# 정보시스템 신뢰성 향상을 위한 위험점수 측정모델 연구

## - A Risk Point Measuring Model for Improvement of the Information System Reliability -

조 두 호 *
Cho Doo Ho
서 장 훈 **
Seo Jang Hoon

## Abstract

Many researchers have proved that risk measurement of information systems is a very effective tool for improving confidence of information systems. However, inf ormation system risk in Korea still includes many subjective judgements. This stu dy deals with applying a quantitative model to improve risk measurement of infor mation system quality.

First of all, we have come up with solutions to improve the evaluation efficiency o n risk measurement. We have merged the risk guidelines of COBIT and CMM, and developed a quantified evaluation scheme that call by risk point. We have proved t he validity of this model by interviews with experts and by case studies.

**Keyword : Risk Point Measuring Model, Information System Reliability**

## 1. 서 론

조직의 정보시스템 위험관리를 효율적이며 효과적으로 달성하기 위해서는 위험도를 정확하게 평가해야 한다. 과거 정보시스템 위험분석에 대한 연구들은 기술적 관점을 통한 접근방법을 사용하여 새로운 기술개발이나 시스템구축에 의한 하드웨어 차원에서 해결책을 찾거나, 과거에 발생한 문제점과 대응방안을 통하여 위험분석을 해왔다. 하지만 이들은 정보시스템 발전에 따른 위험요소를 논하고 해결하는데 이에 상응하는 위험분석방법론이 되기에는 충분하지 못하였다. 결과적으로, 기존의 위험분석방법들이

* 한국전산원 선임연구원
** 한국능률협회 컨설턴트
2005년5월 접수; 2005년 6월 수정본 접수; 2005년 6월 게재 확정

빠르게 변화하는 환경에 유연하게 대응하지 못하며 주로 비상계획도, 재해복구능력 등 협소한 측면에 대해서만 평가결과를 제시하고 지속적인 피드백 및 개선방향을 제시하지 못하는 실정이다. 예컨대, 정보시스템 위험도 평가를 위한 방법은 시스템 평가에 대한 점수법을 이용한 'SAFE 체크리스트'(Krauss), 경험이 없는 위험분석가도 기존 시스템을 감사할 수 있도록 만든 '컴퓨터 보안 편람(Computer Security Handbook)'(Hoyt, Hutt et al), 컴퓨터 보안 자체 감사를 위해 만들어진 'AFIPS 체크리스트'(Browne), 미 공군 병참부대(AFLC: U.S. Air Force Logistics Command)를 위해 국립 로렌스 리버모어 연구소(LLNL: Lawrence Livermore National Laboratory)에서 개발한 'LLNL 체크리스트'(Sartorio)등이 있으나 대부분 단순한 체크리스트 접근방법을 이용한 취약성 평가가 주류를 이루었다.

이를 극복하기 위해서 본 논문에서는 위험 발생 확률과 영향의 결합 또는 자산의 가치와 위협수준에 의해 결정되는 위험도 측정 방법 중 두 번째 방법인 자산의 가치와 위협수준을 기초로 하여 조직의 위험도를 종합적이고 객관적으로 평가 할 수 있는 모델인 위험점수 모델을 기존연구 조사와 함께 문제점을 확인하고, 사례를 통하여 이에 대한 정보시스템 조직의 위험도를 종합적이고, 객관적으로 평가 할 수 있는 모델 개선안방안을 연구관점에서 제시하고자 한다.

## 2. 정보시스템 위험분석 기존연구

정보시스템 프로젝트 관리자들의 효율적인 프로젝트 관리를 가능하게 해 주는 가장 널리 사용되는 도구가 위험관리 방법론과 위험요인 체크리스트이다. Applegate[1996], Higuera[1995], COCOMO II[1998], Boehm[1989], Barki et al.[1993, 2001] 등이 정보시스템의 개발과정, 개발환경, 개발계획의 맥락에서 체크리스트를 제시하였고, Schmidt et al.[2001]은 최신 기술을 적용한 정보시스템 프로젝트에서의 위험요인 체크리스트를 프로젝트 관리 관점에서 제시하였다.

Applegate[1996]는 정보시스템 프로젝트 위험관리 사례를 통해 위험요인을 프로젝트 크기, 기술분야의 경험정도, 프로젝트의 구조화 정도에 따라 체크리스트 형태로 제시하였으며, Boehm[1991]은 위험요인별 관리기술을 제시하였다. Higuere[1995]는 위험관리를 방법론의 형태로 접근하는 체계를 제시하였다.

5개 영역의 체크리스트를 제시하였던 Barki et al.은 후속 연구[Barki et al., 2001]에서 75개 기업에서 진행중인 120개의 정보시스템 개발 프로젝트를 대상으로 프로젝트 위험 체크리스트를 사용하여 발생된 위험 요인에 대한 대처방안이 정보시스템 프로젝트의 성과에 미치는 영향에 관하여 실증적 연구를 수행하기도 하였다. Schmidt et al.[2001]은 새로운 정보시스템 환경에 맞는 위험요인 체크리스트를 탐색적 연구를 통하여 제시하였다. 이들은 정보시스템 프로젝트 관리 관점에서 조직환경, 후원/주인의식(Sponsorship/ Ownership), 관계관리, 프로젝트 관리, 범위, 요구사항, 자금, 일정, 개발과정, 인적자원, 프로젝트 수행인력, 기술, 외부의존성, 계획에 이르기까지 프로젝트의 전반적인 요인들을 고려하여 14개 영역으로 분류하였으며, 기존 위험요인 리스트 이외

에 26개의 새로운 위험 요인을 생성함으로써 53개의 위험요인으로 구성된 새로운 리스트를 제시하였다. Schmidt et al.[2001]의 연구에서는 위험요인에 대한 우선순위가 국가별로 상이하게 나타난다는 것을 보임으로써 정보시스템 위험요인에 대한 인식은 문화적, 환경적 요인을 반영하고 있다는 점을 제시하였다. 또한 Jiang et al.[2002]은 Barki et al.[1993]이 제시한 위험요인을 기반으로 152명의 프로젝트 관리자를 대상으로 한 실증연구를 통하여 45개 위험요인리스트를 제시하였다.

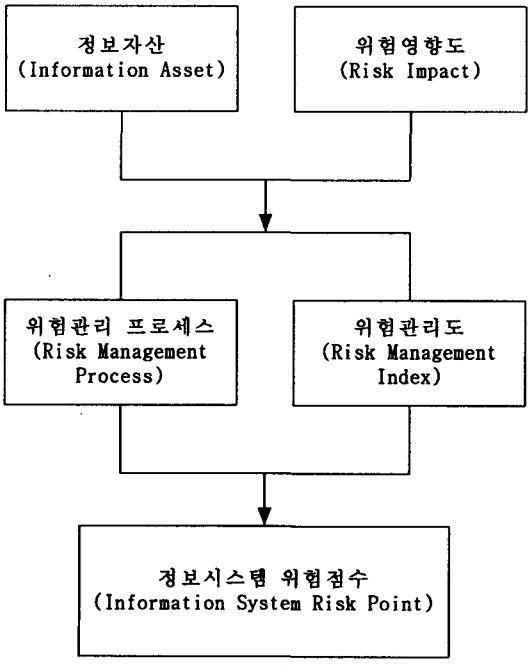
# 3. 정보시스템 위험분석 제안모델

## 3.1 위험분석 제안모델

본연구는 위험분석 제안모델을 통하여, 기존 연구들의 한계점을 수용하는 평가모델을 개발하기 위해서 다음과 같은 요구사항을 고려하여 제안모델을 도출하였다.

첫째, 환경변화에 유연하게 대응하는 평가모델이어야 한다.
둘째, 자산가치를 고려한 종합적인 평가를 수행해야 한다.
셋째, 시스템 개선방향을 제시해야 한다.

위 세가지 요수사항을 기준으로 본 연구에서는 정보시스템 위험을 체계적으로 관리하고, 종합적 분석하기 위한 복합적인 접근방법(Combined Approach)인 위험점수모델을 제시하고자 한다.




< 그림 1 > 정보시스템 위험점수 제안모델

위험점수 모델은 위험분석 모델로서 위험분석에 적용되는 개념적인 틀에서 출발하여 체계적인 접근과 분석을 위한 지침으로 활용하기 위한 것이다. 위 < 그림 1 >에서 보는 것과 같이 위험점수 제안모델은 보호대상인 정보자산의 식별 · 분석을 통해 위험영향도(Risk Impact)를 산정해내고, 그러한 위험관리 프로세스 평가를 통해서 관리되고 있는 위험관리 프로세스 평가에 의해 위험관리도(Risk Management Index)를 산정해내고, 최종적으로 정량적인 위험점수모델(Risk Point Model)을 제시하였다. 그리고, 위험영향도는 위험요소 발생가능성에 대한 정보시스템 조직에 영향을 끼치는 수준을 의미하며, 위험관리도는 정보시스템 조직관리 프로세스의 수준을 의미한다.

## 3.2 정보자산분석에 의한 위험영향도 산정

정보자산 가치 평가는 위험분석대상 정보시스템과 관련 있는 모든 자산을 조사하고 이들 자산들의 가치를 산정하는 과정이다. 그리고 정보시스템 자산을 유형 및 가치별로 분류하는 작업도 병행하고, 정보시스템 관리자 및 사용자는 위험점수기준에 비추어 보아 영향(Impact)을 적게 받을 것으로 판단되는 정보시스템자산은 분석대상에서 제외시킬 수도 있다.

기존의 위험분석 방법론은 자산분석 시 절차상의 복잡함, 평가의 어려움, 위험관리 정책의 부재 때문에 전문적인 업체 및 외주를 통한 평가를 해왔으나 위험점수모델에서는 이를 벗어나 정보시스템 관리자 및 사용자에 의해 위험도를 측정하는 방식으로 대안을 제시하는 것으로서 정보시스템 유형에 따른 위험점수 모델의 예측능력과 활용성을 높이기 위해서는 우선적으로 해당 정보시스템의 정확한 자산 분류 및 영향도를 산정해야만 한다.

분석 대상 정보시스템이 명확하게 정의되고, 외부 시스템과의 구분이 분명해진 상태에서 IT자산, 비IT자산, 인간, 무형자산의 4가지 유형으로 자산을 분류한다.

정보자산 가치 평가에 의한 손실영향지수 단계는 위험점수모델에서 가장 중요한 프로세스로 분류된 정보자산에 따라 위험 영향도를 산정하는 작업이다.

정보자산 가치 산정은 자산의 화폐가치를 이용하여 정량적으로 산출하는 방법이 있고 화폐가치로 산출이 어려운 자산들은 정해진 상수나 기술변수(Descriptive Variable: 예) 상, 중, 하)등을 부과하여 정성적으로 산출하는 방법이 있다.

위험점수모델의 위험영향도 산정에서는 정보시스템 관련 자산들에 대한 일관적인 기준을 제시하고 위험영향도를 산출해내기 위하여 업무중지, 해킹 등으로부터 발생 가능한 조직 내의 자산의 피해액을 기준으로 정성가치를 평가하여 영향지표를 측정한다. 이와 같이 업무중지, 해킹 등으로 인한 영향을 분석하는 것을 업무영향분석(BIA : Business Impact Analysis)이라고 한다.

< 표 1 >에서와 같이 자산별 정성가치 계산유형에 대해 < 표 2 >~< 표 4 >와 같이 각 자산유형별 정성가치 위험평가기준을 정의하였다.

여기서 제시한 정성가치 평가기준은 평가대상 정보시스템의 위험대책, 평가정책 및 조직의 매출규모에 따라 측정스케일 및 기본 변수(비용)에 대한 변동이 가능하다.

< 표 1 > 위험점수모델의 정보자산 분류 및 계산유형

| 자산 | | 계산유형 |
|---|---|---|
| 자산유형 | 세부자산항목 | |
| 1. IT자산 | 1.1 응용 | <표 A> |
| | 1.2 시스템 S/W | <표 A> |
| | 1.3 서버시스템 | <표 A> |
| | 1.4 보조장비 | <표 A> |
| | 1.5 네트워크시스템 | <표 A> |
| | 1.6 컨텐츠 | <표 B> |
| 2. 인간 | 2.1 사용자 | <표 C> |
| | 2.2 응용담당자 | <표 C> |
| | 2.3 IT 담당자 | <표 C> |
| 3. 비IT자산 | 3.1 사무기 | <표 A> |
| | 3.2 설비 | <표 A> |
| | 3.3 문서자료 | <표 B> |
| 4. 무형자산 | 4.1 비즈니스협력관계 | <표 A> |
| | 4.2 노하우 | <표 A> |
| | 4.3 지재권 | <표 A> |
| | 4.4 명성 | <표 A> |

< 표 2 > H/W, S/W 및 IT 자산 위험영향도 수준(계산유형 A)

| 영향도 (Impact) | 등급화 기준 (평가대상기관의 자산규모, 매출규모에 따라 금액을 조정함) |
|---|---|
| 0 (매우낮음) | 금전적 손실이 적거나 없는 수준의 금액 (예 : 조직의 자산규모의 5%) |
| 0.25 (낮음) | 최소한의 금전적 손실을 야기하는 수준의 금액 (예 : 조직의 자산규모의 10%) |
| 0.5 (중간) | 보통의 금전적 손실을 야기하고 비즈니스 프로세스에 부정적인 영향을 미치는 수준의 금액 (예: 조직의 자산규모의 20%) |
| 0.75 (높음) | 심각한 손실을 야기하고 비즈니스 프로세스가 실패가 되는 수준의 금액 (예: 조직의 자산규모의 30%) |
| 1 (매우높음) | 개별 또는 조직에 막대한 손실을 입히는 수준의 금액 (예: 조직의 자산규모의 50%) |

< 표 3 > 데이터 및 무형 자산 위험영향도 수준(계산유형 B)

| 영향도 (Impact) | 등급화 기준 (평가대상기관의 자산규모, 매출규모에 따라 금액을 조정함) |
|---|---|
| 0 (매우낮음) | 기밀성/무결성/가용성이 중요하지 않은 데이터로 금전적 손실이적거나 없음 (예 : 조직의 자산규모의 5%) |
| 0.25 (낮음) | 기밀성/무결성/가용성이 그다지 중요하지 않은 데이터로 최소한의 금전적 손실을 야기함 (예 : 조직의 자산규모의 10%) |
| 0.5 (중간) | 기밀성/무결성/가용성의 중요도가 보통인 데이터로 심각한 금전적 손실을 야기하고 비즈니스 프로세스에 부정적인 영향을 미침 (예: 조직의 자산규모의 20%) |
| 0.75 (높음) | 기밀성/무결성/가용성의 중요도가 비교적 높은 데이터로 매우 심각한 손실을 야기하고 비즈니스 프로세스가 실패함 (예: 조직의 자산규모의 30%) |
| 1 (매우높음) | 기밀성/무결성/가용성의 중요도가 매우 높은 데이터로 개별 또는 조직에 막대한 손실을 입힘 (예: 조직의 자산규모의 50%) |

< 표 4 > 인간 자산 위험영향도 수준(계산유형 C)

| 영향도 (Impact) | 등급화 기준 (평가대상기관의 자산규모, 매출규모에 따라 금액을 조정함) |
|---|---|
| 0 (매우낮음) | 금전적 손실이 적거나 없는 수준 (예: 업무 차질 없음) |
| 0.25 (낮음) | 최소한의 금전적 손실을 야기하는 수준 (예: 업무 75%가동) |
| 0.5 (중간) | 보통의 금전적 손실을 야기하고 비즈니스 프로세스에 부정적인 영향을 미치는 수준 (예: 업무 50% 가동) |
| 0.75 (높음) | 심각한 손실을 야기하고 비즈니스 프로세스가 실패가 되는 수준 (예: 업무 25% 가동) |
| 1 (매우높음) | 개별 또는 조직에 막대한 손실을 입히는 수준 (예: 업무중단) |

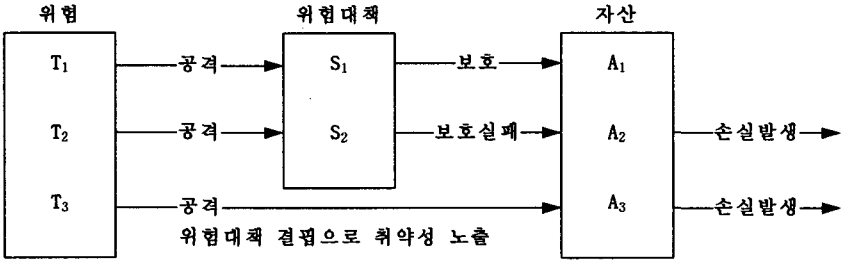
위험영향도 산정의 목적은 일반적인 위험분석 방법론에서 사용하는 정보자산분류에 의한 화폐가치 측정이 아닌 자산유형에 따른 위험영향도를 측정하는 것이므로, < 표 2 >~< 표 4 >와 같이 영향도를 5점 척도에 의해서 각 0, 0.25, 0.5, 0.75, 1로 영향정도를 주관적으로 점수화 하였다.

## 3.3 프로세스 평가에 의한 위험관리도 산정

특정 정보시스템에 취약성이 존재하여 바로 손실을 입지는 않지만, 이는 위협요소들이 침입할 수 있는 근거를 제공하게 된다. 위험관리 프로세스 평가의 목적 역시 손실의 양을 산정하는 것이 아니라 해당 정보시스템이 어느 정도의 위험관리 프로세스를 가지고 있으며 그에 따른 위험요소의 양을 얼마나 내재하고 있는가를 산정하는 것이고, 그에 따라 위험관리도를 산정하게 된다.

아래 < 그림 2 >은 위협공격에 노출되어 있는 시스템의 상태로서 위험점수 모델에서의 취약성 개념을 나타낸 것이다.

위협 $T_1$이 자산 $A_1$을 공격했을 때, 자산 $A_1$은 보안대책 $S_1$에 의해서 보호된다. 위협 $T_3$가 자산 $A_3$을 공격했을 때는 위험대책이 없어서 손실이 발생되는 경우이다. 그러나 위협 $T_2$가 자산 $A_2$를 공격했을 때, 자산 $A_2$는 위험대책 $S_2$ 에 약점이 있어서 보호되지 못한다. 이와 같은 확률을 실제 정성적으로 측정하기는 어렵다. 그러므로 위험점수 모델에서는 정보시스템의 위험관리 프로세스를 평가하고 그에 따른 위협 및 취약성을 통하여 위험관리도를 산정하는데 있으므로, 취약성 개념을 위험대책시스템 내의 약점으로 인해 보호 실패되는 경우와 같이 위험대책의 결핍상태로 정의하여 취약성 및 위협 평가를 한다.




< 그림 2 > 취약성 모형

만일 위험점수모델에서 취약성을 앞에서 설명한 취약성의 첫 번째 개념인 '자산의 속성'으로만 정의하면, 취약성을 정성적으로나 계량적으로 평가하기가 어렵다. 또한 두 번째 개념인 '자산과 위협의 관계'로 정의하면, 관계에 대한 구체적 모형이 제시되어야 하는데, 그러기 위해선 자산과 위협의 관계에 대한 구체적 모형이 제시되어야 한다.

그러나 정량적인 평가모형을 도출하더라도 실증적으로 적용하는 데는 위협발생 혹은 손실발생에 대한 확률추정을 해야 하는데, 이에 대한 과거자료를 확보한다는 것은 사실상 어려운 문제이다. 그러므로 위험점수모델에서는 취약성을 위험대책의 결핍상태로 정의하고, 위험관리 프로세스를 평가하여 위험관리도를 도출한다.

위험점수모델의 위험관리도 산정에서는 조직 내 취약성 및 위협 평가를 위하여 위험관리 프로세스 체크리스트를 이용하여 실시한다.

위험관리 프로세스 체크리스트 항목은 ISACA(국제시스템감사통제협회)가 정보시스템 감사의 세부적 지침 마련을 위해 개발한 COBIT(Control Objectives for Information and related Technology)를 이용하여 작성하였다.

위험관리 프로세스 체크리스트의 목적은 정보시스템 자산의 특정 위협을 통해 발생하는 공격에 대한 취약성을 평가하고 그에 따른 위험도를 산정하는 것이다.

또한, 보안대책의 유무를 묻는 질문들로 구성되어 있어, 보안대책의 제시까지도 가능해 지게 되는 장점이 있다. 그러므로 정보시스템 관리자 및 사용자는 최종 위험점수를 산정 후 위험대책에 소요되는 비용과 위험대책의 효과를 비교한 후에 최선의 대책을 선택할 수 있다.

< 표 5 > 위험관리 프로세스

| 위험관리 업무영역 | 번호 | 상세 프로세스 | 세부활동 항목 수 |
|---|---|---|---|
| 계획 및 조직 | P1 | 위험관리 정책 개발 | 5 |
| | P2 | 위험관리 정책 유지관리 | 4 |
| | P3 | 조직관리 | 3 |
| | P4 | 인적자원관리 | 3 |
| | P5 | 상위위험분석 | 4 |
| | P6 | 기본통제분석 | 3 |
| | P7 | 상세위험분석 | 5 |
| | P8 | 위험대책 선정 | 7 |
| 획득 및 구현 | A1 | 공급자 선정 | 3 |
| | A2 | 공급자 모니터링 | 3 |
| | A3 | 위험대책 구현 | 6 |
| 운영 및 지원 | O1 | 위험사고관리 | 5 |
| | O2 | 유지보수 | 3 |
| | O3 | 형상관리 및 변경관리 | 4 |
| | O4 | 문서화 | 7 |
| | O5 | 문제해결 | 6 |
| | O6 | 훈련 및 교육 | 3 |
| 통제 | C1 | 위험감사 | 4 |
| | C2 | 모니터링 | 4 |
| | C3 | 프로세스 관리 | 7 |

정보시스템 위험관리 목표를 달성하기 위해 위험관리 프로세스를 수행하며 위험관리 프로세스를 평가하는 것이 곧 위험도를 평가하는 것으로서 위험분석모델의 체크리스트의 평가항목은 위 < 표 5 >과 같이 총 4개의 위험관리 업무영역에 대하여 20개의 상세 프로세스를 도출하였으며 각 위험관리 업무영역 별 목적 및 상세 프로세스는 다음과 같다.

위험관리 업무영역 내 각 상세프로세스 항목에서 세부활동의 활용도에 대한 가중치는 매우 높음(VH), 높음(H), 보통(M), 낮음(L), 매우낮음(VL)의 5점 척도에 의해서 각 1, 0.75, 0.5, 0.25, 0로 중요성 정도를 주관적으로 점수화 하였으며, 모든 질문은 예, 아니오, 해당사항 없음(또는 적용불가) 등 3가지 중에서 하나에만 응답하도록 되어 있다.

먼저, 조정 전 위험관리도(Unadjusted Risk Management Index)는

$$\mathbf{URMI} = \sum\{(\text{가중치 } i\text{가 부여된 항목 중 응답 항목수}) \times \text{가중치}\}$$

$$= \{NY(VH) \times 1 + NY(H) \times 0.75 + NY(M) \times 0.5 + NY(L) \times 0.25 + NY(VL) \times 0\} \text{----(3.1)}$$

여기서 NY는 정보보호분야 가중치별 항목의 응답한 항목 수이다.

그리고 최종적으로 실제 응답한 항목 수의 타당성 및 위험관리도의 일관성을 보장하기 위해서 항목별 점수를 산정하여 조정 후 위험관리도를 산출한다.

조정 후 위험관리도(Adjusted Risk Management Index)는

$$\mathbf{ARMI} = \sum\{(\text{항목별 점수}) \times \mathbf{USI}\} = \sum(\mathbf{YT/NT}) \times \mathbf{USI} \text{--------(3.2)}$$

여기서 YT는 상세프로세스별 항목의 응답한 항목수이고, NT는 상세프로세스별 질의 항목 수이다.

## 3.4 위험점수 산정

제안된 위험점수모델에 대한 점수를 산정하고, 해당 정보시스템이 어느 정도의 위험도를 가지고 있는가를 평가하는 것이다. 그리고, 아래 식(3.3)에서와 같이 위험점수는 낮을수록 정보시스템 조직구성요소에 대한 영향이 작음을 의미하며, 위험수준에 대한 관리 방법은 정보시스템 기업 조직의 상황에 따른 관리 표준이 설정되어야 할 것이다. 앞서 위험점수를 산정하기 위해 정보자산분석에 의한 위험영향도를 산정하고, 위험관리 프로세스 평가에 의한 위험관리도(RMI)를 산정하였다.

이에 정보시스템 자산에 취해지는 모든 위협 및 취약성, 운영되고 있는 위험대책을 고려함으로서 분석 대상 시스템에 발생할 수 있는 위험에 대한 점수화가 가능해 지며, 제안 모델에서는 다음과 같이 구한다.

$$\text{위험점수}(RP) = \frac{\text{위험영향도}(RI)}{\text{위험관리도}(RMI)} \text{----------(3.3)}$$

# 4. 위험분석 제안모델 사례연구

위험점수 모델의 목적은 조직의 정보시스템의 위험도를 종합적이고, 객관적으로 평가할 수 있는 모델을 개발하는 것이다. 그러나 기업을 비롯한 국내 대부분의 조직들은 위험관리에 대한 인식이 낮기 때문에 기존의 위험분석 데이터 수집의 어렵고, 조직에 직접 적용하여 모델의 적합성을 검증하는 것이 어렵다. 따라서 기존의 위험관리 소프트웨어 정보시스템 관리자들의 설문을 수집하여 모델의 적합성을 검증하도록 하였다. 본 연구에서의 사례기업은 20~25정도의 중소 IT 정보시스템 조직을 구성하고 있으며, Mobile 시스템과 IDC(Internet Data Center) 서비스 개발 회사이다. 이 기업을 통해서 Mobile 시스템과 IDC 시스템의 위험영향도를 측정하였다.

## 4.1 위험영향도 평가

< 표 6 > 정보자산 위험영향도 조사

| 자산 | | 위험영향도 | |
|---|---|---|---|
| 자산유형 | 세부자산목록 | Mobile 서비스 | IDC 서비스 |
| 1. IT자산 | 1.1 응용 | 0.25 | 0 |
| | 1.2 시스템 S/W | 1 | 0.75 |
| | 1.3 서버시스템 | 0.75 | 1 |
| | 1.4 보조장비 | 0 | 0.5 |
| | 1.5 네트워크시스템 | 0.25 | 0.5 |
| | 1.6 컨텐츠 | 0.25 | 0.25 |
| 2. 인간 | 2.1 사용자 | 0 | 0.25 |
| | 2.2 응용담당자 | 0.5 | 0.5 |
| | 2.3 IT 담당자 | 0.25 | 0.75 |
| 3. 비IT자산 | 3.1 사무기 | 0 | 0.25 |
| | 3.2 설비 | 0.5 | 0.5 |
| | 3.3 문서자료 | 0.25 | 0.25 |
| 4. 무형자산 | 4.1 비즈니스협력관계 | 0.75 | 0 |
| | 4.2 노하우 | 0.5 | 0.75 |
| | 4.3 지재권 | 0.5 | 0.5 |
| | 4.4 명성 | 0.25 | 0.25 |
| 합계 | | 6 | 7 |

위 < 표 6 >에서는 중소 IT 정보시스템 조직을 구성하고 있는 Mobile 시스템과 IDC(Internet Data Center) 서비스 개발 회사를 사례로서 < 표 1 >~< 표 4 >에서 제시한 자산 유형에 따른 평가방법을 통하여 위험영향도를 측정하였다.

## 4.2 위험관리도 평가

< 표 7 > 조정 전·후 위험관리도(URMI) 조사

| 상세 프로세스 | 매우 높음 (VH) | 높음 (H) | 보통 (M) | 낮음 (L) | 매우 낮음 (VL) | URMI |
|---|---|---|---|---|---|---|
| 가중치 | 1 | 0.75 | 0.5 | 0.25 | 0 | |
| P1 | 1 | 1 | 1 | 0 | 0 | 2.25 |
| P2 | 0 | 2 | 0 | 1 | 0 | 1.75 |
| P3 | 0 | 1 | 1 | 0 | 0 | 1.25 |
| P4 | 0 | 0 | 1 | 0 | 2 | 0.50 |
| P5 | 0 | 0 | 2 | 1 | 1 | 1.25 |
| P6 | 2 | 0 | 1 | 0 | 0 | 2.50 |
| P7 | 0 | 2 | 1 | 1 | 0 | 2.25 |
| P8 | 3 | 1 | 1 | 0 | 1 | 4.25 |
| A1 | 0 | 0 | 1 | 1 | 1 | 0.75 |
| A2 | 0 | 0 | 1 | 1 | 1 | 0.75 |
| A3 | 1 | 2 | 1 | 1 | 0 | 3.25 |
| O1 | 1 | 1 | 1 | 0 | 0 | 2.25 |
| O2 | 0 | 1 | 1 | 0 | 0 | 1.25 |
| O3 | 0 | 0 | 1 | 1 | 0 | 0.75 |
| O4 | 0 | 2 | 1 | 0 | 1 | 2.00 |
| O5 | 0 | 1 | 3 | 1 | 1 | 2.50 |
| O6 | 1 | 1 | 0 | 0 | 0 | 1.75 |
| C1 | 2 | 1 | 1 | 0 | 0 | 3.25 |
| C2 | 0 | 1 | 2 | 1 | 0 | 2.00 |
| C3 | 0 | 1 | 0 | 1 | 2 | 1.00 |
| 합계 | 11 | 18 | 21 | 10 | 10 | 37.50 |

| 상세 프로세스 | 매우 높음 (VH) | 높음 (H) | 보통 (M) | 낮음 (L) | 매우 낮음 (VL) | URMI |
|---|---|---|---|---|---|---|
| 가중치 | 1 | 0.75 | 0.5 | 0.25 | 0 | |
| P1 | 1 | 0 | 2 | 1 | 0 | 0.25 |
| P2 | 1 | 0 | 1 | 1 | 1 | 1.75 |
| P3 | 0 | 1 | 1 | 1 | 0 | 1.50 |
| P4 | 0 | 2 | 1 | 0 | 0 | 2.00 |
| P5 | 0 | 1 | 1 | 0 | 1 | 1.25 |
| P6 | 2 | 1 | 0 | 0 | 0 | 2.75 |
| P7 | 0 | 2 | 1 | 0 | 1 | 2.00 |
| P8 | 2 | 1 | 1 | 1 | 0 | 3.50 |
| A1 | 0 | 1 | 1 | 0 | 0 | 1.25 |
| A2 | 0 | 1 | 1 | 1 | 0 | 1.50 |
| A3 | 2 | 2 | 0 | 0 | 0 | 3.50 |
| O1 | 2 | 1 | 0 | 0 | 0 | 2.75 |
| O2 | 0 | 2 | 0 | 1 | 0 | 1.75 |
| O3 | 1 | 1 | 1 | 0 | 1 | 2.25 |
| O4 | 1 | 2 | 1 | 1 | 1 | 3.25 |
| O5 | 1 | 2 | 1 | 0 | 1 | 3.00 |
| O6 | 1 | 2 | 0 | 0 | 0 | 2.50 |
| C1 | 2 | 1 | 1 | 0 | 0 | 3.25 |
| C2 | 1 | 2 | 0 | 0 | 0 | 2.50 |
| C3 | 2 | 0 | 1 | 2 | 1 | 3.00 |
| 합계 | 19 | 25 | 15 | 9 | 7 | 47.50 |

위 < 표 7 >에서는 식 (3.1)과 (3.2)를 통하여, 위험관리 프로세스 평가에 의한 조정 전·후 위험관리도(URMI) 조사 결과를 나타내고 있다. 조종 후 위험관리도(ARMI)는 최종적으로 실제 응답한 항목 수의 타당성 및 위험관리도의 일관성을 보장하기 위해서 항목별 점수를 산정하여 조정 후 위험관리도를 산출한 것이다.

< 표 8 > 조정 전 위험관리도(URMI)

| 상세 프로세스 | 질문 항목수 | 응답 항목수 | 항목별 점수 | UR MI | AR MI |
|---|---|---|---|---|---|
| P1 | 5 | 3 | 3/5=0.60 | 2.25 | 1.35 |
| P2 | 4 | 3 | 3/4=0.75 | 1.75 | 1.31 |
| P3 | 3 | 2 | 2/3=0.67 | 1.25 | 0.84 |
| P4 | 3 | 2 | 2/3=0.67 | 0.50 | 0.34 |
| P5 | 4 | 4 | 4/4=1.00 | 1.25 | 1.25 |
| P6 | 3 | 3 | 3/3=1.00 | 2.50 | 2.50 |
| P7 | 5 | 4 | 4/5=0.80 | 2.25 | 1.80 |
| P8 | 7 | 6 | 6/7=0.86 | 4.25 | 3.66 |
| A1 | 3 | 3 | 3/3=1.00 | 0.75 | 0.75 |
| A2 | 3 | 3 | 3/3=1.00 | 0.75 | 0.75 |
| A3 | 6 | 5 | 5/6=0.84 | 3.25 | 2.73 |
| O1 | 5 | 3 | 3/5=0.60 | 2.25 | 1.35 |
| O2 | 3 | 2 | 2/3=0.67 | 1.25 | 0.84 |
| O3 | 4 | 2 | 2/4=0.50 | 0.75 | 0.38 |
| O4 | 7 | 4 | 4/7=0.57 | 2.00 | 1.14 |
| O5 | 6 | 6 | 6/6=1.00 | 2.50 | 2.50 |
| O6 | 3 | 2 | 2/3=0.67 | 1.75 | 1.17 |
| C1 | 4 | 4 | 4/4=1.00 | 3.25 | 3.25 |
| C2 | 4 | 4 | 4/4=1.00 | 2.00 | 2.00 |
| C3 | 7 | 4 | 4/7=0.57 | 1.00 | 0.57 |
| **합계** | **89** | **69** | **69/89 =0.78** | **37.50** | **29.25** |

< 표 9 > 조정 후 위험관리도(ARI) 조사

| 상세 프로세스 | 질문 항목수 | 응답 항목수 | 항목별점수 | URMI | ARMI |
|---|---|---|---|---|---|
| P1 위험관리 정책 개발 | 5 | 4 | 4/5=0.80 | 0.25 | 0.20 |
| P2 위험관리 정책 유지관리 | 4 | 4 | 4/4=1.00 | 1.75 | 1.75 |
| P3 조직관리 | 3 | 3 | 3/3=1.00 | 1.50 | 1.50 |
| P4 인적자원관리 | 3 | 3 | 3/3=1.00 | 2.00 | 2.00 |
| P5 상위위험분석 | 4 | 3 | 3/4=1.75 | 1.25 | 2.19 |
| P6 기본통제분석 | 3 | 3 | 3/3=1.00 | 2.75 | 2.75 |
| P7 상세위험분석 | 5 | 4 | 4/5=0.80 | 2.00 | 1.60 |
| P8 위험대책선정 | 7 | 5 | 5/7=0.71 | 3.50 | 2.49 |
| A1 공급자 선정 | 3 | 2 | 2/3=0.67 | 1.25 | 0.84 |
| A2 공급자 모니터링 | 3 | 2 | 2/3=0.67 | 1.50 | 1.01 |
| A3 위험대책 구현 | 6 | 4 | 4/6=0.67 | 3.50 | 2.35 |
| O1 위험사고관리 | 5 | 3 | 3/5=0.60 | 2.75 | 1.65 |
| O2 유지보수 | 3 | 3 | 3/3=1.00 | 1.75 | 1.75 |
| O3 형상관리 및 변경관리 | 4 | 3 | 3/4=0.78 | 2.25 | 1.76 |
| O4 문서화 | 7 | 6 | 6/7=0.86 | 3.25 | 2.80 |
| O5 문제해결 | 6 | 5 | 5/6=0.83 | 3.00 | 2.49 |
| O6 훈련 및 교육 | 3 | 3 | 3/3=1.00 | 2.50 | 2.50 |
| C1 위험감사 | 4 | 4 | 4/4=1.00 | 3.25 | 3.25 |
| C2 모니터링 | 4 | 3 | 3/4=0.75 | 2.50 | 1.88 |
| C3 프로세스 관리 | 7 | 6 | 6/7=0.86 | 3.00 | 2.58 |
| 합계 | 89 | 73 | 73/89=0.82 | 47.50 | 38.95 |

## 4.3 위험점수 산정

< 표 10 > 시스템 별 위험점수(Risk Point) 산정

| 시스템 | 위험영향도 (RI) | 위험관리도 (RMI) | 위험점수 (Risk Point) |
|---|---|---|---|
| Mobile 서비스 | 6 | 29.25 | 0.21 Point |
| IDC 서비스 | 7 | 38.95 | 0.18 Point |

본 연구에서의 위험점수 분석 제안모델을 통해서 < 표 10 > 시스템 별 위험점수(Risk Point)가 산정되었다. 결과적으로 Mobile 서비스 0.21, IDC 서비스 0.18 수준으로서 정보시스템 자산가치를 고려한 정보시스템 관리프로세스의 위험노출 수준은 Mobile 서비스가 IDC 보다 높은 것으로 판단할 수 있기 있다. 이에 대한 차후 관리 노력이 더 필요하다는 것을 알 수 있다.

## 5. 결론 및 제언

정보화에 따른 정보의 의존도가 심화됨에 따라 정보시스템의 취약성 및 위협에 의한 위험을 방지하기 위한 심층적 위험분석 방법론이 요구된다. 이에 따라서 본 논문에서는 개선된 위험분석의 전체흐름을 제시하여 일반적인 환경에 적용하기 쉽고 실용적으로 활용할 수 있는 위험점수 모델을 제시하였다.

본 모델은 초기시스템 구축 시에는 전체위험분석에 사용이 가능하며, 이후 위험관리 프로세스 구축 또는 기존 시스템 위험관리 재구축 후 재분석이 필요할 시에는 잔류위험 평가 피드백과 중복된 대응책 및 위험대책 식별에 사용이 가능하여 위험관리 프로세스 예산의 낭비를 방지할 수 있다. 특히, 자산별 위험영향도를 식별 프로세스를 통해 조직의 핵심 정보시스템 자산 식별 및 관리가 가능하고, 불필요한 대응책을 구현하지 않도록 하여 경제적인 대응책의 구현이 이루어 질 수 있도록 하여 기존 위험분석 방법론의 단점을 개선하였다. 하지만, 본 모델은 제한적인 검증만 이루어 진 것이므로 앞으로 다각적인 위험관리 프로세스 환경과 구체적인 검증이 필요하다. 또한 충분한 검토를 통하여 위협이나 대응책의 산출 시 필요한 다양한 위험관리 프로세스 평가 체크리스트의 개발이 필요하며, 효율적인 자동화 방안이 연구되어야 할 것이다.

## 6. 참 고 문 헌

[1] 김현수, 정보시스템 진단과 감리, 법영사, 2002, p92-95

[2] "Governace, Control and Audit for Information and Related Technology", ISACA Korea, 2003

[1] B.D. Jenkins, "Security Risk Analysis and Management," Countermeasures, Ins., 1998.

[2] "Information Technology-Security Techniques-Guidelines for The Management of IT Security," ISO/IEC JTC 1/SC 27, 1997

[3] Ginzberg, M. J. and Moulton, R.T., "Information Technology Risk Management," 'Next Decade in Information Technology,' Proceedings of The 5th Jersusalem C onference, pp602-608, 1990.

[4] Harold F. Tipton and Micki Krause, "Information Security Management Volume 3," 4th Edition, Auerbach Publications, pp.417-430, 2002

[5] "Risk Analysis and Management Standards for Public Information Systems Sec urity-Concepts and Models," 한국정보통신기술협회(TTA), 1998

[6] "Risk Analysis and Management Standards for Public Information Systems Sec urity-Risk Analysis Methodology Model," 한국정 보통신기술협회(TTA), 2000

[7] "Information Technology-Security Techniques-Guidelines for The Management of IT Security," ISO/IEC JTC 1/SC 27, 1997
[8] "Information Technology-Security Techniques-Guidelines for The Management of IT Security," ISO/IEC JTC 1/SC 27, 1997/"BS7799-Gide to Risk Assessment and Risk Management," BSI, 1998.
[9] "A Guide to Security Risk Management for Information Technology Systems," MG-2, CSE Manual, 1996.
[10] "A Guide to Risk Assessment and Safeguard Selection for Information Technol ogy," MG-2, CSE Manual, 1996

## 저 자 소 개

조 두 호 : 명지대학교 산업공학 석사, 현재 한국전산원 차세대인터넷팀 선임연구원, 관심분야는 정보시스템 보안, 감사, 시스템분석 및 소프트웨어 기능점수 측정

서 장 훈 : 명지대학교 산업공학박사, 아주대 경영대학원 MBA, 현재 Ubipia SI 사업부 수석컨설턴트, 한국능률협회컨설팅(KAMC) 컨설턴트, 관심분야는 BPM, 6시그마, IT 프로세스 평가, 정보시스템 감사, 정보시스템 품질