새로운 경영관리 기법으로 ERM의 개념과 적용방안에 대한 연구

최세업*, 김진경*, 이창국*
*㈜LG CNS 컨설팅부문

The Study of Enterprise Risk Management as a New Corporate Management Approach : Concept and Implementation

Choi, Seh eob *, Kim, Jin Kyung *, Lee, Chang Kook *
LG CNS Consulting Division
E-mail : sechoi@lgcns.com, jinkkim@lgcns.com, leeck@lgcns.com

요 약

현재의 경영환경은 기업경영에 긍정적 또는 부정적인 영향을 미칠 Event가 다양하고 예측이 어려워지고 있는 상황에 직면하고 있다. 반면에 각종 경영상의 규정과 규제는 주주와 시장의 입장에서 기업의 경영의 투명성과 신뢰성을 요구하고 있다. 대표적으로 금융산업은 Basel II, 미국증시에 상장된 기업은 SOA라 불리는 Sarbanes-Oxley법안, 국내기업은 집단소송제, 외감법, 증권거래법 등에 기업의 경영 성과와 재무제표에 대한 경영진의 서명 및 외부감사인의 검토를 규정하고 있다. 경영진은 전략적인 목적 달성에 영향을 미치는 내외부에서 발생하는 상황과 규정/규제에 대한 대응현황을 종합적으로 판단해야만 하게 되었다. 이러한 상황에서 2004년 9월 Committee of Sponsoring Organization of the Treadway Commission(이하 COSO)에서는 Enterprise Risk Management Framework을 발표하였다. 이는 기존 내부통제(Internal Control) 개념을 확장/보완한 개념으로 전사적 관점에서 기업에 영향을 미치는 Event를 식별하고 통제하는 일련의 과정을 정의하고 있다. 대부분 기업에서는 법규와 규정중심의 대응을 추진하고 있는 현황이며, 추진 과정시 리스크에 대한 개념이나 관리 수준에 대한 혼란을 격고 있다. 리스크 정의시 일관된 관점을 유지할 수 있는 관리 범주와 관리 목적의 부재를 제기하고 있며, 일회적인 관리가 아닌 정례화된 프로세스로 운영하도록 하는 관리체계 정립을 위한 방법론이나 실행가이드를 필요로 하고 있다. 이에 새로운 관리체계로서 Enterprise Risk Management(이하 ERM) 도입을 위하여 ERM에 대한 명확한 이해와 적용시 주요이슈에 대한 실천적 해결안을 제시하는 것을 본 연구의 목적으로 삼고자 한다

1. 서론

1.1 연구배경

현재의 글로벌 선진 기업의 CEO들은 세계경제 성장율이 둔화되고 있음에도 성장전략을 가속화할 의지를 가지고 있는 것으로 파악되었다. 경영진들은 목표달성을 위해 리스크에 대한 방침을 재점검하고 있으며 경영진들이 말하는 당면한 위험은 경쟁의 심화, 시장 변화에 즉각적인 대응의 어려움, 지속적이며 시장에 매력적인 기술이나 역량을 보유하지 못하는 것을 가장 높게 평가하고 있다. [1] 반면에 시장에서의 각종 경영상 규정과 규제는 주주와 시장의 입장에서 기업 경영의 투명성과 신뢰성을 요구하고 있다. 대표적으로 금융산업은 Basel Ⅱ, 미국증시에 상장된 기업은 Sarbanes-Oxley Act, 국내기업은 증권관련집단소송법, 주식회사의 외부감사에 관한 법률(외감법), 증권거래법 등에 기업의 경영성과와 재무제표에 대한 경영진의 서명 및 외부감사인의 검토를 규정하고 있다. 이에 적절히 대응하지 못하는 경우 경영을 지속할 수 없는 상황에 처하게 되므로 경영진은 전략적인 목적달성에 영향을 미치는 내/외부에서 발생하는 상황과 규정/규제에 대한 대응현황을 종합적으로 판단해야만 하게 되었다. 경영진은 전략적 목표 달성에 영향을 미치는 외부의 변화와 규제에 즉각적으로 대처할 수 있는 체계적인 운영시스템을 갖출 필요성을 느끼고 있으며 PWC (PricewaterhouseCoopers) 조사에 의하면, 미국 CEO 경우 20%만이 전사적 리스크 관리에 필요한 정보를 받고 있다고 한다. [2]

2003년 7월 Committee of Sponsoring Organization of the Treadway Commission(COSO)에서 Enterprise Risk Management Framework Draft를 발표하게 되면서 본격적인 ERM에 대한 논의가 활발해 졌으며, 2004년 9월 COSO에서는 Enterprise Risk Management – Integrated Framework을 정식 발간하였다. 이 프래임워크는 리스크 관리의 구성, 운영 프로세스에 대한 가이드라인을 제시하고 있다. 각 기업에서는 법규 및 규정에 대응하기위한 리스크 관리를 실시하고 있는 실정이며, COSO 프래임워크를 바탕으로 현재의 리스크 관리 체계를 점검하고 정비하고자 하는 움직임을 보이고 있다.

국내 금융산업의 경우 BaselⅡ 대응을 위해 규정에서 정의하고 있는 리스크에 대한 통제 프로세스 구축을 진행중에 있으며, 제조/서비스 산업을 포함한 상장기업들은 외감법에서 요구하는 내부회계 관리제도 운영을 위해 내부회계통제시스템 도입을 하고 있다. 즉 현재 국내 기업들이 전면적인 리스크 관리 체계 운영보다는 법/규제 대응에 우선하고 있음을 알 수 있다. 그러나 이러한 법/규정 대응을 구축한 기업에서는 구축된 체계가 제한적이며, 기업이 처한 리스크에 대한 종합적인 분석 요구가 대두되어 ERM에 대한 도입을 검토하거나 파일럿형식으로 추진하고 있다.

본 연구는 기업들이 한정적인 리스크 범주에 대응하는 법/규제 준수의 한계를 벗어나고, 이를 넘어서 새로운 경영기법의 조류로 ERM을 이해할 수 있도록 개념을 정리하고 적용시 당면하는 이슈들에 대한 실천적인 방안을 제시하고자 한다.

1.2 연구개요

ERM에 대한 개념 정리를 위해 COSO Enterprise Risk Management – Integrated Framework 을 중심으로 관련 문헌을 통해 ERM에 대한 정의, 논의되고 있는 이슈를 검토하여 기업 경영관리기법으로의 활용하기 위한 해석을 하고, 최근 대두되고 있는 내부회계제도, Basel Ⅱ 등 법/규제 대응과의 관계를 정의하여 ERM과 관련 경영이슈에 대한 의견을 제시하고자 한다.

기업경영기법들이 정보기술의 도움없이 수행될 수 없는 현실에 비추어 ERM이 요구하는 정보기술기능 요소와 관련 솔루션과의 관계를 정의하여 정보기술 계획 수립시 참고가 되도록 하고자 한다.

마지막으로 연구 결과로 ERM과 관련한 국내외 시장의 현황과 도입시 이슈 및 합리적인 추진전략

을 제안하고자 한다.

2. 본론

2.1 ERM 정의

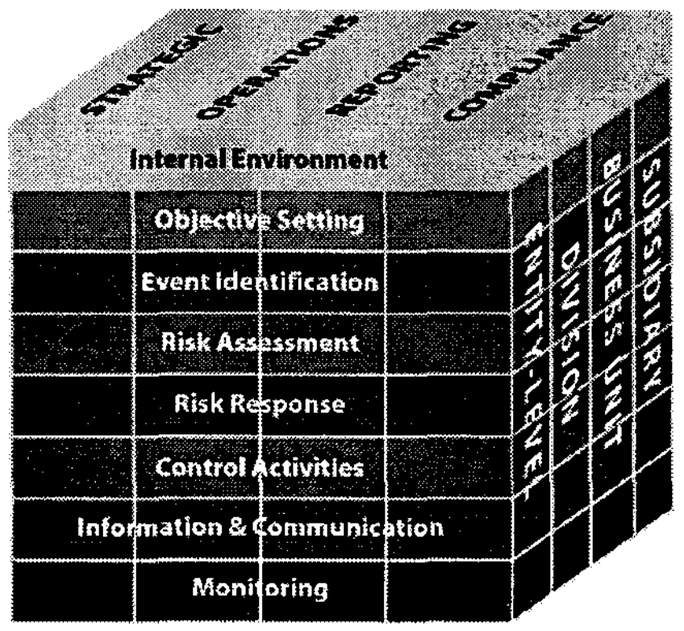
COSO에서는 ERM을 " ERM은 기업전체적인 시각에서 기업에 영향을 미칠 수 있는 잠재적인 위험 및 사건 등을 파악하고, 일정한 취향내에서 위험을 적절하게 관리하며, 기업의 목적을 달성하기 위해 합리적인 대응 방안을 강구하는 프로세스이다. 이는 전사적인 기업전략에 적용되어 명확한 책임주체에 의해 실천되어야 한다"라고 정의하고 있다. 미국 손해보험 협회(Casualty Actuarial Society(CAS))에서는 " 기업의 장단기의 주주가치를 증대하기 위해 모든 유형의 리스크를 평가, 통제, 식별, 재무적 대응, 모니터링하는 모든 기업에 적용되는 프로세스"로 정의하고 있다.

이러한 정의들은 리스크를 바라보는 관점이 기존의 과거 데이타를 취합하여 통계적기법을 통한 분석 결과에 대응하는 수준이 아니라 리스크의 다양성을 인지하고 원인을 찾아 전사적인 관점에서 대응을 하되 경영진의 적극적인 뒷받침을 바탕으로 해야함을 보여주고 있다.

COSO는 AICPA, IIA, FEI, IMA, AAA 등 기업회계, 재무관련 공인 기관들이 스폰서로 참여하는 비영리 조직이다. 이 기관은 1985년 기업이 신뢰할 수 있는 재무정보를 제공할 수 있도록 Governance, Reporting과 관련한 가이드등을 개발하고 있다. 현재 ERM 프래임워크는 2004년 9월 발표된 것으로 기존의 내부통제 개념을 리스크 관리로 확장하여 디자인 한 것이다.

ERM 프래임워크는 목적(objectives), 구성항목(Component), 범위(Level of organization) 3가지 축으로 구성되어있다.[3]

그림 1 – COSO ERM Framework



ERM 체계 구성시 우선적으로 고려되어야 하는 것은 리스크 관리의 목적이 무엇인지를 정의하는 것이다. 목적은 전략달성(Strategic), 운영의 효율성(Operation), 대내외 보고/공시의무(Reporting), 기업경영에 영향을 미치는 법/규제 대응(Compliance)로 구분해 볼 수 있으며 이에 따라 관리해야 하는 리스크의 유형과 관리방안이 결정이 된다.

목적에 따라 관리 체계는 1) 리스크관리에 대한 기업내부 환경 평가 및 조성, 2) 리스크 관리 목표 설정, 3) 리스크를 유발시키는 Event 인식, 4) 리스크 평가, 5) 리스크 대응 방안 도출, 6) 리스트 통제 활동 설계, 7) 리스크 관리를 위한 필요 정보 및 관련 정보기술과 조직내 의사소통체계 구성, 8) 지속적인 모니터링 및 개선활동으로 구성하고 있다. ERM은 체계는 전사수준에서(Corporate-level)에서 구성되어 각 사업단위, 사업장으로 수정/확산하는 형태를 가지게 된다.

COSO 프래임워크의 내재된 개념은 기업문화에 기반을 둔 전사적인 관리체계라 할 수 있다. 첫째, ERM은 업무 프로세스이다. 즉 ERM은 기업 목표 달성을 위한 지속적 프로세스며, ERM 구성요소가 인프라 및 전략에 융합되어 운영되야 효과적이다. 둘째, ERM은 명확한 책임주체에 의한 실천되어야 한다. 성문화된 정책(Policy)이나 규범(Regulation)에 의해서가 아닌, 이사회, 경영자, 직원 등 모든 구성원들에 의해 실천되는 구체적인 활동이 되어야 한다. 셋째, ERM은 기업전략에 적용되어야 한

다. ERM의 궁극적인 목표는 기업의 경영 목적을 달성하는 것이며, ERM의 구성요소들은 기업전략 및 사업전략 등에 반영되어 일관적으로 추진되어야 한다. 넷째, ERM은 기업전체적인 시각에서 정의되어야 한다. 대내외적인 모든 영역에서 발생 가능한 위험들을 전사차원의 시각에서 인식하는 것이 ERM의 기초개념이다. 다섯째, ERM은 잠재적인 위험 파악과 일정한 위험수준 허용하는 것이다. 기업의 경영성과나 가치에 부정적 영향을 주는 잠재적 위험요인을 인식하고, 감당할 수 있는 수준 및 범위에서 존재하도록 효과적으로 관리되어야 한다. 여섯째, ERM은 합리적인 대응방안을 강구한다. 수동적 활동이 아니라 위험을 적절한 수준으로 관리하기 위한 구체적 대응 및 통제방안이 포함된다. 일곱째, ERM은 기업목적 달성을 목표로 해야 한다. 개별 위험을 감소시키는 것이 아니라 기업가치 극대화 같은 기업경영전략목표를 달성하는 것다.

COSO가 ERM 프래임워크를 발표하기 이전의 위험관리 모습은 '70~'80년대 방어적 관리개념에서 제조업의 경우 손실방지 및 전가에 초점을 맞추어 신용관리, 투자 및 부채정책과 감사 프로세스 수립을 하였으며, 금융기관은 ALM(Asset & Liability Management) 중심의 금리 및 환율관리에 따른 손실최소화 위주였다.

'90년대엔 통제지향적 관리 형태로 발전하여 제조업은 사업 및 재무적 결과에 대한 Volatility관리 위주로, 금융업은 ALM을 중심에서 Basel Ⅰ안에 따른 시장위험을 감안한 BIS 비율관리로 변하였으나, Operation에 의한 위험이나 Reporting의 신뢰성 달성을 고려한 위험에 대한 관리개념은 부족하였다. COSO는 이러한 부족한 개념을 보충하고, 기업이 직면한 위험요인에 대한 전사적 관리 체계를 완성하였다고 볼 수 있다. 현재까지 ERM을 실천하기 위해 발표된 회계법인, IT 리서치 기관, 컨설팅기업에서 발표한 프래임워크나 방법론들도 COSO 프래임워크를 기반으로 하고 있다. COSO 프래임워크는 현재까지 ERM에 관한 가장 표준이 된다 하겠다.

ERM의 기대효과로는 Event 발생 시 충격과 손실을 줄이는 효과뿐만 아니라 리스크를 전략과 연계하여 의사결정의 효율화를 제고하고 새로운 가치의 기회를 포착하여 궁극적으로는 기업의 가치 창출로 볼 수 있다. 첫째 전략과 리스크를 연계함으로써 전략수행에 따른 위험을 미리 정해둔 Tolerance내로 한정시키고 발생가능한 리스크를 미리 인식함으로써 전략 수행 성공확률을 향상시키며, 둘째, 리스크가 발생하였을 경우 사전에 리스크에 대응하는 시나리오를 설정해 놓음으로써 의사결정 능력의 질을 높일 수 있으며, 셋째로 리스크를 조기에 발견하고 대응전략을 설정함에 따라 실제 리스크 발생시 충격을 완화할 수 있으며, 넷째로 조직원들 자신이 하는 업무에서 발생하는 리스크에 대해 상시적으로 자각하여 회사 전체적인 리스크 관리문화가 정착되고 궁극적으로 관리수준이 향상되며, 다섯째로 ERM은 리스크만을 도출/관리하는 것이 아니라 Event를 관리함으로써 내, 외부 요인에 의해 발생하는 기회를 포착, 전략에 반영함으로써 새로운 수익원을 창출할 수 있도록 도우며, 여섯째로 한정된 자원을 효과적으로 배분하기 위해서는 사업부/상품/서비스의 수익성 측면뿐만 아니라 리스크를 고려함으로써 최적의 자원배분이 이뤄질 수 있도록 돕는다는 것이다

그러나 COSO 프래임워크는 개괄적 개념이므로 기업에 적용하기 위해서는 상세한 구현 방법론이 필요하다. ERM을 구현하고자 하는 기업의 형태 및 위험의 종류가 다양하여, ERM을 구현하기 위한 구체적 이미지를 정의할 필요가 있으나 COSO 프래임워크에선 실제 이를 기업에 실천하기 위한 정의가 아닌 전체적 의미에서의 ERM의 개념과 구성요소를 정의하고 있으므로 실제로 구현하려는 기업이 어떻게 이 개념들을 조합하여 전사적 위험관리를 통해 기업목적 및 전략달성에 기여한다는 목표를 이룰 수 있는지에 대해서는 상세한 로드맵

과 이미지가 필요하다.

2.2 ERM 특징

ERM의 특징은 기존의 리스크 관리 체계와의 비교를 통해 이해할 수 있다. 기존의 리스크관리 체계로는 내부통제제도와 법/규제에서 명시하고 있는 리스크 관련 요건 등에 대응하는 Compliance/Reporting 체계로 구분해 볼 수 있다. ERM과 내부통제 그리고 규제대응의 개념을 구분하여 살펴보면 표1과 같다.

표 1 – ERM과 다른 리스크 관리체계와의 차이

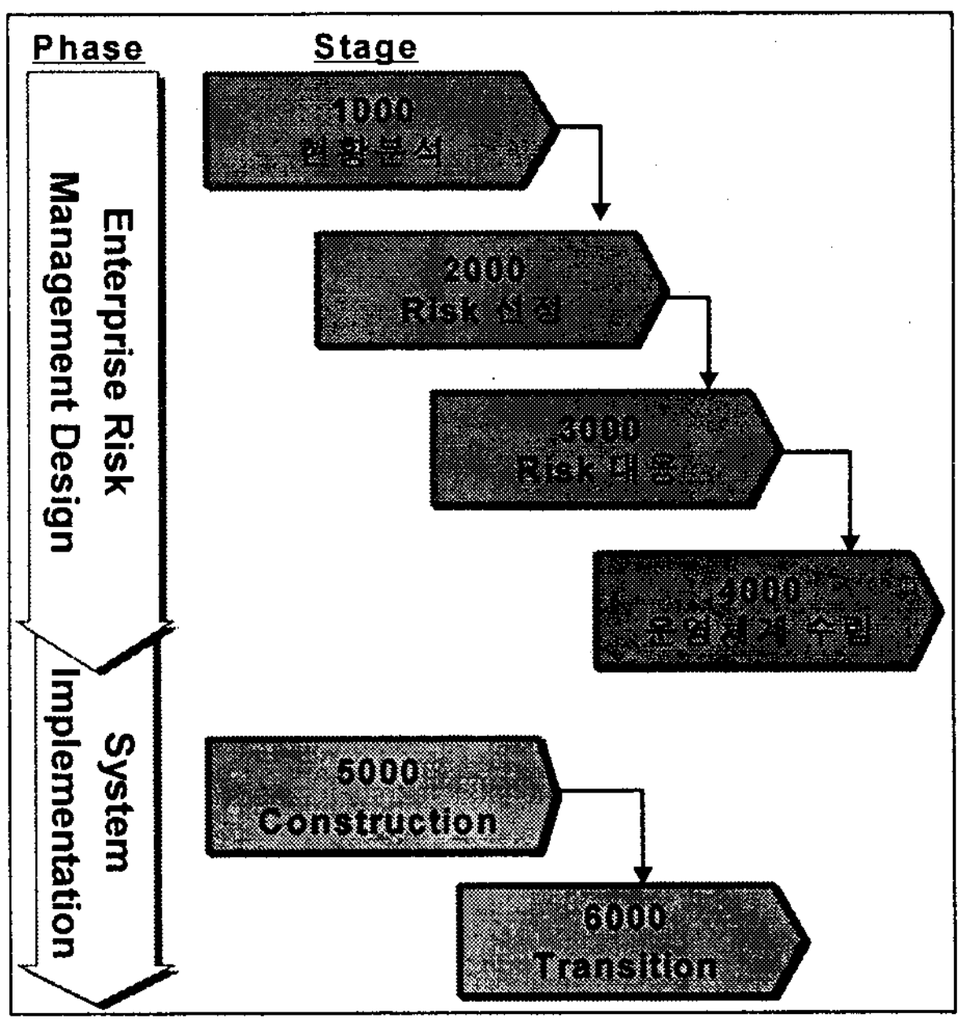
구분	ERM	내부통제	규제대응
Risk 관리 목적	• 전략달성 • 업무효율성 • 내/외부 보고 • 법/규제 대응	• 업무효율성 • 외부보고 • 법/규제 대응	• 외부보고 • 법/규제 대응
Risk 범주	• 목적달성에 영향을 미치는 내/외부 모든 Event를 대상 • Event Category관리	• 회계기록 정확도/공정성 위협 • 직무수행 기준 미준수	• 법/규정에서 정의하고 있는 Risk에 한정
Risk 인식/평가	• Event 불확실성, 목적달성 Impact에 따른 평가 • 기회요소 분석 • Key Risk 정의	• Process 또는 회계계정 기준분석	• 법/규제 요구사항 준수
Risk 대응	• 대응전략 수립후 개별 통제활동 정의	• 개별 통제활동 정의	
비고	• COSO ERM Framework	• COSO Internal Control Framework	• Sarbanes-Oxley Act • Basel Ⅱ • FDA Validation 등

특히 내부통제의 경우 ERM간의 관계에 혼동을 많이 가져오고 있으나, ERM은 내부통제를 포괄하는 개념으로 이해하는 것이 마땅하다. 그러므로 내부통제 체계를 구현했다고 해서 ERM을 구현했다고 생각하면 안 될 것이며, 각기 별도로 운영되는 체계가 아님으로 종합적인 계획에 따른 이행이 요구된다.

2.3 ERM 도입을 위한 추진절차

앞에서 지적한 바와 같이 ERM을 새로운 경영기법으로 기업에 적용할 때 COSO 프래임워크만으로는 한계가 있다. 이에 ERM도입을 위한 추진절차를 제안하고자 한다. COSO 프래임워크를 준수하되 기업고유의 체계를 구축하고 적용할 수 있도록 작업의 단위를 분류하고 작업단위간의 연관관계 및 결과물을 개발함으로 추진을 위한 기업내 자원을 배정하는 데 참고가 되고 합리적인 추진이 가능하게 하는 데에 목적이 있다.

그림 2 – ERM 추진 절차



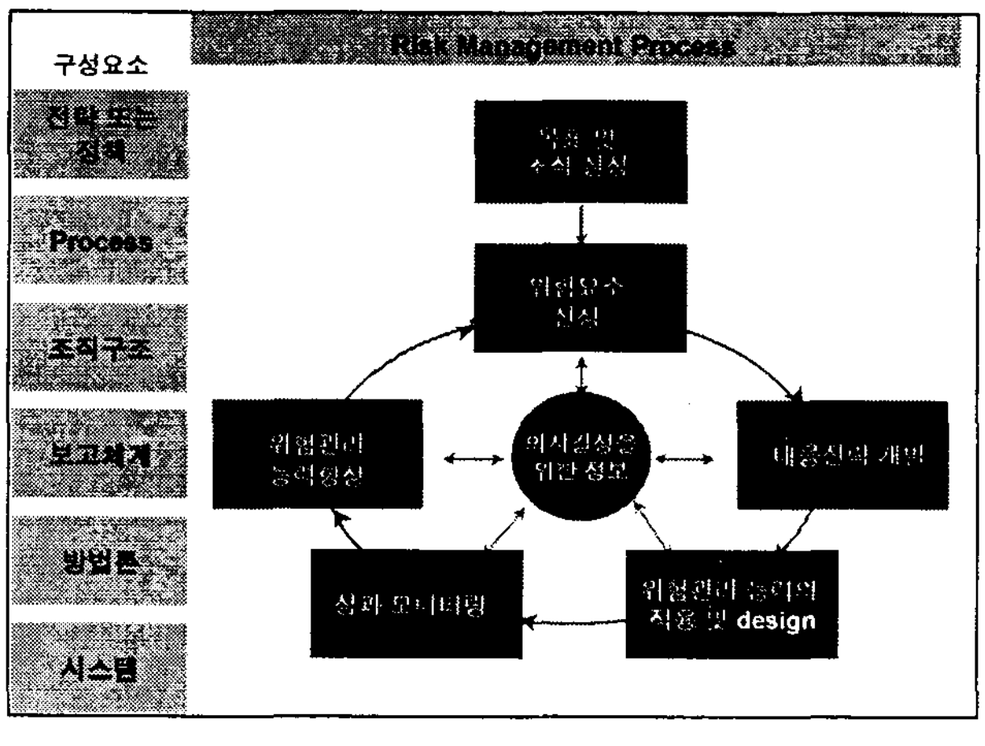
출처 : Entrue Consulting Partners.

본 추진절차는 Phase, Stage를 기준으로 한 세부작업으로 구성되어 있다. 첫째 페이즈는 기업의 비젼, 경영전략 및 문화를 고려하여 전사적 리스크 관리 체계를 설계하는 단계이다. 둘째 페이즈

는 효과적인 리스크관리를 지원하는 정보시스템 기능을 구현하는 단계이다.

각 작업을 추진하는 과정중에는 전략, Process, 조직, 보고체계, 방법론, 시스템의 항목이 모두 고려되어 진행되도록 하여 COSO 프레임워크를 만족하도록 해야 한다.[4]

그림 3 – 리스크관리체계와 구성요소



설계단계에서 가장 고려해야하는 요소는 리스크 식별의 기준이 기업의 비젼과 경영전략이라는 것이다. 현황분석을 통해 기업의 과거 리스크에 대한 인식 및 기록을 분석하고 현재 관리수준을 평가하여 리스크관리 체계 설계의 목표와 범위를 확정한다. 기업 내에서 다루어야 하는 리스크 범주는 예비적으로 해당산업 혹은 공통의 리스크 카테고리를 기준으로 점검 하되 경영전략, 발생빈도 및 목적달성에 미치는 영향을 고려하여 관리대상이 되는 리스크를 정의하도록 한다. 정의된 리스크에 대한 기본적인 대응 전략은 원인을 파악하고 이에 대한 회피(Avoidance), 수용(Acceptance), 최소화(Reduction), 공유(Sharing) 등으로 구분할 수 있다. 이에 따라 초기 리스크 인식단계에서 파악된 기업에 미치는 영향과 대응전략을 통해 감소된 정도를 평가한다. 최종적으로 기업고유의 리스크관리 정책서, 운영조직, 교육 및 훈련, 모니터링 체계를 포함하는 전사적 리스크관리 체계를 완성하게 된다.

리스크 노출(Exposure)규모, 발생의 예측, 목적달성에 미치는 영향, 원인 등에 대한 판단을 위해서는 대용량의 다양한 데이터가 요구되며, 전사적으로 모니터링하기 위해서는 의사결정자들에게 별도의 상황보고가 요구된다. 이러한 요구사항들에 효과적 대응을 위해서는 정보기술의 활용이 필요하며 관련한 정보기술의 기능을 정의하고 구현하는 단계가 진행된다.

2.4 효과적 ERM을 위해 요구되는 정보기술

앞서 살펴본 ERM 체계로부터 도출되는 정보기술 요구영역은 4가지로 구분해볼 수 있다. 첫째, 리스크에 대해 판단하기 위한 관련 데이타를 수집하기 위한 인프라 영역이다. 둘째는 리스크 대응 전략에 따라 업무프로세스 통제, 전결기준의 강화 등의 통제활동 지원영역이다. 셋째는 취합된 데이타를 바탕으로 분석을 실시하여 리스크를 인식하고 평가하는 영역이다. 넷째는 ERM체계 정착을 위해 리스크 관리목적과 현황을 공유할 수 있도록 하는 조직내에 의사소통 지원 영역이다.

표 2 - ERM지원 정보기술 지원 영역

구분	기능요구사항
ERM 문화 정착을 위한 정책 및 활동 공유	•ERM 정책 및 지침 전사적 공유 •리스크관련 사례 및 지식 공유 • 교육 및 각종 활동 소개
Risk 도출, 평가, 분석, 모니터링	•감사, 내부통제 등 정기/비정기 모니터링 프로세스 운영 지원 •통계적 모델, 시나리오 분석기능
통제활동 지원	•업무프로세스 운영상에 통제기능 반영 - 권한, 보안, 한도, 보고, Alarm등
관련 데이타 취합 및 분석	•모니터링 및 통제활동을 위한 데이터 취합 및 분석 기능

요구기능 사항을 충족하는 정보기술 솔루션은

<표 3>과 같다.

표 3 – ERM 지원 정보기술 요소

구분	정보기술 솔루션	설명
의사소통 지원	Portal	•조직의 위험관련 정보 및 각 시스템에서 발생되는 정보를 실시간 공유
모니터링 지원	Business Intelligence	•리스크에 대한 사전적 인식, 사후적 평가를 위한 데이타 분석 • 의사결정 지원을 위한 관리자용 Dashboard 제공 • 통계적 모델 적용 • 시나리오 중심 분석
통제활동 지원	Audit Management System, PMS(Project Management System)	•정기적인 내부감사, 업무감사, 비정기 감사 업무 프로세스 관리
	BPM(Business Process Management)	•업무 프로세스 상에 반영되어야 할 규정, 결제체계 통제, 이상징후 포착
인프라 지원	Contents Management	•ERM 운영시 산출되는 공식 보고서 기록보전 및 참조를 위한 관리 •법적 대응
	Security Management	•정보시스템 권한 및 보완 관리
	Datawarehouse	•리스크인식,평가,모니터링을 위한 관련 데이타 축적

출처 : Entrue Consulting Partners

제시한 바와 ERM 체계를 지원하는 정보기술 구현은 단일 솔루션으로 구성되는 것이 아니라 어플리케이션 로그시점부터 경영진이 전사적인 관점에서 리스크를 파악 의사결정 할 수 있는 영역까지 정보기술을 적용할 수 있으며, 기존시스템 분석과 중요 리스크별 대응 전략에 따라 필요자원을 구비하는 것이 바람직하다.

2.5 ERM 추진 현황

국내외에 ERM을 성공적으로 도입하여 Best Practice로 평가할 수 있는 사례는 많지 않다. 해외의 경우 금융산업이나 에너지/화학/제약 산업에서 사례를 찾아 볼 수 있다. [5] 국내의 경우 ERM관련 활동을 한 주요 기업들의 유형을 구분하면 다음과 같이 구분할 수 있다.

첫째 법/규제 대응을 너머 전략적 목표를 달성하기 위한 기업들이다. 한 예로 BSC 체계를 활용하여 리스크를 인식할 수 있는 지표체계를 정의하고, 이러한 위험지표 Map을 통해 기업의 위험을 측정한다. 그러나 기업이 직면한 위험을 모두 지표화하여 관리하는 것이 관리목적상 편리할 수 있으나 지표화가 어려운 정성적 측면의 중요지표들이 간과될 수 있다.

또 다른 예로는 Operation에 대한 관리체계 구현과 주요 경영지표를 통해 리스크를 모니터링하는 두가지 방안을 혼용하는 방식을 채택한 경우이다.

이러한 유형의 기업은 많은 위험요인들을 체계적으로 관리하기 위해 조직, 프로세스, 정책 및 전략과 정보기술지원체계로 구성한 전사적인 위험관리체계를 필요한다. 그러나 실제로는 Operation영역에 치우치거나, 지표를 중심으로 한 모니터링에 집중되어 전사적으로 확산 및 정착되는데에 장애가 발생할 수 있다.

둘째로 법/규제 대한 대응을 목적으로 리스크관리체계를 추진한 대다수의 상장기업이 이에 해당한다. 여러 기업들이 이런 방식을 선택한 이유는 현재 변화하고 있는 법/규제에 대응하는 것이 시급하기 때문이다. 특히 SOA, 내부회계관리제도등은 회계기록 정확도/공정성 위협과 직무수행 기준미준수를 주 대상으로 하기 때문에 관리하는 리스크가 제한적이다. 따라서 기업이 직면한 위험을 통합관리 하기 위해서는 경영전략 달성 관점에서 리스크에 대한 충분한 검토를 통해 균형잡힌 체계로의 개선이 필요하다 하겠다.

셋째로 리스크 관리 체계 운영을 추진하고자 탐색중에 있는 기업들이다. ERM을 새로운 경영기업

으로 도입을 고려하고 있으나 COSO의 완성된 ERM 개념에 의한 Best Practice가 충분하지 않아 아직 추진방향을 정의하지 못한 기업들이다.

이상에서 언급한 것처럼 아직까지 국내에 ERM 체계를 충실히 구현한 기업은 없지만, 여러 기업이 각자의 방식으로 리스크 관리의 중요성을 인식하고 대응하고자 다방면의 모색을 시도하고 있다. ERM을 구현하기 위해서는 유일한 하나의 방식이 존재하는 것도 아니며, 정보기술지원체계만 구현한다고 되는 것도 아니기 때문에 각 기업의 현황, 사업의 성격 등에 맞춰진 적합한 ERM구현방식을 찾아 전사적 관점에서 관리체계를 구현해야 할 것이다.

2.5 ERM 도입전략

COSO 프래임워크와 국내 추진 사례를 기반으로 기업에서 리스크 관리 체계 도입을 고려할 때 추진하는 전략은 두가지로 정리할 수 있다. 첫째 전면적인 ERM의 도입이다. 이러한 전략을 선택시에는 경영전략이 정비되어 있고 BSC(Balanced Scorecard)와 같은 기법이 도입되어 전략에 대한 모니터링 역량이 있을 때 효과적이다. 거듭 강조되는 바와 같이 경영전략 달성을 기준으로 리스크를 인식하게 되기 때문이다. 이러한 기반이 부족한 경우에는 사전적으로 전략에 대하여 전사적으로 재 검토를 하고 리스트관리 목적을 명확히 한 뒤 추진하는 것이 바람직하다. 두번째는 시장에 직접적인 제약을 받게 되는 법/규제 대응을 우선적으로 실시하고 대응체계가 안정화되고 관리기술이 조직내에 어느정도 축적되었을 때 전사적인 내부통제 체계를 운영하고 이를 확장하여 ERM을 구축하는 방법이다. 이 방법은 단계적 추진의 특성상 자원의 효율적 운영, 조직내 변화관리 용이성이 장점이 될 수 있으며, 단점으로는 ERM에 대한 비젼, 목적을 명확히 한 상태에서 전체적인 추진 로드맵을 사전적으로 마련하지 않으면 리스크 관리의 혼선을 초래하게 될 수 있다.

3. 결론

3.1 ERM 도입에 대한 제언

ERM을 도입하여 기업의 전략목표 달성을 지원하고, 점점 증가하고 있는 기업 내/외부의 위험요인들을 사전에 관리할 수 있도록 하기위한 ERM을 도입하기 전에 다음을 고려할 것을 제언한다.

첫째는 인식을 명확히 해야 한다는 것이다. ERM의 개념이 현재는 법/규제 대응과 내부통제와 혼용되어 쓰이고 있다. 개념상 상호 공통되는 것이 존재하나 각각의 관리 기법의 목적과 범위에는 차이가 있으므로 개별 관리기법에 대한 이해를 충분히 한뒤, 기업이 추구하고자 하는 목표가 무엇인지 정의한 뒤 추진 방향성을 결정해야 한다.

둘째, ERM은 경영전략 달성을 위한 관리 기법이므로 리스크에 대한 관리 기준은 기업 경영 전략이 되어야 한다는 것이다. 기업의 전략은 시장환경에 따라 계속적으로 변화되는 속성을 가지고 있다. 즉 리스크에 대한 인식 및 평가도 전략에 따라 변경되어야 함을 의미하며 ERM이 일시적인 체계가 아닌 지속적으로 운영되야 하는 체계임을 인식해야 한다. 따라서 명확한 전략에 대한 이해와 지속적으로 운영가능한 적절한 조직 구성 및 문화정착이 필요하다.

셋째는 ERM은 IT Solution이 아닌 경영기법이며 ERP(Enterprise Resource Planning)나 BPM(Business Processs Management)과 같은 단일 솔루션은 더욱 아니라는 것이다. 기업의 위험을 전부 지표화하여 모니터링 할 수도 없으며 하나의 솔루션으로 관리할 수 있는 것도 아니다. 기업이 직면하고 있는 위험을 통합하여 관리하기 위해서는 통합관리를 담당할 조직(가상 또는 CRO를 중심으로한 실재 조직)을 구성하고, 업무 프로세스를 구성하고, 기존의 위험대응 프로세스를 변경하는 많은 과제를 동반하며 이러한 과정을 진행하면서 필요한 정보기술 요소를 판단하고 추진해야 한다.

3.2 향후 연구과제

현재까지 ERM에 대한 연구작업은 COSO가 발표한 ERM 프래임워크를 기업에 적용할 수 있도록 개념을 발전시키고, 실천적 의미를 연구한 것이다. 그러나 아직까지 이런 개념을 체계적으로 구현한 사례가 없고, 개별적으로 일부 ERM 구성요소를 구현하고 있는 실정이다. 따라서 검증된 방법론으로써 체계를 갖추기 위해서, 추진 경험을 바탕으로 추진 단계별 세부 작업에 적용되는 분석 기법과 테크닉을 정형화하여야 한다. 또한 관리하여야 하는 리스크에 대한 균형잡힌 관점 유지를 위하여 산업별 Risk Universe 또는 Risk Category를 개발함으로써 전체 리스크에 대하여 빠짐없이 검토한 후 기업 고유의 리스크 프로파일을 설계 할 수 있도록 제시하여야 한다. 마지막으로는 ERM에 대한 Cost/Benefit 모델을 개발함으로 도입 결정시, 도입후 결과를 객관적으로 평가할 수 있는 모델을 제시하는 것이다.

[참고문헌]

[1] Economist Intelligence Unit, "CEO Briefing: Corporate priorities for 2005", 2005

[2] PricewaterhouseCoopers, "Managing Risk: An Assessment of CEO Preparedness", 2004

[3] Committee of Sponsoring Organization of the Treadway Commission, COSO Enterprise Risk Management – Integrated Framework, 2004

[4] James W. Deloach, "Enterprise-Wide Risk Management – Strategies for linking risk and opportunities", 2000

[5] Thomas L. Barton, William G. Shenkir, Paul L. Walker, "Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management", 2002