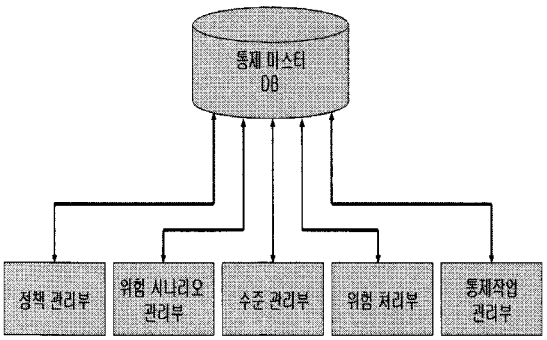

그림 5 정보기술 위험관리 시스템 구성체계
Fig 5. Information technical risk management system configuration

통제마스터 DB는 통제정책을 통제 가능한 최소한단위로 분해한 후 그 분해된 통제요소들 각각으로부터 하나의 통제항목(예컨대 명사(Noun), 하나의 통제행위(Verb, ISO9000, ISO14000, 및 CMM에서는 "프로세스" 라고 한다), 통제수

행자(Actor) 및 준수자를 정의하여 저장한다. 즉 통제 마스터 DB는 NVAM (Noun -Verb-Atomic-Measurable) 타입 통제 DB이다.

정책관리부는 통제 마스터 DB에서 정의된 통제요소를 관리한다. 특히 정책관리부는 통제 마스터 DB를 바탕으로 수행자 유형별/자산유형별/정책유형별 통제요소 조회 및 관리, 국제규격(ISO 27001, ISO9000, ISO 14000 등) 및 자체규격의 세부 통제 요소를 검색한다. 또한 통제 마스터 DB를 바탕으로 각 통제요소의 시행일자 및 개정일자에 대한 통제별 버전(version) 관리, 자체규정과 국제규격과의 연관성을 보여주는 SOA(Service of Applicability) 생성 및 조회 관리, 각 통제별 필요한 서식 및 양식의 연관관계 관리(문서 및 기록 관리)를 수행한다.

위협시나리오관리부는 통제 마스터 DB에서 정의된 통제요소를 역방향으로 정의하여 취약점을 추출하고, 그 취약점과 통제요소, 정보자산 및 위협간의 상관관계를 명시한다. 특히 통제 요소와 취약점간 상관관계의 정확도를 확보하기 위해 최하위 레벨(leaf level)의 통제요소와 취약점과의 1:1 관계를 설정한다. 또한 자산 유형별로 위협별 취약점에 대한 위험도를 계산하여 위험도가 높은 취약점에 대한 통제대책의 기존 수준을 파악하고, 위험완화를 위하여 제거해야 할 취약점과 이에 대한 통제 대책을 자동 매칭한다.

수준관리부는 통제요소 중 통제행위를 관리생명주기에 따라 시계열적으로 배열하고 각각의 통제행위의 존재여부를 판단함으로써 조직의 통제행위 성숙도(maturity)를 측정하고, 설정된 준수통제에 대한 조직 구성원들의 통제이행도(compliance)를 측정한다. 특히 계획(Plan), 이행(Do), 검토(Check) 및 개선(Act)을 포함하는 관리생명주기(PDCA)에 따라 상기 통제행위를 시계열적으로 배열한다. 이 때 계획(Plan)은 정책표준화, 담당자의 지정 및 권한 위임, 자원의 할당, 교육 및 전파 그리고 자동화지원도구의 할당을 포함하고, 이행(Do)은 계획단계에서 정의되고 위임된 통제대책의 준수 및 통제행위의 기록을 포함하고, 검토(Check)는 검토, 평가, 분석, 측정, 보고 및 감사를 포함한다. 또한 개선(Act)은 위험분석, 보고된 문제점에 대한 해결대안의 선택, 통제비용의 계산, 보증수준결정, 기회비용 계산 그리고 정책 및 프로세스 개선을 포함한다.

위험처리부는 통제개선유형에 대한 의사결정을 지원한다. 특히 통제 마스터DB를 바탕으로 위험을 분석하여 위험도가 높은 취약점에 대한 통제요소를 식별하고, 식별된 통제요소에 대한 통제비용에 의거하여 해당 통제요소 수행 시 기회비용을 자동으로 산정한 후 기회비용이 높은 통제요소부터 통제를 실시 의사결정을 지원하며, 통제개선유형을 단기/장기 및 긴급/통상으로 구분하여 작업관리를 위한 통제 개선지시를 분류하여 지원한다.

통제작업관리부는 상기 통제 보증수준 및 통제 개선유형에 따라 통제에 대한 작업을 지시하고 관리한다. 특히 통제 마스터DB를 바탕으로 수행자 및 통제항목별로 작업지시를 한 후 그에 대한 작업 완료율을 추적하고, 미 수행 된 통제에 대해 재작업지시를 한다. 또한 각 부서별 작업 이행율을 분석한다.

제안시스템의 처리과정은 통제 마스터DB구축, 현황분석, 자산평가, 위험평가, 위험처리, 통제이행, 모니터링, 작업관리, 종료단계를 거친다.

3.3. 제안 정보기술위험관리 시스템의 특성

제안시스템의 특징은 정보자산의 통합위험관리를 수행하며, 통제수준(모니터링)관리가 가능하고, KRI(Key Risk Indicator) 개념을 도입하고 있으며, 위협시나리오 DB를 구축하는 특성이 있다. (그림 6)에서는 NVAM 타입 DB를 바탕으로 한 ITRMS(Information Technology Risk Management System)의 다양한 정책 및 통제 검색화면의 예를 보여 주고 있다. [4]

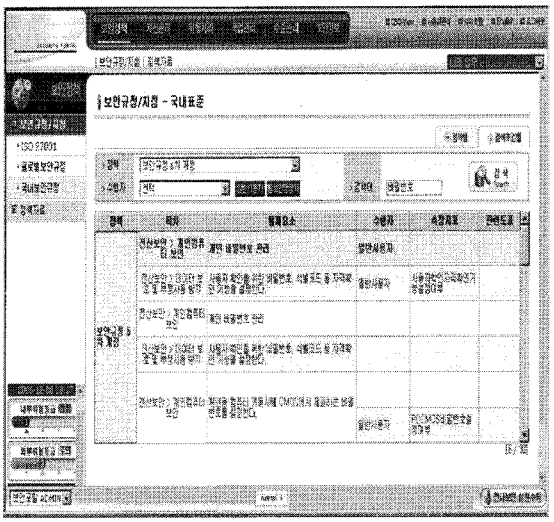

그림 6 제안 시스템인 ITRMS의 다양한 정책 및 통제 검색화면의 예
Fig 6. Example of the policy which the ITRMS which is a proposed system is various and the control search screen

3.4 보안측정 모델의 성숙도 분석 검토

기존에 발표되고 있는 보안성숙도 측정을 위한 모델들에 있어 성숙도 수준에 대해 비교 검토하면 (표 2)와 같으며[9], 본 논문에서 제안하고 있는 ITRMS와의 비교를 통해 모델성숙도에 대한 특성을 알 수 있다.

표 2 기존 보안성숙도 측정모델과의 비교
table 2.existing security maturity comparison of measurement model

모델 성숙도	SSE-CMM/ISO 21827	COBIT	ISM3	ISFSo GP	IBM-ISF	MeteRisk - ITRMS
5	지속적 개선	최적화 단계	최적화 단계		최적화 단계	지속적인 개선
4	계량 통제가능	관리 단계	조정 단계	모두 통제가	효율적 단계	측정 및 평가
3	잘 정의 됨	정의된 단계	관리 단계	대부분 통제가	적용 단계	프로세스 표준화
2	계획 및 추적가능	반복 단계	정의 됨	절반 통제가	기본 단계	정책,지침,교육 정의
1	비공식적 수행	초기 단계	미정의	일부 통제가	초기 단계	임의수행
0		미존재		통제불		통제없음

Ⅳ. 결론

본 논문은 정보보호관리시스템의 표준화 동향에 대해 연구하고, 정보자산의 통합관리를 수행하며, KRI개념을 도입하고 위협시나리오 DB를 구축하는 논문이다.

국내외 표준들과 모델들은 기본적으로 보안성숙도를 PDCA (Plan-Do-Check-Act)를 기준으로 하여 성숙도의 각 단계별로 구분 정의하고 있다. 여기서 성숙도 기준과 각 PDCA 통제행위와 비교가 필요하다.

PDCA에서 Plan은 보안활동에서는 보안정책, 지침, 절차, SOP(Standard Operation Procedures), 통제활동에 대한 R&R(Roles and Responsibilities)을 정의하고 표준화하는 프로세스를 의미한다. 이를 프로세스 성숙도의 관점에 연결 분석하면 대부분 2단계 및 3단계에 걸쳐있다고 할 수 있다. Do와 관련해서는 이행로그의 생산, 저장, 및 관리부분이 해당한다. 한편 Check단계에서는 각 통제행위에 대한 측정(정량적) 및 평가(정성적) 프로세스가 이루어진다. 이를 바탕으로 Act단계에서 평가 및 측정결과를 바탕으로 자동적이고 자발적인 개선활동이 지속적으로 실시되어야 한다.

본 연구에서는 기존의 개량된 성숙도 모델을 바탕으로 각 통제항목의 이행도를 결합한 새로운 수준측정 방법을 제시한다.

기존의 보안솔루션들은 기술적인 취약점과 통제에 집중되어 있다. 그러나 본 논문에서 제안하는 시스템은 기존 정책서 및 법률, 국제/국내 표준서 등과 같은 모든 규범서에 대한 수행자를 명확히 지정하고, 측정 가능하도록 KPI(Key Performance Indicator: 핵심성과지표)와 KRI(Key Risk Indicator: 핵심위험지표)를 통제 항목별로 할당/정의하므로 조직의 정책 이행도와 성숙도를 실질적으로 증진시킬 수 있도록 한다. 또한 각 사용자 유형별로 자신에게 해당되는 규정 및 지침 정보(통제정보)를 항상 최신의 상태로 사용할 수 있게 지원한다. 규범 및 정책 사용자 및 수행자(Actor) 유형별로 자신이 인지하고 준수해야 하는 보안관련 조항과 통제요소만 구분하여 조회 및 준수할 수 있게 됨으로써, 품질/서비스 경영 및 정보보호경영의 가장 중요한 요소인 통제(품질/보안/서비스) 마인드 확산과 이해도를 급속도로 증진시킬 수 있다. 또한 지금까지 사각지대였던 관리적, 물리적 보안에 대한 정형화된 위험분석기법의 통합 적용이 가능하다.

개별적으로 관리되던 각종 정보기술자원에 대한 보안관리를 전사차원에서 통합적으로 관리할 수 있다. 또한 본 제안시스템은 ISO 27001, ISO 9000, ISO 14000인증지원 및 인증 수준 유지를 자동화하여 관리함으로써 인적, 물적 자원의 효율적 운영이 획기적으로 향상된다. 또한 본 제안시스템은 지속적으로 보안관련 컨설팅 결과(위협시나리오 DB)를 최신의 상태로 유지할 수 있으며, 컨설팅의 효율성을 극대화 할 수 있다. 또한 보안관리 프로세스를 지속적으로 개선할 수 있는 개선체계 구축(CMM 5 level 획득)을 지원하는데, ISO 27001를 기반으로 하는 본 제안시스템을 적용함으로써 최소한 CMM 레벨 3은 확보 할 수 있는 장점을 갖게 된다. 또한 기업 및 조직 내에 산재한 정책서, 지침서, 표준서, 절차서 등의 통제관련 정보를 일관된 원칙하에 분류하여 체계적으로 DB화하고 관리할 수 있는 장점을 갖는다.

향후과제는 본 논문에서 제안하는 시스템이 국내, 외적으로 효율성 측면에서 보다 객관적으로 평가될 수 있도록 현장에서 많이 적용되고, 실무사례를 통해 지속적으로 보완해가며 최적의 솔루션을 찾을 수 있도록 계속적인 연구가 요구되는 분야이다.

참고문헌

[1] 국가정보보호수준 측정 및 활용에 관한 연구, 황철증 외 3명, 정보화정책 제 13권 제 3호, 2006.. 09. 18
[2] 정보보호관리 표준화 및 인증 연구, 한국정보보호진흥원, 2002.12
[3] 위험관리와 정보보호 사례 분석, 연구자료 RM 2006-75, 한국교육학술정보원, 2006. 11.
[4] 정보기술 위험관리시스템 및 그 방법, (주) 메타리스크,

대한민국 특허청, 2007.08.29
[5] 정보보호관리 체계인증동향, 한국정보보호진흥원, 2002.12
[6] Effective Management of Information Security and Privacy, Alicia Anderson, Educause quarterly, 2006
[7] INTERNATIONAL STANDARD ISO/IEC 27001, Information technology-Security techniques-Information security management systems-Requirements, First edition 2005.10.15
[8] The ISO/IEC 27000 Dictionary Standard, an introduction to iSO 27001, ISO 27002.... ISO27008, 2007. 07. 16
[9] Information Security Maturity Models, Alan Heward cissp cism Senior Information Security Architect IBM Security and Privacy Services, 2007
[10] ISO/IEC JTC 1/SC27 N5094, Information technology-Security techniques, Germany, 2006. 07.17

저 자 소 개

김 태 달

1979. 2. 숭실대학교 전자계산학과 졸업(學士)
1992. 2. 숭실대학교 정보과학대학 정보산업학과 졸업(理學碩士)
1997. 2. 숭실대학교 대학원 컴퓨터학과 졸업(工學博士)
1986. 08. 04 정보처리기술사
1997.3~현재 청운대학교 컴퓨터학과 교수
1997. 08. 01 정보통신기술공인감리인
2004. 6. 3 정부포상 (국무총리상)
(제17회 정보문화의달 국가정보화유공자)

〈관심분야〉 소프트웨어 엔지니어링, 프로젝트 관리, 정보시스템 감리, 정보시스템 품질관리, ITS, GIS 등 컴퓨터 응용분야.