정보시스템 위험관리 프로세스 특성에 관한 연구

김 태 달† · 이 형 원††

요 약

정보시스템 장애는 단순한 소프트웨어 오류에서부터 프로그램 시험 미비, 물리적인 방재시설 미비 등 다양하다. 비록 장애가 사소하더라도 그 결과는 엄청난 피해를 야기 시키기도 한다. 최근에는 이런 문제를 해결하는데 있어 단순한 외부 보안시스템만으로는 어렵게 되었다. 이제는 기업의 전반적인 정보기술에 대해 위험과 관련된 종합적인 대응책 수립과 적절한 대응이 필요한 시점에 도래하였다. 이와 관련하여 본 논문에서는 조직체 내에서 IT자원에 대한 무결성, 가용성, 기밀성을 고려하여 조직 내부와 외부에서 발생할 수 있는 각종 정보 및 시스템과 데이터에 대한 통제는 물론이고 위험에도 대처 할 수 있는 종합적인 위험관리시스템을 모델링하기위한 특성에 대해 연구하였다.

키워드 : 전사적위험관리, 네트워크관리시스템, 서버관리시스템, 변경관리시스템, 전사적암호관리, 기업위험통합데이터베이스, 정보기술위험관리시스템, 형상관리, 비즈니스프로세스관리, 비즈니스통합, 그룹웨어

The research regarding an information system risk management process characteristics

Tai-Dal Kim† · Hyung-Won Lee††

ABSTRACT

Information system failure is various such as program test unpreparedness, physical facilities for damage prevention unpreparedness from simple software error. Although cross is trifling the result causes vast damage. Recently, became difficult by simple outside security system to solve this problem. Now, synthetic countermove establishment and suitable confrontation connected with danger came in necessary visual point about general Information Technology of enterprise. In connection with, in this paper, various informations and system and control about data that can happen information inside and outside considering integrity for IT resource, solubility, confidentiality within organization studied about special quality to model synthetic Risk Management System that can of course and cope in danger.

Key Words : ERM(Enterprise Risk Management), NMS(Network Management System), SMS(Server Management System), CMS(Change Management System), ESM(Enterprise Security Management), ERDB(Enterprise Risk Database), ITRMS(Information Technology Risk Management System), CM(Configuration Management), BPM(Business Process Management), BI(Business Intelligence), GW(GroupWare)

1. 서 론

위험관리란 정보시스템 개발 프로젝트를 수행함에 있어 일어날 수 있는 여러 가지 프로젝트 수행 저해 요인들 또는 예기치 않은 돌발 상황에 대해 적절하게 대응할 수 있는 체계를 연구하는 것이다[5, 6, 7, 8].

각종 위험 요인들에 대해 사전에 예측하고 계획을 수립한 후 적절하게 대응하지 못함으로 해서 프로젝트가 위기에 직면하게 되는 것을 경험하고 있다[2, 4].

일반적으로 위험분석방법론 및 도구와 위험분석 프로세스로는 ISO/IEC-13335, OCTAVE 2.0, 캐나다 CSE, CRAMM, 영국 BS-7799, 한국 TTA 표준을 들 수 있다[3].

전 세계적으로 정보기술 위험관리에 대한 솔루션이나, 추천할 수 있는 특별한 패키지가 아직까지는 없는 상태로 조직체에서는 주로 외부보안(바이러스 백신. 방화벽. 침입방지시스템. 암호화 등)과 내부보안(접근제어. 문서유출 방지 등)에만 관심이 집중되고 있는 상황이다. IT기술과 수요자의 정보 욕구가 증가함으로서 조직체 내에서 IT자원에 대한 무결성. 가용성. 기밀성에 대한 내, 외부의 정보 및 시스템과 데이터 통제는 물론이고 위험에 대해 종합적으로 관리할 수 있는 시스템 솔루션 개발이 시급히 요구되고 있다[9].

현재 기업의 전체 IT전산자원에 대한 내, 외부의 위협 중 대다수의 솔루션이 외부보안에 치중하고 있어, 외부 보안보다 더욱 중요하고 비중이 큰 내부통제 및 보안관리 분야는

† 종신회원 : 청운대학교 컴퓨터학과 교수
†† 정 회 원 : (주) 매타리스크 대표이사
논문접수 : 2006년 10월 17일, 심사완료 : 2007년 4월 9일

위험이 그대로 노출되고 있는 실정이다[1].

본 논문에서는 기업 IT위험관리(자산식별. 위험분석. 통제설계. 통제구현. 위험모니터링. 위험대응. 발생한 위험 평가. 통제재설계 및 개선)의 일련의 기업 위험관리 프로세스 자동화 분야에 대해 관심을 갖고, 국내 (주)메타리스크의 정보기술 위험관리시스템(ITRMS)의 연구 및 개발 결과와 선진국 사례를 중심으로 정보시스템위험관리 프로세스 특성을 조사, 분석하였다.

2. 선진 사례 조사 검토

2.1. ISACA CoBIT 프레임워크

정보시스템 내부통제 및 감사에 관한 대표적인 국제조직인 ISACA(Information System Audit and Control Association)는 1980년대 후반부터 CoBIT(Control OBjectives for IT)이라하는 지침 가이드라인을 (그림 1)과 같이 제시하였으며, 이를 바탕으로 미국, 일본의 정부기관은 물론 대형 금융회사 등이 내부통제 지침으로 활용하고 있다[11, 12].

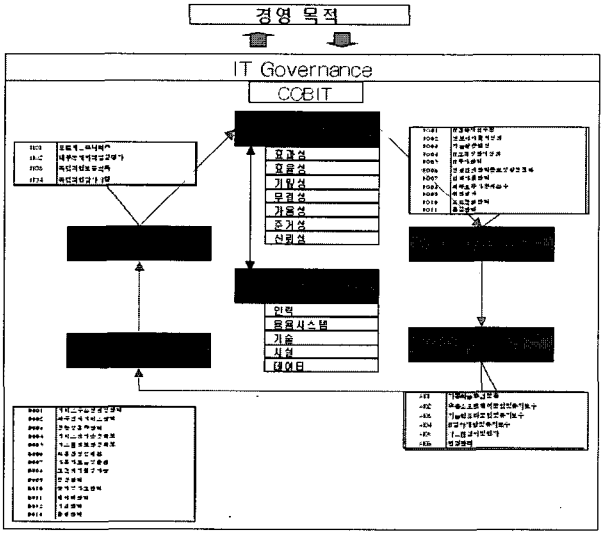
ITRMS도 CoBIT의 기본적인 프레임워크와 통제요소를 기반으로 솔루션을 기획-설계하고 있다.

CoBIT은 4개 도메인(기획. 획득 및 도입. 구축 및 운영. 모니터링 등)에 32개 통제영역에 관한 포괄적인 통제요소와 감사지침을 지원하고 있다[13].

2.2 캐나다 연방정부 위협 및 위험분석 가이드

캐나다는 1999년 자국의 정부기관 및 공공기관의 정보시스템 보호를 위하여 "Threat and Risk Assessment Working Guide"를 제정 공표하였다[12].

캐나다의 TRA모델은 (그림 2)와 같으며, 위험분석을 TRA (Threat and Risk Assessment) Model에 입각하여 위험관리를 실시하게 하고 있다.



(그림 1) CoBIT의 구성체계

2.3 PMBOK의 위험관리 분석

프로젝트 위험관리는 프로젝트 착수단계에 위험의 예측과 그 영향력 및 대응을 계획하고 프로젝트 수행단계에 이를 감시 및 관리하는 접근방식이 필요하다.

PMBOK에서 나타내고 있는 각 프로세스 내용을 구체적으로 정리 하면 <표 1>과 같다[14].

2.4 미국 정보기술 위험관리 권고안

미국 Carnegie Melon University의 Software Engineering Institute는 위험관리에 대하여 다음과 같이 정의하고 있다. CMU/SEI는 지속적인 위험 관리를 중요한 것으로 강조하고 있다.

리스크 관리란 어떤 프로젝트에 있어 리스크들을 관리하기 위한 프로세스, 방법. 도구들을 연구하는 소프트웨어 엔지니어링의 한 분야로 두고 연구하고 있다.

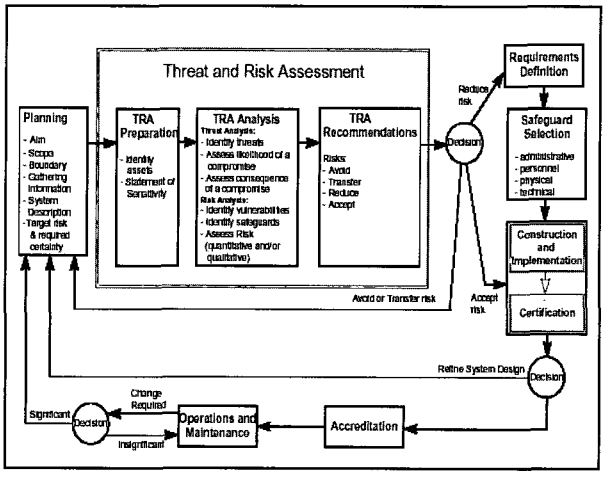
미국의 표준기구인 NIST는 미 연방정부 및 기관들을 위해 정보기술에 대한 위험관리 지침을 제정 권고하고 있다. NIST는 시스템개발주기와 위험관리를 상호 매핑하여 사용자가 시스템 개발 시부터 위험관리를 할 수 있도록 <표 2> 같이 가이드라인을 제시하고 있다[10, 15].

3. 국내 정보기술 위험관리시스템

현재 국내 수많은 기업에서 사용하고 있는 IT 관리시스템인 NMS, SMS, CMS 및 정보보호시스템(방화벽, 바이러스 백신, 암호화 도구 등)을 계측 및 제어할 수 있는 통합위험관리 시스템 구축이 요구되고 있다[2].

ITRMS란 기업의 정보기술자원의 기획, 개발 및 운영과 관련된 프로세스, 프로젝트 및 IT자원 전반에 대한 위험을 통합적으로 관리할 수 있게 지원하여 주는 시스템이며, ITRMS 개념도는 (그림 3)과 같다.

ITRMS의 기본기능은 (그림 4)와 같이 다음 6가 지로 기능으로 구성된다.



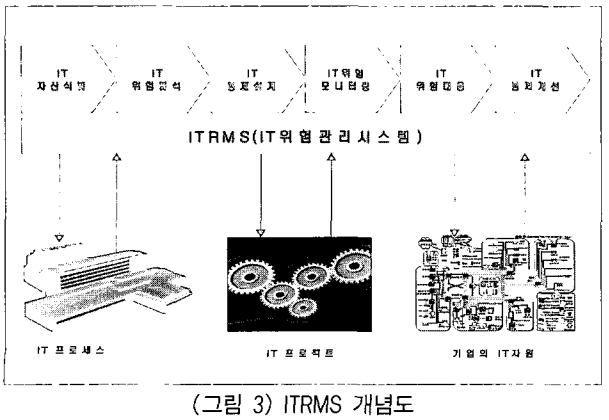
(그림 2) 캐나다 정부의 위협 및 위험요소분석

〈표 1〉 PMBOK 위험관리 프로세스

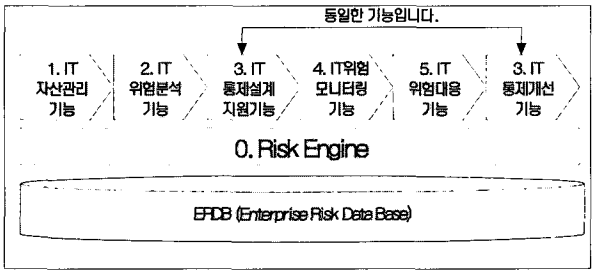
절차	입력(기초 정보) (Inputs)	도구와 기법 (Tools and Techniques)	출력(산출물) (Outputs)
위험관리 계획	1. 프로젝트 구성 2. 조직방침 3. 역할 및 책임 정의 4. 투자자의 우험 허용도 5. 조직의 위험 관리 계획을 위한템플릿 6. WBS(Work Breakdown Structure, 작업 분담 구조)	1. 계획의 회의	2. 위험 관리 계획서
위험요소 상정	1. 위험 관리 계획서 2. 프로젝트 계획 산출물 3. 위험 요소 분류 4. 실적 정보	1. 문서 검토 2. 정보 수집 기술 3. 검토 목록 4. 가정 조건 분석 5. 다이어그램 기법	1. 위험 2. 트리거 3. 다른 프로세스에 대한 영향력
위험요소 규명	1. 위험 관리 계획서 2. 상정된 위험 요서 3. 프로젝트 상태 4. 프로젝트 유형 5. 데이터 정확도 6. 확률 및 영향력 측정 척도 7. 가정 조건	1. 위험 확률과 영향력 2. 확률 및 영향력에 대한 위험 평가 알람 3. 프로젝트의 가정 조건 테스트 4. 데이터 정확도 순위	1. 위험 요소 순위 2. 우선 순위에 따른 위험 요소 일람 3. 추가 분석 및 관리가 필요한 위험 요소 4. 규명 분석 결과의 경향
위험요소 정량화	1. 위험 관리 계획서 2. 상정된 위험 요소 3. 우선 순위에 따른 위험 요소 일람 4. 실적 정보 5. 전문가 판단 6. 다른 프로세스의 계획 자료	1. 인터뷰 2. 가모분석 3. 의사 결정 xfl 분석 4. 시뮬레이션	1. 정량화된 위험 요소의 우선 순위 일람 2. 프로젝트 확률 분석 3. 비용과 일정 목표 달성 확률 4. 정량적인 위험 요소 분석 결과의 경향
위험대응 방법	1. 위험 관리 계획서 2. 우선 순위에 따른 위험 요소 일람 3. 프로젝트의 모든 위험 요소에 대한 비중 평가 4. 정량화된 위험 요소의 우선 순위 일람. 5. 프로젝트의 확률 분석 6. 비용과 일정 목표 달성 확률 7. 잠재적인 위험 요소 대응방법 8. 위험 임 계치(Risk Threshold) 9. 위험 요소에 대한 책임자 10. 일반적인 위험 요인 11. 위험 요소 규명 및 정략적인 위험 분석 결과의 경향	1. 회피(Avoidance) 2. 이전(Transference) 3. 경감(Migration) 4. 수용(Acceptance)	1. 위험 대응 계획서 2. 잔존 위험 요소 3. 2차 위험 4. 계약서 5. 필수적인 우발성(contingency)예비비 6. 다른 프로세스에 대한 기초 정보 7. 프로젝트 계획서에서 변경된 기초 정보
위험감시 및 관리	1. 위험 관리 계획서 2. 위험 대응 계획서 3. 프로젝트 내부 의사소통 방식 4. 위험 규명 및 분석에 대한 추가 작업 5. 범위 변경	1. 프로젝트 위험 대응 감사 2. 정기적인 위험 검토 3. 수확 가치(Earned Value) 4. 기술적인 실적측정 5. 위험 대응 계획서의 추가사항	1. 우회안 계획 2. 시정 방법 3. 변경 요청서 4. 위험 대응 계획 변경 5. 위험 요소 데이터베이스 6. 위험 요소 상정을 위한 검토 목록 갱신

〈표 2〉 개발수명주기로 본 통합위험관리

단 계	단계 특성	활동지원내용
1단계(착수)	문서화를 통해 목적과 목표와 필요성에 대해 서술	위기관리가 보안 요구들과 보안운영개념을 포함한 시스템요구사항들이 시스템 개발 요구사항들을 위해 지원하는데 사용되는 것을 알려준다.
2단계(개발/ 획득)	정보기술 시스템이 설계, 구현, 프로그래밍, 개발 또는 구축	시스템을 개발할 때 시스템구조와 설계 시 보안을 감안 설계한다.
3단계(구현)	시스템 보안 특성을 고려해서 구축, 시험, 검증	위험관리는 모델링 된 범위 내에서 시스템 요구사항에 대해 시스템 구현을 위해 평가를 지원한다.
4단계(운영 /유지보수)	조직의 프로세스, 정책, 절차에 따라서 하드웨어와 소프트웨어를 계속 추가할 것인지 수정 할 것인지 판단	위기관리 활동은 주기적으로 시스템을 재인정할 것인지 또한 운영 및 환경에 따라 언제 변경 할 것인지를 판단하도록 한다.
5 단계(처분)	현재 운영 중인 정보, 하드웨어, 소프트웨어에 대해 폐기 하는 단계	현재 운영 중인 시스템에 대해 적절하게 보안을 감안해서 파기하고 운영하고 이전한다.



(그림 3) ITRMS 개념도



(그림 4) ITRMS 기능구성도

1) 리스크 엔진 : ITRMS 외부로부터 각종 위험 관련 데이터를 자체의 DB 포맷에 맞게 전환 하고, ERDB를

구축하며, 자산가치의 산정, 각종 이벤트에 대한 필터링, 이벤트와 취약점, 통제 대책을 맵핑하여 주는 기능을 갖는다.

2) 자산관리 기능 : 응용 및 서비스의 중요도를 산정하고 이를 바탕으로 자산 (응용 S/W. H/W. DB. 서버. 네트워크 장비. 시스템 관리 솔루션. 보안관련 포인트 솔루션 등)의 자산가치를 산정하며, 자산의 이력. 현황통계. 추적 및 연동을 지원하는 기능을 갖는다.

3) 위험분석 기능 : 식별된 자산의 중요도를 기준으로 자산연동법칙에 의거하여 위협, 취약점, 개선해야 할 통제대책을 연계하여 정의하고 제시하는 기능을 갖는다.

4) 통제 및 관리정책/지침관리기능: 식별된 통제대책을 중심으로 관리정책 및 지침을 온라인으로 편집 및 수정, 조회하는 기능을 갖는다.

5) IT 위험 모니터링 기능 : 각 솔루션(NMS. SMS. DBMS. OS. ERP. ESM. CM. BPM. Bi. GW 등) 툴로부터 위험이벤트를 사전에 설정된 기준에 의거 필터링하여 사용자에게 실시간으로 위험 발생의 예보, 발생 경보, 발생 후 조치상황 등을 알려 주는 기능을 갖는다.

6) IT 위험 대응 기능 : 모니터링 되고, 보고된, 발생 위험에 대하여 이와 관련된 사람(프로세스 오너. 프로젝트 책임자, 실무책임자. 유지보수 요원. 하드웨어 장비 업체. 네트워크 관련업체 등)에게 즉각(인터넷의 Push 알림기능이나 휴대폰의 SMS를 이용하여)통보하고, 이에 상응하는 대응 프로세스를 각 사용자에게 전개하여 주는 기능을 갖는다.

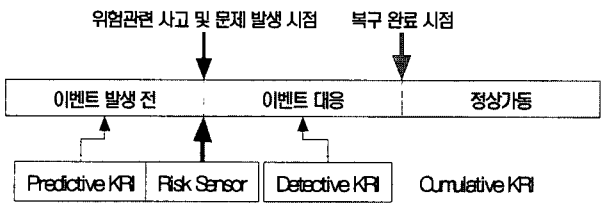
4. 위험관리 프로세스 모델 제안

4.1. 제안 위험관리 시스템 개념 정립

기업은 그 활동을 영위하는 과정에서 수많은 위험에 직면하게 되지만, 모든 위험을 관리할 필요는 없다. 즉 수용할 수 있거나 간과할 수 있는 위험까지도 관리하기 보다는 기업의 생존과 목적에 치명적인 핵심 위험만을 관리하는 것이 효율성 측면에서 바람직하다 할 수 있다. 이러한 측면에서 핵심위험지표는 (그림 5)와 같이 본 ITRMS의 핵심 용어이다.

ITRMS는 핵심위험지표를 3가지 유형으로 분류하는데, Predictive 핵심위험지표, Detective 핵심위험지표, Cumulative 핵심위험지표가 그것이다.

(1) Predictive 핵심위험지표는 주로 주요 위험이 발생할 것임을 사전에 알려주는 중요한 핵심위험지표이며, 대표적인 예로는 중요한 자산에 대한 불법접근 시도 (3회 이상 이상 패스워드 입력 오류), 중요한 자금 트랜잭션관리 프로그램의 유지보수 시행계획, 데이터베이스 이전계획 등이 있다. Predictive 핵심위험지표를 구현하기 위해서는 응용프로그램에 핵심위험지표 로직을 삽입하거나, 데이터베이스에서 관련데이터에 대한 접근패턴을 check하는 방식으로 구현될 수 있다. 구현의 효율성과 시스템의 유연성을 보장하기 위해서 ITRMS 는 Rule-based 데이터베이스 방식을 권고한다.



(그림 5) 각종 이벤트와 핵심위험지표 유형

(2) Detective 핵심위험지표는 주로 시스템에서 제공하는 로그를 이용하여 특정 사건이나 사고가 발생하였을 경우, 발생함과 동시에 또는 사후적으로 이 사건의 행위자, 발생원인, 피해범위 등을 추적하고 검출하기 위해 사용하는 핵심위험지표다.

Detective 핵심위험지표의 대표적인 예로는 침입시도자, 침입일자, 정보자산에 대한 부정당 행위 등과 관련된 것이다. 이를 구현하기 위해서는 정의된 핵심위험지표 관련 이벤트 검출 모듈 및 위험센서의 구현 그리고 로그관리시스템을 구축하여야한다.

(3) Cumulative 핵심위험지표는 기업에서 위험과 관련된 DW(DataWare-House)나 DM(Data Mining)기술을 이용하여 기존에 축적됐던 각종 데이터를 취합하여 향후에 어떠한 위험의 발생가능성이 높은 지를 예측하고, 각종 위험관련 데이터에 대한 통계처리를 위해 사용하는 지표이다.

4.2 IT Project 핵심 위험지표

대형 시스템 개발이나 도입 시 주로 관리해야 하는 핵심위험지표를 정의할 수 있다. 이를 IT 프로젝트 핵심위험지표(KRI : Key Risk Indicat -or)라고 한다.

이러한 IT 프로젝트의 핵심위험지표와 미국에서의 평균적인 프로젝트 당 발생빈도를 보여주는 조사 결과는 <표 3>과 같다.

〈표 3〉 SI 프로젝트 핵심위험지표 조사 요약

분야	KRI	발생빈도
MIS risk	사용자 요구사항의 증가	80
	과도한 일정상의 압력	65
	낮은 품질	60
	경비 초과	55
	부적절한 형상통제	50
시스템소프트웨어 risk	장기간 소요	70
	부적절한 비용 예측	65
	과도한 문서화	60
	오류가 많은 모듈	50
	프로젝트의 취소	35
상용소프트웨어 리스크	부적절한 사용자 문서화	70
	낮은 사용자 만족도	55
	마케팅에 소요되는 과도한 시간	50
	적대적 경쟁행위	45
	소성비용	30
군사용소프트웨어리스크	과도한 문서화	90
	낮은 생산성	85
	장기간 프로젝트 기간	75
	사용자 요구사항의 증가	70
	사용하지 않는 소프트웨어	45
SI형 소프트웨어	높은 유지보수 비용	60
	고객과의 불화	50
	사용자 요구사항의 증가	45
	예측하지 못한 검수기준	30
	소프트웨어와 전달물에 대한 법적 소유권한	20
최종사용자리스크	제공불가능한 응용	80
	숨겨진 오류	65
	유지보수가 불가능한 소프트웨어	60
	중복된 응용	50
	소프트웨어와 전달물에 대한 법적 소유권한	20

4.3. 위험센서(Risk Sensor)

핵심위험지표에 대한 정보를 수집하기 위해 ITRMS는 리스크센서의 설치를 필요로 한다. 여기서의 리스크센서는 입.출입통제장치, 지문인식기, 영상기록기 등의 하드웨어 센서뿐만이 아니라, 소프트웨어 센서도 포함한다. 특히 소프트웨어 센서는 중요한 정보자산 노드인 메인서버, DBMS, 응용서버, 네트워크 장비 등에 설치되어 핵심위험지표에 필요한 각종 정보를 수집하는 역할을 수행한다. 또한 위험센서는 문제발생주기와 관련하여 주로 문제 및 장애 발생시 작동된다. (그림 6)은 문제발생주기와 센서위치를 보여주고 있다.

응용센서는 핵심위험지표와 관련된 IPO 통제 컴포넌트를 응용에 삽입하여 핵심위험지표관련 이벤트나 트랜잭션을 검출하고, DBMS센서는 DB내 주요 테이블의 핵심 컬럼에 대한 무결성 로직(Domain Integrity)을 삽입하고, 트랜잭션 시 핵심위험지표에 해당하는 DB트랜잭션을 검출하며, System 관리 도구 Agent 센서는 NMS, SMS, CMS 등 시스템관리 도구가 설치된 서버에 로드되어 핵심위험지표 관련 트랜잭션 및 이벤트를 검출한다.

보안관련 포인트 솔루션 센서는 외부보안과 관련된 방화벽, IPS, 백신프로그램 및 외부로부터의 주의 및 긴급메일 등에서 핵심위험지표 관련 이벤트나 트랜잭션을 검출하며, 기타센서는 필요시 출입통제장치관리시스템, 원격모니터링 시스템, 경비관리시스템 등과 연동하여 핵심위험지표 관련 이벤트나 트랜잭션을 검출한다.

4.4 응용분야 중요도(Application Criticality)

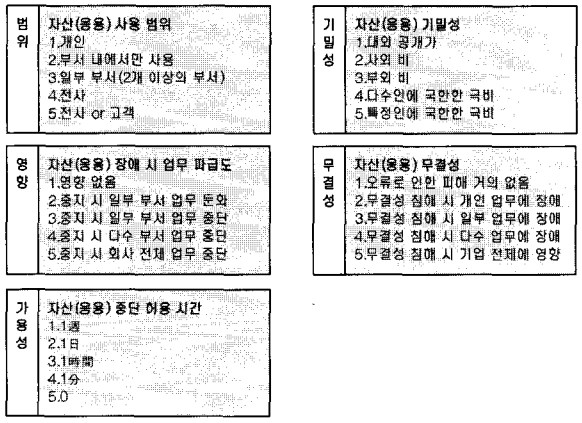
기업의 IT자산은 상대적으로 복잡하고 많은 요소로 구성되어 있다. ITRMS에서 응용분야는 응용업무시스템과 각종 정보기술 서비스를 의미하며, 응용업무시스템 및 서비스의 중요도를 결정짓는 속성은 응용의 사용범위. 응용의 영향도. 필요로 하는 무결성의 정도. 기밀성의 정도 및 가용성의 정도에 의해 수치적으로 명확히 정의된다. 기존의 위험관리시스템의 자산식별기법과 다른 방법이다. 또한 응용분야는 비즈니스 프로세스의 자동화된 형태로 표현되기도 한다. 정보자산에 대하여 그 중요도를 사용범위. 영향. 서비스 가용성 수준. 기밀성 수준 및 무결성 정도로 측정하고 이를 바탕으로 각 정보자산의 중요성을 산정한다. 여기서 중요한 것은 정보자산의 중요도가 응용프로그램 및 서비스 중요도에 의해 거의 결정된다는 것이다.

이는 응용과 서비스는 데이터와 관계를 가지며, 응용과 데이터는 플랫폼(서버 및 운영체제, 시스템소프트웨어)과 네트워크 노드(라우터, 스위치 등)와 긴밀하게 연관되어 있다는 것이다. (그림 7)에서는 응용분야의 중요도를 구분 짓는 5가지 속성인 범위. 영향. 가용성. 기밀성. 무결성에 대해 명시적으로 구분하고 있다.

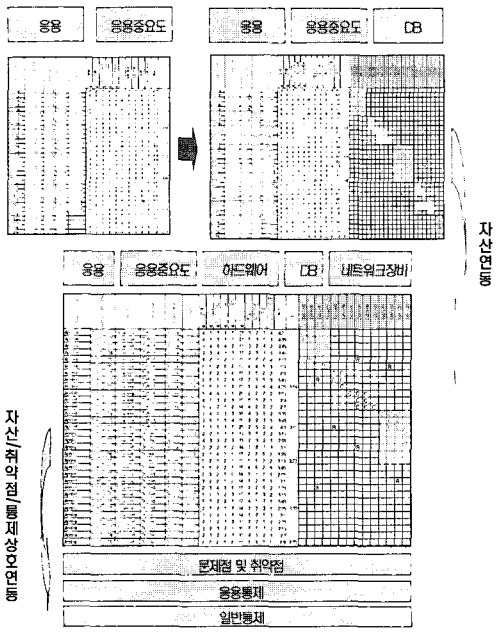
4.5 자산 연동 방식

기존의 위험분석패키지들이 대부분 위험분석 방법은 단위자산(예를 들어 서버. 네트워크 장비 등)에 대하여 위험분석을 시도하고 있다.

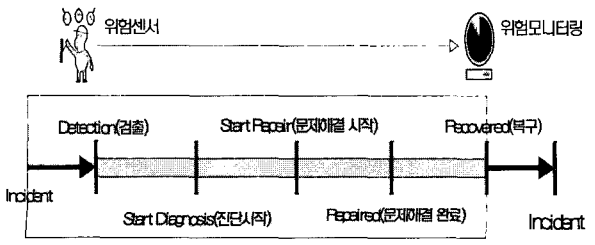
본 논문에서 제안하는 ITRMS는 자산연동방식을 채택하여 주요 응용분야와 서비스에 대한 중요도만 식별되면, 그 응용분야가 사용하는 데이터베이스, 응용분야에 로드된 서버와 클라이언트. 사용자. 네트워크 노드(예 : 라우터. 스위치. 방화벽 등)의 중요도와 같이 결정(MAX함수와 관계형함수 그리고 조합함수에 의해 자동 결정)되도록 설계되어진다. 이러한 연동설계는 ITRMS의 정보자산 메타데이터와 라이브러리에 의해 관리된다. 이러한 정보를 담고 있는 정보자산 마스터 테이블의 생성과정과 예시는 (그림 8)과 같다.



(그림 7) 응용 및 서비스 중요도 척도



(그림 8) 정보자산과 마스터테이블 생성과정



(그림 6) 문제발생주기와 센서위치

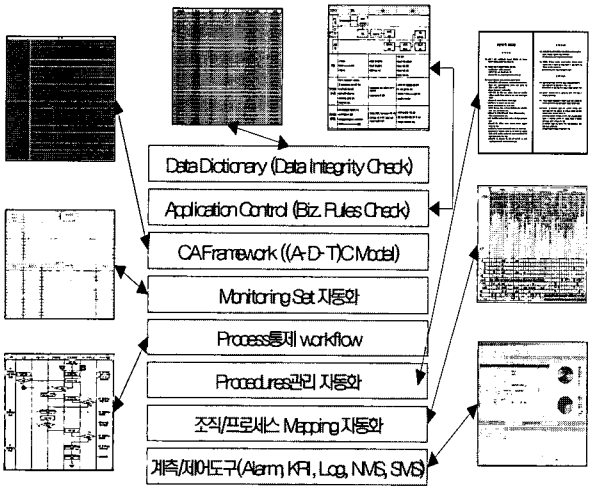
4.6 기업통제구조

기업에서 정보기술관련 아키텍처로서 EA (Enterprise Architecture)는 지금까지 DA(Data Architecture). BA(Business Architecture)와 TA(Technical Architecture)로 구성되어 있는 것으로 정의된다[6, 7]. 하지만 현재는 거대한 규모와 복잡한 구성요소로 이루어진 정보기술 및 정보시스템의 어디에도 신경계통과 같은 제어계측구조에 대해 언급되거나 통합적으로 관리되지 않고 있는 것이 사실이다. 그리고 ITRMS는 기존의 DA, BA, TA 구조 이외에 EA를 효율적이고, 효과적으로 그리고 실시간으로 계측제어하기 위한 관리구조로서 ECA(Enterprise Control Architecture)를 필요로 하는 것으로 정의하고 있다. (그림 9)는 ECA를 구성하는 통제요소를 보여주고 있다.

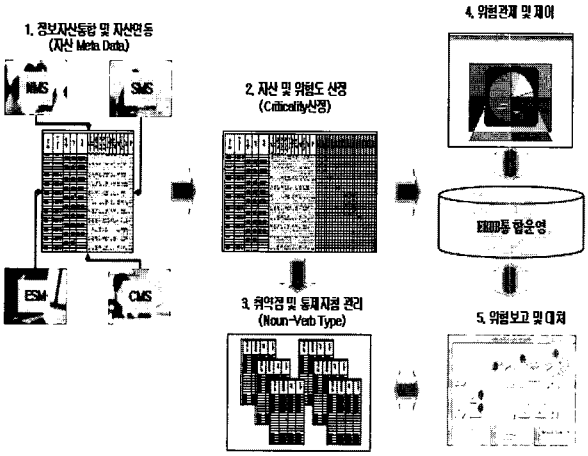
5. 위험관리 프로세스 모델 제안시스템

5.1 위험관리 프로세스 제안구성도

위험관리 프로세스 모델 제안시스템(ITRMS)은 기존의 NMS, SMS, ESM 및 ERP 등 (그림 10)과 같이 IT 및 Business 솔루션으로부터 위험관리대상 정보자산데이터베이스를 구축한다.



(그림 9) 기업통제구조 구성요소와 구조



(그림 10) ITRMS 구성체계도

또한 통합된 정보자산에 대하여 정보자산 중요도(달리 말하면 정보자산 가치)를 산정하는 특성을 갖는다.

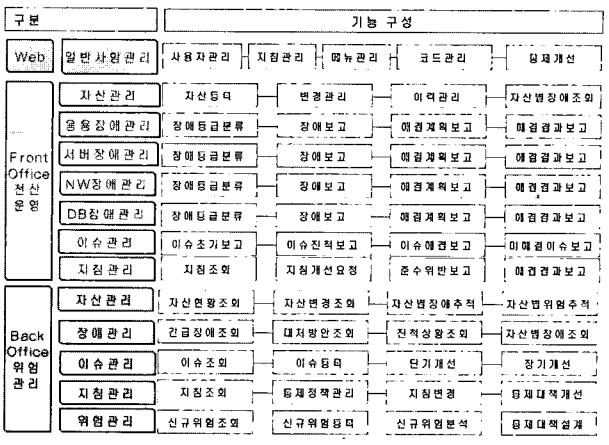
ITRMS는 응용분야 및 프로세스에 대한 중요도를 산정하며 이를 바탕으로 응용분야 및 프로세스와 연관된 정보자산의 중요도가 같이 산정한다. 그리고 파악된 정보자산에 대하여 정보자산에 대한 위협시나리오 생성기를 통하여 위협이 식별하고, 식별된 위협에 대한 취약점과 현재의 통제대책이 매핑되며, 이를 바탕으로 필요한 통제대책과 지침 안이 시스템에서 생성되도록 한다. 그리고 각종 솔루션 및 응용프로세스에 내장된 핵심위험지표에 대한 모니터링을 실시하고, 발생한 위험에 대하여 대처할 수 있도록 지원한다. 위에서 언급한 일련의 과정은 자산의 변동, 위험의 신규 발생 등에 의하여 지속적으로 갱신 및 최신화 되는 과정을 거친다.

5.2. 위험관리 프로세스 제안 기술 사양

ITRMS는 기본적으로 전사적 차원에서의 정보자산 통합관리를 할 수 있어야 한다. 또한 각 정보자산 간의 연동을 기본으로 설계된다. 그리고 연동체계는 저장된 자산스펙, 자산이력, 자산관련 위협, 위협에 대한 현재의 통제대책, 존재하는 취약점 그리고 개선하거나 신규로 도입해야 하는 통제대책을 FDD(Formal Descriptive Definition)에 의해 분류하여 저장하게 함으로써 각 위험관리 요소들 간의 정확한 연관관계와 추적가능성을 확보하도록 설계 제안하며, 본 논문에서는 IT위험관리시스템 기능구성을 (그림 11)과 같이 제안한다.

전산자원의 운영을 담당하는 Front Office와 이에 대한 위험관리를 담당하는 Back Office의 두 서브시스템으로 구성하고, 각각의 핵심은 보호하고 관리해야 할 정보자산 관리부분이다. 이러한 정보자산에 대한 각종 위험에 대해 발생예보. 발생경보. 발생 상황추적. 대응프로세스 전개. 사후보고 및 위험평가. 개선대책의 이행 등을 지원할 수 있게 설계한다.

ITRMS를 기업에서 도입하여 운영하기 위해서는 IT 위험관리관련 데이터베이스 구축 및 사용이 요구되는데, <표 4>과 같이 상위레벨의 데이터/기능 메트릭스를 통하여 고객과 기업이 원하는 데이터를 정확하게 구축하고 사용할 수 있게 한다.



(그림 11) ITRMS 의 기능 및 메뉴체계도

〈표 4〉 ITRMS 의 상위수준 데이터/기능관계도

기능 / 데이터	데이터 입력관리	자산관리 (변동 및 추적관리)	프로세스 및 지침관리	이슈 및 장애관리	현황 및 통계 조회
담당수작업입력 - 이슈사항입력 - 장애 및 문제보고 - self assessment 입력	●		●	●	●
솔루션데이터로딩 - 자산관리 - 변경관리(Harvest 등) - 운영관리(NMS□) - 보안관리(eTrust등)	●	●		●	●
기존데이터입력 - 자체관리 데이터입력 - 기타 데이터 로딩	●		◐		●
기존컨설팅결과입력 - 가용여부판단 - 취약점입력 - 정보자산데이터	●	◐		◐	●
분컨설팅입력 - 프로세스지침생성 - 진단결과입력 - 정보자산데이터 입력	●		●	●	●

6. 선진국 사례와 제안 한 ITRMS의 비교

기존 선진국 사례인 ISACA CoBIT 프레임워크. 캐나다 연방정부 위협 및 위험분석 가이드. PMBOK의 위험관리 분석. 미국 NIST 정보기술 위험관리 권고안과 본 논문에서 제안하고 있는 ITRMS와의 지원기능과 체계를 비교한 결과 <표 5>와 같은 특성을 갖는 것으로 분석되었다.

7. 결 론

기존에 ISACA ITGI의 COBIT, 미국 NIST의 기준 등은 위험관리 전주기에 대한 모델이라기보다는 위험분석에 중점을 둔 모델이다. 또한 COSO(Committee Of Sponsoring Organization)에서 2004년 10월 발표한 ERM 프레임워크는 현재 실시기준(Practice Guideline)등이 제시되지 않고 있으며, 각 프로세스 간의 연관성에 대한 정의가 미흡한 수준이다.

지금까지 발표된 여러 선진사례들과 비교하였을 때 본 연구결과는 다음과 같은 차이점을 가지고 있다.

첫째 : ITRMS는 위험관리전주기를 시스템화하여 PDCA (Plan-Do-Check-Act)가 가능하도록 설계되었다. 이는 정책관리, 자산관리, 위험처리, 통제작업관리, 수준관리 등 위험관리 각 프로세스가 위험관리 DB와 연동하여 순환적인 프로세스 성숙이 가능하도록 지원하는데 의의가 있다.

둘째 : 위험관리를 하기 위하여 우선적으로 정의되어야 할 것은 어떠한 자산에 대하여 어떠한 위험을 관리할 것인가에 대한 주제영역의 문제이다.

우선 ITRMS는 지금까지 보안부문에서 집중해 왔던 서버 및 네트워크 자산을 포함하여, 보다 중요한 종이문서자산, 전자정보자산, 이동식매체자산, PC자산 등을 통합하여 중요한IT자산에 가해지는 위험을 중점적으로 다루고 있다.

셋째 : ITRMS는 기존에 위험관리 방법론들이 모든 위험을 관리한다는 측면에서 접근하고 있지만, KPI개념을 도입하여 핵심위험지표를 개발하고 이를 DB화하여 집중적으로 관리한다는 측면에서 사용자 입장에서 효율적이다.

넷째 : IT위험관리에 대한 메타데이터를 설계하여 위험관리 프로세스를 지원하도록 되어 있어, 위험관리를 위한 CASE 툴로 사용가능하.

다섯째 : 맥아피의 파운드스톤, 시만택의 ESM 및 국내 정보보호 솔루션업체들의 위험관리제품들은 주로 서버 및 네트워크 단위 취약점 분석을 기반으로 하는 기술보안 위주의 제품으로 각 서버 등의 취약점 여부를 확인할 수 있는 기능이 없거나, 다아니면 발견한 취약점을 바탕으로 작업관

〈표 5〉 선진국 권고안과 ITRMS 비교. 분석

권고안	지원기능 특성	지원체계 특성
ISACA CoBIT	4개 도메인(기획. 획득 및 도입. 구축 및 운영. 모니터링 등)에 32개 통제영역에 관한 포괄적인 통제요소와 감사지침을 지원한다.	위험관리 개념이 반영되어 있지 않다. 위험관리에 대한 기본적인 절차만 통제항목의 한 구성항목으로 정의한다.
캐나다 권고안	위험분석을 TRA(Threat and Risk Assessment) Model에 입각하여 위험관리를 실시하도록 지원한다.	위험관리 중 위험분석에 집중하여 제시 위험분석은 단지 위험을 인지하고, 이의 정성적, 정량적 위험도만을 산정하는데 국한된다.
PMBOK	프로젝트관리 측면에서 프로젝트 착수단계에 위험의 예측과 그 영향력 및 대응을 계획하고 프로젝트 수행단계에 이를 감시 및 관리하는 접근방식을 지원한다.	프로젝트 수행 상 발생할 수 있는 위험분야에 대한 관리. 위험정책의 설정 등이 조직차원이 아니다.
미국 NIST	시스템개발주기와 위험관리를 상호 매핑하여 사용자가 시스템 개발 시부터 위험관리를 할 수 있도록 지원한다.	소프트웨어 개발과 관련된 프로젝트 위험관리에 집중하고 있다.
미국 COSO (Committee Of Sponsoring Organization)	1.전사적 위험관리의 적절성 2.프레이임워크 개요 3.내부 환경 4.목표 설정 5.사건의 인식 6.위험 평가 7.위험에 대한 대응책 8.통제활동 9.정보와 의사소통. 10.모니터링(Monitoring)등으로 구성되어 있으며, 재무위험뿐만 아니라, 비재무위험관리까지 총괄적으로 관리할 수 있는 최초의 모델	현재 프레임워크만 제공되고 있으며, 실용모델은 위험관리 전주기를 지원하지 못하고 있다. 지금까지 COBIT, SOX법 등은 주로 Control framework만 준용하여 적용되고 있다. 각 프로세스 간 연관성에 대한 정의가 결여되어 있다.
ITRMS	전사적 차원에서의 정보자산 통합관리를 할 수 있어야 한다. 또한 각 정보자산 간의 연동을 기본으로 설계하고 통제대책을 FDD(Formal Descriptive Definition)에 의해 분류하여 저장하게 함으로써 각 위험관리 요소들 간의 정확한 연관 관계와 추적가능성을 확보하도록 설계 지원한다.	미국 COSO의 전사적 위험관리 프레임의 하부 프로세스를 상호 연동하여 설계하고 있다. 현재는 ISO27001을 기반으로 설계되어 있으며, 향후 COBIT, ITIL등에 적용 확장할 수 있도록 구축되어 있다. 한편 위험관리에 KPI (Key Performance Indicator)개념이 KRI(Key Risk Indicator)를 적용하여 중요한 위험지표만을 집중적으로 관리한다. ITRMS는 조직의 각종 프로세스를 위험관리 차원에서 지휘 통제할 수 있는 솔루션 체계이다.

리를 연계하여 처리할 수 있는 기능이 미약한 점이 있다.

이에 비하여 ITRMS는 자체 포인트 솔루션 기능은 없지만 방화벽, IDS, 스케너 등을 연동하여 위험도를 고객의 환경과 특성에 맞게 산정하며 각 위험도를 조정(감소)하여 잔존위험처리를 할 수 있는 연계통제작업관리가 가능하다.

결론적으로 요약하면, ITRMS는 기존의 위험분석기법이나 표준 및 위험관리의 각 프로세스를 상호연동 시켜, PDCA가 가능하도록 설계되어 있어 조직의 프로세스 성숙도를 지속적으로 향상시킬 수 있는 장점을 지닌다.

한편 ITRMS는 이의 주제영역으로 IT부분의 운영위험관리와 보안위험관리부문을 집중적으로 다루고 있어, 자칫 모든 주제영역의 위험관리가 가능한 것처럼 오인될 소지를 감소시켜 그 효과를 제한하고자 한다. 또한 너무 많은 위험에 주의를 분산하지 않고 핵심위험에 집중하도록 하여 동 핵심위험을 위험관리전주기를 거쳐 우선적으로 관리할 수 있도록 설계되어 있으며, 통합위험관리를 지원한다.

참 고 문 헌

[1] 이형원, "IT창업경진대회 ITRMS 출품 명세서," 정보통신부, 2004.

[2] (주)메타리스크, "IT위험관리시스템 제품 사양서," 2006.

[3] 김인중, "정보통신 기반시설에 관한 위험분석 및 피해산정 연구", 성균관대학교 대학원 박사학위 논문, 2005.

[4] e-TQM, "위험관리", 삼성SDS, 2003.

[5] KSA0000, "리스크관리 용어-규격에 사용하기 위한 지침", 한국표준협회, 2001.

[6] "ARM standard," AIRMIC,ALARM,IRM,2002.

[7] "Annual defense report," http://www.dod. mil/ execsec/ adr2003/index.html, 2003.

[8] Jerry, Micccolis, Samir Shah, "Enterprise Risk Management," 2000.

[9] "Enterprise Risk Management-Integrated framework," COSO, 2004.

[10] Gary Stonebumer, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology systems," NIST, 2001.

[11] "RM Terminology Guidelines for use in standard," ISO/IEC Guide 73, 2000.

[12] CSE, "Threat and Risk Assessment Working Guide," http://www.cse-cst.gc.ca /publications /gov-pubs/itsg/itsg04-e.html, 2006.

[13] ISACA, "serving IT governance professionalsCOBIT online," 2006.

[14] ANSI/PMI 99-001-2000, an American National Standard, "A Guide to the Project Management Body of Knowledge (PMBok Guide)," 2000 Edition.

[15] U.S DOD, "Risk Management Guide for Acquisition," sixth Edition(V1.0), August 2006.

김 태 달

e-mail : ktd@chungwoon.ac.kr

1979년 숭실대학교 전자계산학과 (學士)

1992년 숭실대학교 정보과학대학원 정보산업학과 (理學碩士)

1997년 숭실대학교 대학원 컴퓨터학과 (工學博士)

1986년 정보처리기술사(情報處理技術士)

1997년 정보통신기술 공인수석감리원 (情報通信技術公認首席監理員)

2004년 국무총리상 수상(제17회 정보문화의달 국가정보화유공자로 선정)

1978년 ~1989년 쌍용정보통신(주), GIS 팀장, 국방프로젝트(PM)

1989년 ~1991년 현대전자(주) 시스템 소프트웨어 개발부(현, 현대정보기술) 시스템 소프트웨어 개발부, 중대형시스템 지원부 (부장)

1991년 ~1995년 도로교통안전협회 교통과학원 (수석연구원)

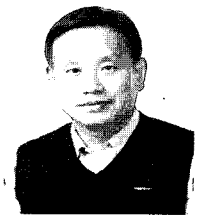
1995년 ~1997년 도로교통안전협회 (전산실장)

1997년 ~현 재 청운대학교 컴퓨터학과 교수

2003년 ~2005년 (사)한국정보통신기술사협회 감사

2005년 ~현 재 (사)한국정보처리학회 UTS 연구회 위원장

관심분야 : 소프트웨어 엔지니어링, 프로젝트 관리, 정보시스템 감리, 정보시스템 품질관리, ITS, GIS, u-city 등 컴퓨터 응용분야.



이 형 원

e-mail : hwlee@metarisk.com

1987년 한국외국어대학교 서양어대학 독어학과 졸업

1999년 한국정보통신대학원대학교 소프트웨어공학 석사과정 자퇴

1988년 CISA자격취득(EDPAA 현 ISACA)

1997년 국가정보화유공자로 정보통신부장관표창

2001년 국가공인정보시스템감리사(한국전산원)

2004년 정보통신부 주관 "제4회 IT벤처창업경진대회" ITRMS (IT위험관리시스템)으로 대상 수상 1990.12~1993.6 한국생산성본부 정보화사업부 선임연구원

1993년 ~1998년 한국전산원 전산망감리본부 선임연구원, 감리1팀장

2000년 ~2001년 제임스마틴코리아(주) 컨설팅사업부 책임컨설턴트

2001년 ~2002년 (주)에스큐브(정보보호전문업체) 보안컨설팅사업부 부장

2002년 ~2003년 (주)안철수연구소 보안컨설팅사업부 부장

2005년 ~현 재 (주)메타리스크 대표이사

관심분야 : 기업공학, 기업위험관리, 정보기술통제자동화, ISO27001 ISMS자동화, 데이터무결성 및 데이터 품질