2011.8.9

POSRI CEO REPORT

전사적 관점의 리스크 관리의 이해

전략컨설팅실 外

posco
포스코경영연구소

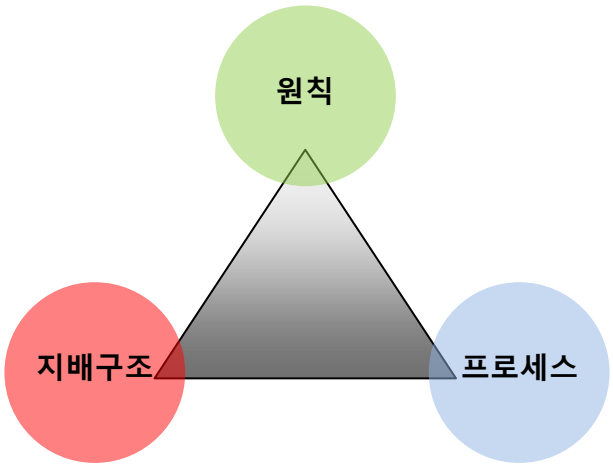
Executive Summary

전사적 관점의 리스크 관리의 이해

□ 대내외 경영환경 불확실성의 급증과 세계 각국의 리스크 기준 강화는 전통적인 리스크 관리에 대한 관점의 변화를 요구

○ 그 동안 기업의 각 부문에서 관리해오던 리스크를 전사적인 차원에서 체계적으로 관리해야 한다는 새로운 관리 방식인 전사적 리스크 관리(Enterprise Risk Management: ERM)가 등장

□ ERM 체계는 조직 내 공유된 리스크 *관리 원칙*과 효율적인 리스크 관리를 위한 *지배구조*를 구축하여 리스크를 식별, 평가, 대응, 모니터링 하는 일련의 *프로세스*로 구성



○ (원칙) 기업의 모든 업무에 내재되어 있는 리스크를 고려하는 방법에 대한 공유된 믿음과 태도. ERM이 운영되는 방식에 영향을 미치기 때문에 모든 구성원들에게 전사적으로 이해되고 공유되어야 함

○ (지배구조) 리스크 전담 부서 및 리스크 관리위원회를 설치하여 리스크 관리 기반을 구성함으로써 리스크 관련 최적의 의사결정 체제로 변화

○ (프로세스) 모든 부서가 리스크의 식별, 평가, 대응, 모니터링을 실행하는 전사적이고 지속적인 리스크 관리 프로세스의 확립

□ 우리 기업들도 리스크 관리에 대한 시대적 관점의 변화 요구를 인식하고, 자사의 상황에 맞는 프레임워크를 개발해 ERM을 효과적으로 수행할 필요가 있음

Contents
목 차

Ⅰ. ERM 추진 배경

□ 대내외 경영 활동의 불확실성이 날로 커지고 있는 상황에서 기업들은 더욱 예측하기 어려운 다양한 리스크에 노출

○ 성장성과 수익성 확보에 주력해 온 기업들은 잘 나가던 기업이 한 순간에 부실 기업 혹은 도산 기업이 될 수 있음을 IMF를 통해 몸소 체험

○ 또한 2006년 하반기에 불거진 미국 서브프라임 모기지 부실문제, 2008년 글로벌 금융위기 등과 같은 지속적인 금융시장의 불안요소와 그 여파는 글로벌 실물경기 침체를 야기

□ 이러한 환경 속에서 기업의 전사적인 수준에서 잠재해 있는 리스크를 찾아내고 이를 보다 체계적으로 관리해야 할 필요성 고조

○ 과거 환율, 금리 등 재무적인 영역에 국한되었던 리스크 관리를 기업 전반적 수준에서 체계적으로 관리하고자 하는 요구가 증대

○ 각국의 정부 및 관련 기관들은 기업의 리스크 관리에 대한 기준을 점차 강화하고 있어 기업이 전사적인 시각에서 리스크 수준을 측정하고 체계화된 위험관리 활동을 수행하는 것이 의무화되는 추세

- 미국증권거래위원회(SEC)는 기업들의 리스크 수준과 이에 대한 관리 활동을 문서화해 사업보고서에 수록하도록 의무화

- 독일 역시 1998년에 주요 경영 리스크에 대한 모니터링 체계를 구체화하고 리스크 관리 활동을 감독 기관에 주기적으로 보고하도록 하는 법안을 도입

<표 1> 각국의 위험관리 활동 수행 의무화

국가	기관	관련규제/지침	내용
미국	증권거래소	Requirement in 10K, 10-Q	▪경영 리스크 수준을 문서화해 공시할 것을 규정 ▪기업들은 10-K, 10-Q 등의 사업보고서에 노출된 리스크 수준과 리스크 관리 활동 내역 등을 공시
독일	공정거래 위원회	KONTRAG (1998)	▪주요 경영 리스크에 대한 관찰 및 관리체계를 구체화 ▪리스크 관리 활동을 감독 당국에 주기적으로 보고하도록 법제화
캐나다	토론토 증권거래소	Dey Report (1994)	▪효율적인 내부통제를 정착하기 위한 규범 요구 ▪리스크 평가와 대응 활동을 포함하는 체계적인 내부통제 활동을 수행할 것을 권고
영국	런던 증권거래소	Turnbull Report (1999)	▪리스크 관리 활동과 내부통제제도의 효율성을 측정하는 보고서 제출 의무화

Ⅱ. ERM의 개념과 특징

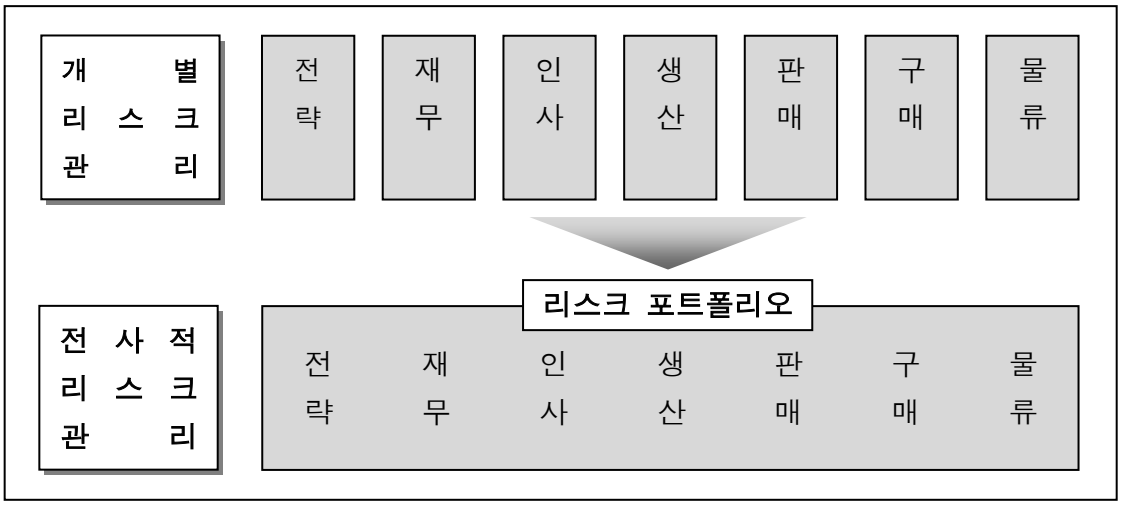
1. ERM의 개념

□ ERM은 COSO[1]가 ERM이라는 용어와 함께 새로운 모델과 방법론을 소개하면서부터 주목 받기 시작

○ ERM은 기업의 전체적인 시각에서 기업에 영향을 미칠 수 있는 잠재적인 위험 및 사건 등을 파악하고, 일정한 수준 내에서 위험을 적절하게 관리하며, 기업의 목적을 달성하기 위해 합리적인 대응 방안을 강구하는 프로세스로 정의[2]

○ 즉, ERM이란 기업이 직면하는 여러 가지 경영 위험들을 전사적인 시각에서 통합적으로 인식하고 관리하는 새로운 위험관리 방식을 의미

○ 기존의 리스크 관리 방식은 각각의 기능 및 부서단위로 리스크를 인식하고 관리하는 것이었으나, ERM 방식은 전사적 리스크 관리의 책임 주체를 중심으로 각 부문의 리스크 관리를 통합



<그림 1> 개별 리스크 관리와 전사적 리스크 관리 비교

[1] Committee of Sponsoring Organizations of the Treadway Commission의 약자로 미국의 회계, 재무, 내부감사 등 각 분야의 전문가들로 구성되어 있으며, 기업의 회계, 재무, 내부통제 구조에 관한 연구를 진행하는 연구기관

[2] *Enterprise Risk Management– Integrated Framework*, 2004, COSO

2. 전통적인 리스크 관리와 ERM의 차이점

☐ **ERM 이전의 리스크 관리는 기업에서 필요할 때마다 수행하는 경우가 대부분**

○ '필요할 때' 란 리스크가 이미 현실화되어 손실이 발생하거나, 이미 손실 발생이 거의 확실시 되어 사후적인 대응 차원이 필요한 경우

☐ **그러나 ERM은 경영환경의 변화를 지속적으로 모니터링 해 손실 발생을 미리 막는 것을 목표로 리스크 요소를 표면화하고, 리스크 관리를 체계화하며, 리스크 요소를 공유화 한다는 특징**

[리스크 요소의 표면화]

○ 기존의 리스크 관리 방식은 소극적인 성격으로 기업의 CEO와 임원조차도 중요한 위험요인들이 무엇인지 모르는 경우가 많음

○ ERM은 이러한 숨어 있는 위험요인들을 과감히 노출함으로써 그 동안 간과돼 왔던 위험요인들을 새롭게 인식하는데 도움

[리스크 관리의 체계화]

○ 일반적으로 기업에서는 다양한 경영 리스크들의 존재를 인식하고 있더라도 그 관리방법에 문제점을 갖고 있는 경우가 많음

○ 즉, 구매부서에서는 가격 변동 위험을, 재무부서에서는 환율과 금리 변화 위험을, 최고경영진들은 전략 위험을 담당하는 식으로 개별 리스크 관리 업무를 수행

○ 이러한 방법으로 모든 리스크들을 관리한다는 것은 사실상 불가능할 뿐만 아니라 경영자원의 비효율적 분배를 초래

○ ERM은 산발적으로 분리되어 있는 리스크 관리를 체계적으로 재구성해 그 효과를 극대화 시킨다는데 의의

[리스크 요소의 공유화]

○ 기존의 리스크 관리는 개인 또는 부서 단위의 독자적 리스크 관리로 인해 개별 상호간 리스크에 대한 인식과 정의가 일치하지 않아 조직 내 정보 공유와 의사소통이 어려웠음

○ 따라서 새로운 리스크 관리 시스템이 필요하며, 이를 전사 임직원이 공유함으로써 단점을 극복하는 것이 필요한데, ERM으로부터 그 해결책을 발견

Ⅲ. ERM 체계

1. ERM 원칙(Principle)

□ ERM 원칙은 회사의 모든 업무에 내재되어 있는 리스크를 고려하는 방법에 대한 공유된 믿음과 태도로 다른 ERM 요소의 근간

○ 리스크 관리 원칙은 기업이 리스크를 보는 시각과 리스크를 관리하기 위해 어떻게 행동할 것인가에 대한 실천적인 믿음을 의미하며, 대내외적인 커뮤니케이션의 기반으로 사용되어 모든 이해관계자들과 공유

○ 리스크 관리 원칙은 한 기업의 문화와 운영방식에 영향을 미치는 동시에 기업의 가치를 반영

○ 또한 리스크를 식별하는 방법, 수용된 리스크 종류와 이를 관리하는 방법 등 전사적 리스크 관리 요소들이 적용되는 방식에 영향을 미침

□ 리스크 관리 원칙이 구성원들에 의해 원만하게 형성 · 이해 · 적용될 때, 회사는 효과적으로 리스크를 식별, 관리가 가능

○ 전사적으로 리스크 관리 철학이 잘 형성된 회사에서조차 부서별 문화적 차이가 존재하고, 이것이 전사적 리스크 관리의 적용에 변화를 가져올 수도 있음

○ 구성원이 동의하지 않은 경우, 사업부 · 기능 · 부문 차원에서의 전사적 리스크 관리는 원활히 진행될 수 없을 가능성이 큼

○ 이때 중요한 점은 경영자가 단순히 말로써 리스크 관리 원칙을 공고히 할 것이 아니라, 문서를 통한 방침, 행동 표준, 행위 지침, 예외사항 리포트, 주요 임직원들과의 비공식적인 대면 등 일상 생활의 업무를 통해 원칙을 확고히 해야 함

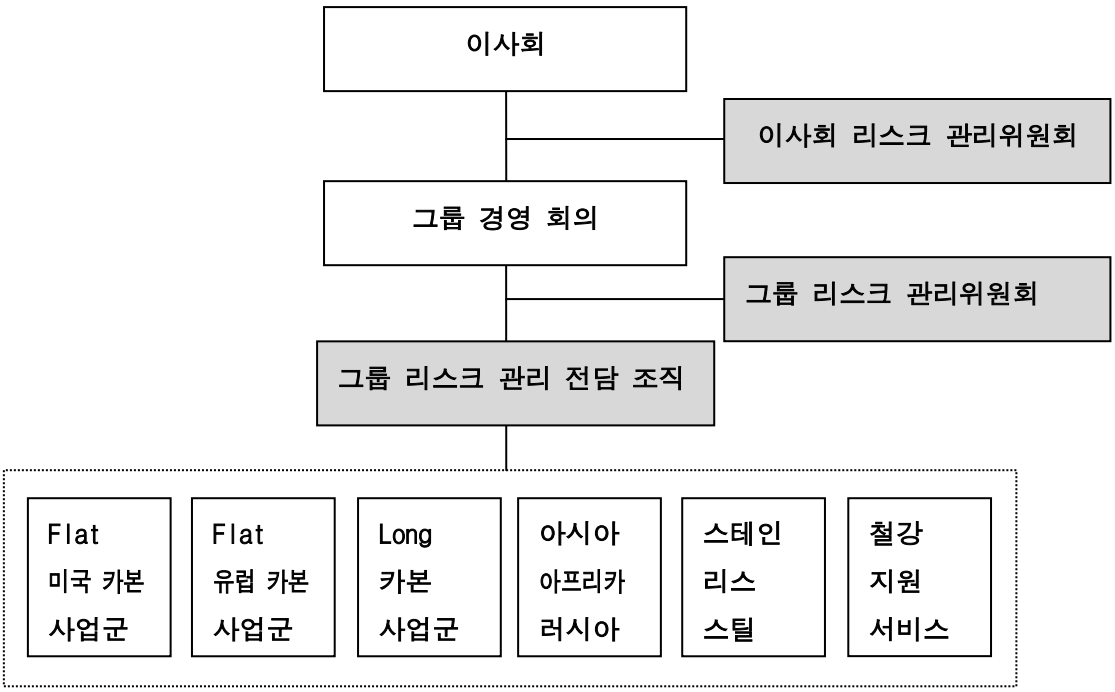
2. 지배구조(Governance)

□ 리스크 관리를 위한 지배 구조는 기업의 효과적인 리스크 관리 기능 제고를 목적으로 한 기업의 리스크 감수 관련 전략 수립 및 그에 대한 감시 · 관리를 위한 관련 경영지배구조 요소를 통칭하는 개념

○ 기업 내 리스크 관리를 위한 지배구조의 구성, 리스크 전담 조직의 역할 설정, 이사회 및 이사회 내 리스크 위원회의 관리 기능 등 리스크 관리와 밀접하게 연관된 경영지배구조 요소들이 모두 리스크 지배구조를 구성하는 요소로 포함

[사례: 아르셀로미탈의 리스크 관리 지배구조]

□ 리스크 관리 최고 의사결정기구로서, '이사회 리스크 관리위원회'를 설치, 또한 최고경영진으로 구성된 '그룹 리스크 관리위원회'를 이사회와 평행(parallel)한 구조로 설치 · 운영



<그림 2> 아르셀로미탈의 리스크 관리 조직도

○ 이사회 내 리스크 관리위원회는 경영 통제와 감독 기능을 위해 그룹의 리스크 관리 체계와 관리 과정을 모니터링

- 이사회 리스크 관리위원회는 경영진의 그룹 리스크 허용 수준(안)을 심사하고, 주요 리스크 노출수준에 대한 한도를 부여

○ 경영진은 CEO 직속 기구로 '그룹 리스크 관리위원회'를 신설하고, 각 부문별 리스크 관리 전담 조직 및 인력을 구축해 통합, 조정 기능을 수행

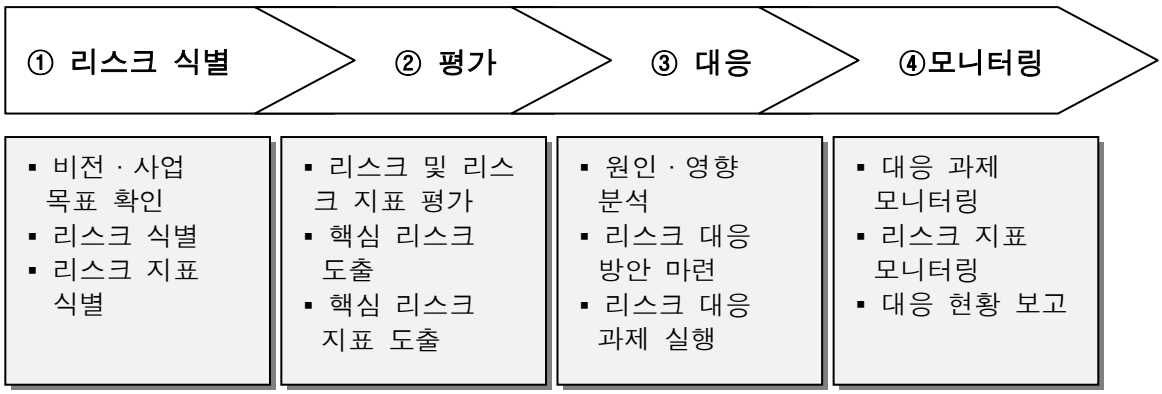
- 그룹 리스크 관리위원회는 기업의 중요한 리스크 관련 정보를 정기적으로 이사회 리스크 관리위원회에 보고

○ 리스크 관리 전담 조직은 그룹 리스크 관리위원회의 위임을 받아 리스크 관련 주요정책 및 사안에 대해 사전 협의 및 조정을 담당

□ **리스크 지배구조의 개선은 결국 리스크와 관련된 정보가 효율적으로 전달되고, 이를 반영한 리스크 관련 의사결정 체계가 운영되는 방식을 개선하는 것이 핵심**

3. ERM 프로세스(Process)

□ **리스크 관리 프로세스는 리스크를 사전적으로 예방하는 관리 프로세스로서 다음과 같이 리스크 식별, 평가, 대응 및 모니터링의 4단계로 구성**



<그림 3> 전사적 리스크 관리 프로세스

[리스크 식별]

□ 리스크 식별은 발생 시 기업에 영향을 끼칠 수 있는 잠재적 사건을 식별하고, 그것이 기회를 의미하는 것인지 혹은 부정적인 영향을 주는 것인지를 판단하는 단계

○ ERM의 일환으로 경영자는 내·외부 리스크 요소와 그로 인해 발생 가능한 사건의 유형을 이해해야 함

<리스크 요소의 분류>[3]

- 전략 리스크(Strategy risk)
- 경쟁자 리스크(Competitors risk)
- 제품/산업 리스크(Product/Industry risk)
- 정보 리스크(Information risk)
- 자원 리스크(Resources risk)
- 기술 리스크(Technological risk)
- 운영 리스크(Operational risk)
- 재무 리스크(Financial risk)
  - *거래상대방 리스크(Counterparty risk)*
  - *자금 조달 리스크(Funding risk)*
  - *통화/금리 리스크(Currency/Interest risk)*
- 국가·지역 리스크(Country risk)
- 거시 경제 리스크(Economic risk)
- 환경 리스크(Environmental risk)
- 법 리스크(Legal risk)
- 정치 리스크(Political risk)
- 전쟁/테러리즘 리스크(War/Terrorism risk)
- 자연재해 리스크(Natural Catastrophe risk)
- 공공 관계 리스크(Public relations risk)
- 평판 리스크(Reputation risk)

[3] Holliwell, J. (1998), The Financial Risk Manual, PITMAN Publishing.

○ 사건 식별 기법으로는 사건 목록 이용, 위크숍, 인터뷰, 질문서, 설문조사, 프로세스 흐름분석, 선행사건 지표 등이 있음

<표 2> 리스크 요인 식별 방법

리스크 식별 방법	내 용
사건 목록	특정 산업에 속한 기업들에게 빈번하게 일어나는 구체적인 사건을 제시해 놓은 리스트를 활용
내부 분석	일상적인 사업부 단위 스텝 회의를 통해 경영 계획에 따른 프로세스의 일부로 수행
임계치	미리 정의되어 있는 기준과 현재의 리스크 사건을 비교하여 리스크 발생 인식
워크숍과 인터뷰	축적된 지식 및 관련자들의 토의를 통해 얻은 경험을 기반으로 리스크 사건을 식별
프로세스 흐름 분석	각 프로세스에 대한 투입물, 과업, 책임, 산출물의 흐름을 단계적으로 분석하여 목표달성에 영향을 줄 수 있는 리스크를 파악
선행 사건 지표	리스크 사건과 관련된 데이터를 모니터링 해 사건을 발생시키는 조건의 존재여부를 파악
손실 사건 자료 방법론	과거의 개별적인 손실 사건에 대한 누적자료 DB를 구축, 이것을 원천으로 리스크 요인을 파악

[리스크 평가]

□ **리스크 평가는 기업에 발생할 수 있는 미래 사건이 목표 달성에 있어 어느 정도의 영향을 미칠 것인가를 파악하는 단계**

○ 리스크를 평가할 때 경영자는 '발생가능성'과 '영향도'의 두 가지 관점에서 사건을 평가

- '영향도'는 사건이 미치는 효과를 의미하는 반면,'발생가능성'은 어떤 사건이 발생할 수 있는 확률을 의미

○ 이러한 평가는 일반적으로 어떤 사건의 발생가능성이 '높음, 보통, 낮음'과 같은 정성적인 기법과 '퍼센트, 발생 빈도, 수치'와 같은 정량적인 기법으로 구분

- 정성적 평가 방법은 측정한 사건의 발생가능성 및 영향에 대한 의견 일치를 이끌어 내기 위해 인터뷰와 워크숍과 같은 방법을 활용

- 정량적 평가 방법은 고도의 노력과 정확성을 요구하며 때때로 수학적 모델을 사용. 따라서 보조 정보 및 가정의 질적인 요소에 의존하여 신뢰성 있는 예측을 가능하게 함

<표 3> 정량적인 리스크 평가 방법

평가 방법	내 용
벤치마킹	특정한 사건이나 과정에 중점을 두고 측정과 결과를 비교해 보면서 개선의 기회를 찾음. 사건, 과정, 측정에 관한 정보는 성과를 비교/평가하는 데 이용
확률모형	특정 가정을 바탕으로 사건의 발생가능성을 사건의 범위 및 영향과 연관시켜 발생가능성과 영향도를 도출. 확률모형의 예는 Value at Risk, Cash flow at Risk, Development of Credit, Operational loss distribution이 있음
비확률모형	사건들의 영향을 추정하는데 사건의 발생가능성을 계량화하지 않고 주관적인 가정을 사용. 비확률모형의 예로는 민감도 분석, 스트레스 테스트, 시나리오 분석이 있음

[리스크 대응]

□ **리스크 대응은 식별된 리스크를 제거하거나, 축소하기 위해 적절한 대응 방안을 수립하고 실행하는 단계. 대응 활동은 크게 리스크 회피, 감소, 공유, 수용의 네 가지 방식으로 이루어짐**

○ 리스크 회피(Avoidance)는 리스크가 발생 가능한 활동을 중단하는 것으로 생산라인 철회, 새로운 지역 시장에 대한 확장 축소, 사업부 매각 등을 포함

○ 리스크 감소(Reduction)는 리스크의 발생가능성이나 영향력 중 하나 또는 모두를 동시에 감소시키는 활동이며, 일상적으로 이루어지는 다수의 사업 결정들이 이에 속함

○ 리스크 공유(Sharing)는 리스크의 일부를 이동시키거나 공유함으로써 리스크의 발생가능성 또는 영향도를 감소시키는 것을 의미하며, 일반적인 방법으로는 보험상품 구매, 헷징거래, 아웃소싱 등이 있음

○ 리스크 수용(Acceptance)은 리스크의 발생가능성 또는 영향도를 줄이는 어떤 행동도 취하지 않는 것임

[리스크 모니터링]

□ **리스크 모니터링은 관리 대상 리스크에 대한 이상 징후를 도출하기 위해 일정한 기준에 따라 검토, 감독, 관찰하고 실행을 관리하는 일련의 활동을 수행하는 단계**

○ 모니터링은 상시적인 활동(Ongoing Activities) 또는 독립 평가(Separate Evaluation)의 두 가지 방법

- 상시 모니터링은 기업의 일반적이고 반복적인 운영 활동으로 구현되며, 실시간 원칙으로 수행되고, 변화된 조건에 동적으로 반응하여 기업 전반에 적용

- 독립 평가의 범위와 빈도는 주로 상시 모니터링 절차의 효과성에 의해 결정되기 때문에, 전사적 리스크 관리의 효과성에 직접적으로 초점을 맞추면서 때때로 새로운 시각을 얻는데 유용

Ⅳ. 결론 및 시사점

□ **시대적 상황과 함께 진화해 온 리스크 관리 활동은 이제 리스크 관리에 대한 관점의 변화를 요구하고 있음. 과거 각 부문에 국한되었던 리스크 관리가 이제는 전사적인 시각에서 통합적으로 인식하고 대응하는 형태로 진화하고 있음**

○ 리스크 관리에 대한 관심은 급격한 환경 변화로부터 발생하는 리스크들을 관리하지 않고 방치할 경우 해당 기업은 누적된 리스크로 인해 막대한 손해를 입을 가능성이 급격히 커지기 때문

○ 따라서 주주, 규제기관, 거래선 등 이해관계자들은 해당 기업의 경영진이 전략 및 사업과 관련된 리스크를 정확히 파악하고, 이를 효과적으로 관리하고 있는지를 확인하고 싶어함

○ 선진 기업들은 이미 전사적 리스크 관리를 목적으로 관련 경영지배구조를 정비하고 있으며, 이러한 활동은 리스크 관리의 효율성을 제고할 뿐만 아니라 주주 등 이해관계자들에게 긍정적인 신호(signal)로 전달되어져 기업가치 극대화에 기여하고 있음

□ 정형화된 ERM 프레임워크는 존재하지 않으며, ERM 구축은 각 기업의 상황에 맞는 프레임워크를 개발해 효과적으로 수행해야 함

○ ERM은 획일적으로 도입만하면 바로 모든 리스크를 없앨 수 있는 도깨비 방망이와 같은 솔루션이 아님

○ 각 기업의 사업 특성에 따라 잠재된 리스크의 종류, 정치 및 경영환경, 소비자 성향 등의 리스크 환경이 각각 다르기 때문에 자사의 리스크 환경에 대한 심층적인 이해가 필요하며, 이를 바탕으로 자사의 상황에 적합한 ERM 프레임워크의 개발이 필요

<참고문헌>

1. 이상열, 표세원. “ERM 구축방법론에 대한 연구: 철강기업 사례를 중심으로,” 「POSRI경영연구」, 제9권 제1호, 2009.
2. ArcelorMittal. *Annual Report*, 2009.
3. _____. *Annual Report*, 2011
4. Committee of Sponsoring Organizations of Treadway Commission (COSO). *Enterprise Risk Management Framework*, 2004.
5. Holliwell, J. *The Financial Risk Manual*, PITMAN Publishing, 1998.

윤수걸 (e-mail: hubyoon@posri.re.kr)
표세원 (e-mail: sewon_pyo@posri.re.kr)
이상현 (e-mail: rightreason@posri.re.kr)

☞ 이 자료에 나타난 내용은 포스코경영연구소의 공식 견해가 아니며, 작성자 개인의 의견임을 밝혀 둡니다.