주류산업의 리스크관리도 이젠 ERM이다

고 재 민
(LG경제연구원 책임컨설턴트, jmgoh@lgeri.com)

■목 차■

1. 왜 ERM인가?

최근 들어 유행이라고 할 만큼 많은 기업들이 전사적 리스크 관리(Enterprise Risk Management : ERM)에 깊은 관심을 보이고 있다. 이처럼 ERM이 전성기를 맞고 있는 것은 기업 내부의 필요와 외부의 요구가 맞아떨어졌기 때문인 것으로 풀이된다.

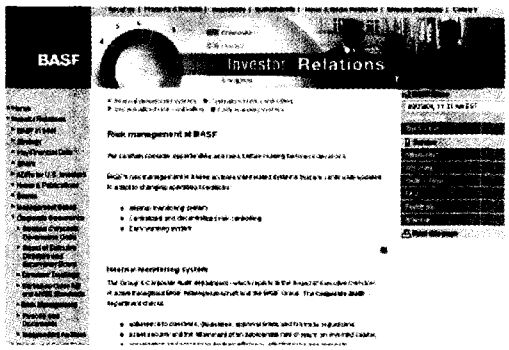
먼저 내부적 필요성으로는 기업을 둘러싼 경영 환경의 불확실성이 커지고 있고, 많은 리스크들이 서로 연관되어 있어 이들을 개별적으로 관리하기보다는 전사 차원에서 통합 관리함으로써 리스크 관리의 포트폴리오 효과를 기대할 수 있으며, 유한한 기업 자원의 효율적인 배분을 통한 적절한 대응이 가능하다는 점을 들 수 있겠다.

그러나 ERM이 기업들의 관심을 끌고 있는 것은 단순히 기업 내부의 필요성 때문만은 아니다. 먼저 세계적으로 정부 및 규제 기관들이 기업의 리스크 관리에 대한 기준을 강화하고 있어, 전사적인 시각에서 리스크 수준을 측정하고 공시하는 것이 의무화되는 추세에 있다. 미국의 SEC는 경영 리스크의 수준과 이에 대한 관리 활동을 문서화하여 공시할 것을 규정하고 있어, 기업들은 10-K, 10-Q 등

사업보고서에 기업의 리스크 수준과 리스크 관리 활동 내역을 수록해야 한다. 영국의 런던 증권거래소는 2000년 이후 기업의 리스크 관리 활동과 내부 통제 제도의 효율성을 측정하는 보고서 제출을 의무화하고 있다. 독일 역시 1998년에 주주들에게 기업 경영에 대한 더 많은 정보를 제공하는 동시에 이사들의 책임을 확대하기 위해 KonTraG라는 법률을 입법화하여, 기업들은 주요 경영 리스크에 대한 모니터링 체계를 구체화하고 리스크 관리 활동에 대한 구체적 내용을 감독 기관에 주기적으로 보고해야 한다.

지속가능경영의 확산 등 기업의 사회적 책임(Corporate Social Responsibility : CSR)이 점점 강조되는 것도, ERM에 대한 요구가 거세지는 또 다른 원인이다. 미국과 유럽에서는 CSR의 연장선 상에서 리스크 관리 활동을 의무적으로 공시하게 만들려는 움직임이 이미 오래 전부터 시작되었다. 특히 최근 UN · OECD · ISO 등에서 CSR의 국제 규범에 대한 논의가 활발해지면서, 앞으로는 우리 나라에서도 리스크 관리에 대한 요구가 더욱 강화될 것으로 전망된다. 특히 인간의 생존이나 건강과 직결되어 사회적 리스크가 높은 주류 산업의 경우, 이익을 많이 내더라도 산업 자체가 가지고 있는 사회적 리스크가 기업 가치 평가 과정에 크게 반영되기 때문에 ERM의 도입이 보다 시급하다. 실제로 선진 기업들은 ERM을 통해 잠재 리스크를 관리함으로써 전략 달성을 촉진하는 것은 물론이고, 한 걸음 더 나아가 IR을 통해 리스크 관리를 적극 수행한다는 사실을 외부 이해관계자에게 알리는 등 ERM을 기업 가치 상승에 활용하고 있다(<그림 1> 참조).

<그림 1> BASF의 리스크 관리를 활용한 IR활동



기업의 지속가능성을 평가하는 데 있어 세계적으로 가장 권위 있는 지표인 다우 존스 지속가능성 지수(Dow Jones Sustainability Indexes : DJSI)는 기업이 장기적으로 생존하려면 ▲경제적 책임 ▲환경적 책임 ▲사회적 책임을 다해야 함을 강조하면서, 경제적 책임 준수를 위한 하나의 평가 항목으로 리스크 및 위기 관리를 포함시키고 있다. 지속가능성 보고서의 국제적 가이드라인을 제정하고 있는 GRI(Global Reporting Initiative) 역시, GRI 2002 Guidelines에서 기업의 운영 계획 및 신제품 출시 과정에서 어떻게 리스크를 관리하고 있는지 명시하도록 권고하고 있다. 이처럼 리스크 관리는 더 이상 기업 내부의 필요에 의한 선택사항이 아니라, 글로벌 스탠더드로 자리 잡고 있어 기업 경영의 필수 요건이 되고 있다.

2. ERM이란 무엇인가?

ERM 이전의 리스크 관리는 주로 개별 리스크를 생산 · 영업 · R&D · 구매 · 재무 등 부서 내에서 개별적으로 관리하거나 혹은 주로 제품 단위로 분할된 사업부별로 관리하는

방식이었다. 그러나 이러한 개별 리스크 관리(Silo-based Approach)로는 현대의 경영 환경 하에서 발생하는 복잡·다양한 리스크들을 효과적으로 인식하고 대응할 수 없다는 한계를 지니고 있다. 또한 부서간의 리스크 관리 업무가 일관성을 지니지 못하는 등 리스크 관리의 부문 최적화 문제가 발생하고, 리스크 관리에 대한 전사적인 커뮤니케이션이 원활하게 이루어지지 못해 리스크 관리의 비효율성을 초래하게 된다.

따라서 이와 같은 한계를 극복하기 위하여 1990년대 중반 이후 기업이 직면하는 다양한 경영 리스크들을 전사적인 관점에서 통합하여, 하나의 리스크 포트폴리오로 인식하고 관리(Integrated Approach)하는 새로운 리스크 관리 방식인 ERM이 등장하게 되었다. ERM 체계 하에서는 전사적인 관점에서 리스크에 대한 체계적인 인식과 대응 전략을 수립할 수 있어 리스크 관리 자원을 최적화시키는 효과를 거둘 수 있다. 또한 구성원 및 조직 전체의 리스크 관리 마인드를 제고하여 내부 통제 활동의 효율화 및 기업지배구조의 강화, 대외적 리스크 관리 커뮤니케이션 등을 통한 이해관계자들의 신뢰 확보 등을 기대할 수 있다.

ERM과 기존 리스크 관리의 가장 커다란 차이라면 무엇보다 전략 리스크에 대한 접근을 들 수 있다. 기존의 리스크 관리는 초점이 주로 내부 통제 중심의 운영 리스크에만 맞추어져 있었던 것이 사실이다. 그러나 운영 리스크는 Bottom-Up 방식의 접근을 통해 'Do Things Right?'와 관련된 문제만을 고려하기 때문에, 개별 부서 혹은 사업부의 리스크가 전사 전략 달성에 얼마나 큰 영향을 미치는지에 대한 고려가 없는 경우가 대부분이다. 반면 전략 리스크란 기업의 전략에 근거한 Top-Down 방식의 접근을 통해 먼저 'Do the Right Things?'에 대한 질문을 던진다. 따라서 ERM에서는 전략 리스크를 관리함으로써 개별 부서 혹은 사업부의 특정 리스크가 전사 목표 달성과 얼마나 큰 관련이 있는지를 규명하고, 전략 목표 달성을 저해할 가능성이 높은 리스크들을 우선적으로 관리하게 된다.

전략 리스크는 신제품 개발 실패로 인한 매출 하락이나 시장의 신뢰 상실과 같이 영향의 범위가 깊고 넓기 때문에 집중적으로 관리해야 한다. 그 대신 전략 리스크는 특정 전략 하에서만 유효한 리스크이므로, 기업 내에서 잠재적으로 발생 가능한 모든 리스크가 포함되지 않을 수 있다. 반면 운영 리스크는 대부분 부정이나 오류와 같이 영향의 범위가 상대적으로 작기 때문에 관리의 중요성은 전략 리스크에 비해 떨어진다. 그러나 일상적인 운영 리스크 중에서도 안전 사고와 같이 파급 효과가 큰 리스크는 상시적으로 관리해야만 한다.

그런데 전략 리스크는 일반적으로 눈에 보이지 않게 잠재되어 있는 경우가 대부분인데 반해 운영 리스크는 일상적으로 흔히 접할 수 있기 때문에, 보통 ERM을 추진하는 과정에서 전략 리스크보다는 운영 리스크에 매몰될 가능성이 크다. 이처럼 리스크 관리의 중요성보다는 긴급성 차원에만 관심을 빼앗기다 보면, 전략 리스크는 도외시한 채 운영 리스크에만 매달려 본말이 전도된 결과를 가져올 수도 있다. 따라서 ERM의 도입에서 가장 주의해야 할 부분은 무엇보다 기업의 전략 리스크와 운영 리스크간의 균형을 추구하는 것이다. ERM의 본질에 충실하기 위해서는 주로 운영

리스크에만 집중하는 감사 혹은 진단 활동과는 달리, 기업 전략과 연관된 리스크를 어떻게 다룰 것인가에 대한 고민이 중요하다.

3. 선진기업들, ERM 어떻게 활용하나?

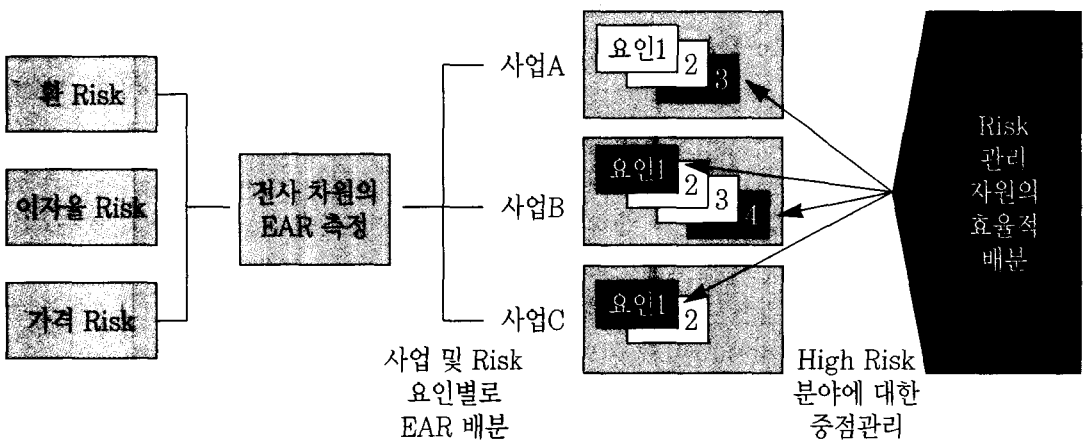
ERM에서 정의하는 리스크란 기업의 목표 달성을 저해하는 모든 요인이다. 그러나 많은 기업들이 리스크 관리를 단지 은행이나 증권사 같은 금융기관만의 문제로 알고 있거나, 이자율이나 환율의 변화에 대처하기 위한 파생금융상품의 활용, 자산부채종합관리(Asset-Liability Management) 등이 리스크 관리의 전부라고 오해하고 있다. 이와 같은 오해를 극복하기 위해 제조업을 중심으로 한 선진기업들의 ERM 활용 실태를 살펴 보자.

● DuPont

듀폰은 ▲전사 리스크 관리 정책(Policy) ▲ 전사 리스크 관리 가이드라인(Guideline) ▲ 라인 관리 전략 및 절차(Strategy & Procedure)로 구성되는 리스크 관리 Framework을 활용하여 ERM을 수행하고 있다. 이처럼 듀폰은 정책 · 지침 · 전략의 3가지 요소로 구성되는 리스크 관리 Framework를 기업 내의 모든 구성원들과 공유함으로써 경영 전략과의 일관성을 추구하고 있다. 결국 리스크 관리란 독립된 개별 프로세스가 아니라 비즈니스 그 자체임을 전 구성원이 인식하고 있는 것이다.

듀폰은 또한 자사의 모든 시장 리스크를 통합적으로 측정하기 위하여 EaR(Earnings at Risk)이라는 통합 지표를 개발했다. 이는 여러 가지 시장 리스크 요인들에 의해 발생 가능한 최대의 이익 감소분을 의미하는데, VaR(Value at Risk)의 개념을 제조업에서도 효과적으로 활용할 수 있도록 하기 위하여 포트폴리오나 재무 포지션의 가치 대신 기업의 리스크 수준을 이익으로 측정하는 방법이다. 듀폰은 전사적 관점에서 EaR을 측정한 후 사업별 · 리스크 요인별로 이를 다시 구분하여 전사 리스크에 대한 각 부문들의 공헌도 및 리스크 수준을 확인하고 이에 따라 리스크 관리 자원 및 역량을 효율적으로 배치하고 있다(〈그림 2〉 참조).

〈그림 2〉 DoPont의 EAR을 활용한 시장 리스크 관리



● **Microsoft**

MS는 1990년대 중반 재무 부서의 리스크 관리 기능을 발전시켜, 전사적 리스크 관리를 수행하는 RMG(Risk Management Group)를 조직했다. 그러나 모든 리스크 관리 활동이 RMG 내에서만 수행되는 것은 아니며, 각 사업부의 경영자 및 관리자 · 재무 · 마케팅 · 법무 등의 스태프들과 긴밀한 협력 및 공조 체제가 구축되어 결과적으로는 MS 전체가 RMG를 중심으로 하나의 리스크 관리 조직이 된 것이다.

MS의 리스크 관리 영역은 크게 재무 리스크 관리(FRM)와 사업 리스크 관리(BRM)로 구분된다. FRM은 주로 VaR(Value at Risk)를 활용하여 이루어지는데, MS에서 VaR는 단순한 측정 지표의 의미를 넘어서 투자자들에게 리스크 수준에 대한 정보를 제공할 뿐만 아니라 실질적인 리스크 대응 활동으로 연결된다. BRM 측면에서는 비재무적인 리스크들을 인지 · 평가하기 위해 Scenario Analysis와 Risk Map을 활용한다. 먼저 Scenario Analysis는 하나의 사건을 단순히 그 결과만으로 평가 · 대응하기보다는 그로 인해 파생될 수 있는 여러 가지 직 · 간접적인 파급 효과들을 찾아내고 그에 대한 대응 방안을 강구하는 것이다. 또한 Risk Map을 활용하여 여러 가지 비재무적 리스크들을 그 심각성과 발생빈도에 따라서 2차원 평면에 배치한다. MS는 80/20 Rule을 적용하여 20%의 주요 리스크들에 대해서 80%의 노력을 집중하여 관리하고 있다.

● **BASF**

바스프는 기업이 관리해야 하는 리스크에 대해서 과거 · 현재 · 미래 등 3차원에서 3중의 안전장치를 두고 입체적인 관리 시스템을 운용하고 있다. 먼저 BASIKS(BASF Information & Communication System)라는 이름의 조기경보시스템을 통해 KRI(Key Risk Indicator)를 측정하고, KRI가 위험한 수준으로 상승하면 리스크 관리 담당자(Risk Owner)에게 즉시 통보하여 필요한 조치를 취할 수 있도록 선행 관리를 수행한다. 다음으로는 동행 관리로서 전사 차원의 리스크에 대해서는 리스크 관리 담당 임원이 분기별로 평가를 실시하고 이에 대한 통제를 수행하며, 사업부 차원의 리스크에 대해서는 12개의 사업부별로 리스크를 관리하고 있다. 마지막으로는 감사팀과 특별위원회가 중심이 되어 사후 모니터링을 실시함으로써, 대응 활동의 적절성 등 리스크 관리 전반에 대해 점검하는 후행 관리를 실시한다.

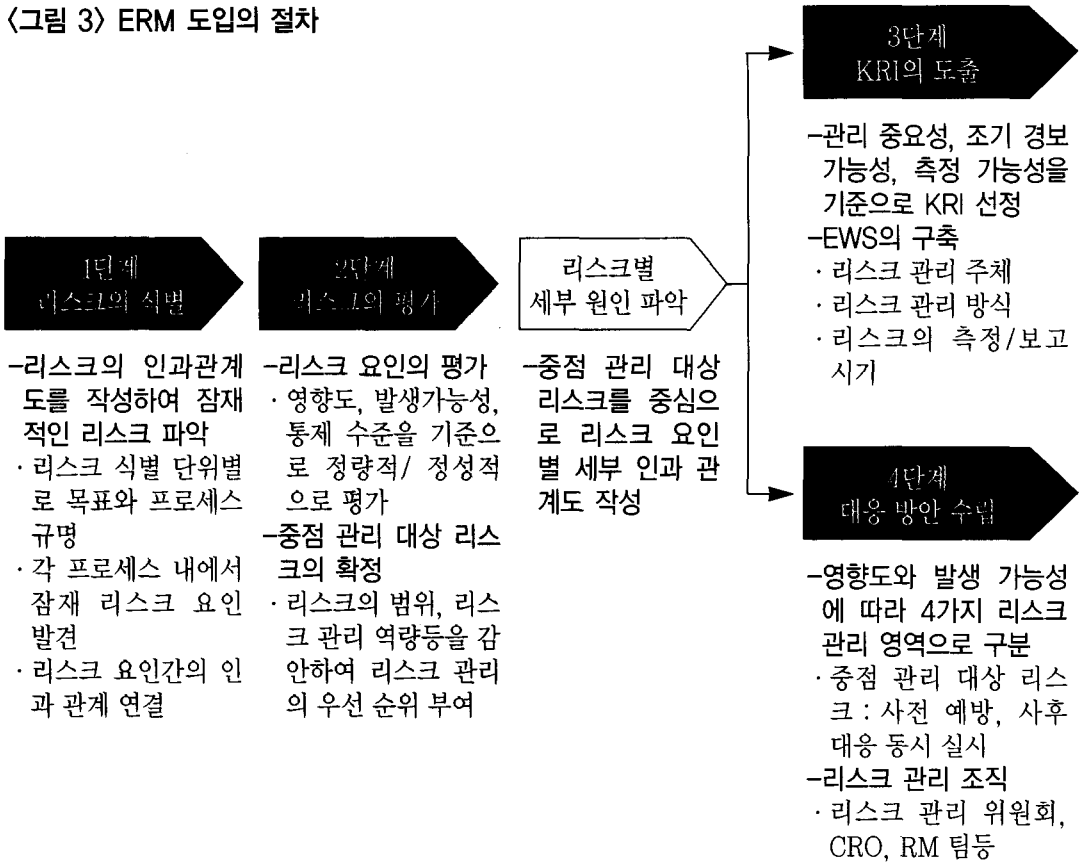
4. ERM, 어떻게 추진할 것인가?

ERM을 도입하기 위한 핵심 절차는 크게 ▲리스크의 식별 ▲리스크의 평가 ▲KRI의 도출 ▲대응 방안 수립의 네 단계로 나누어 살펴볼 수 있다(〈그림 3〉 참조).

● **1단계 : 리스크의 식별**

ERM 도입에서 가장 중요한 과정은 리스크의 식별이다. 리스크 식별의 결과물인 리스크간의 인과관계도(Causal Map) 혹은 영향도(Influence Diagram)를 통해 기업이 미래에 처할 수 있는 모든 잠재적인 리스크를 한 눈에 파악할 수 있기 때문이다. 그런 점에서 이 단계는 ERM의 인프라를 닦는 작

〈그림 3〉 ERM 도입의 절차



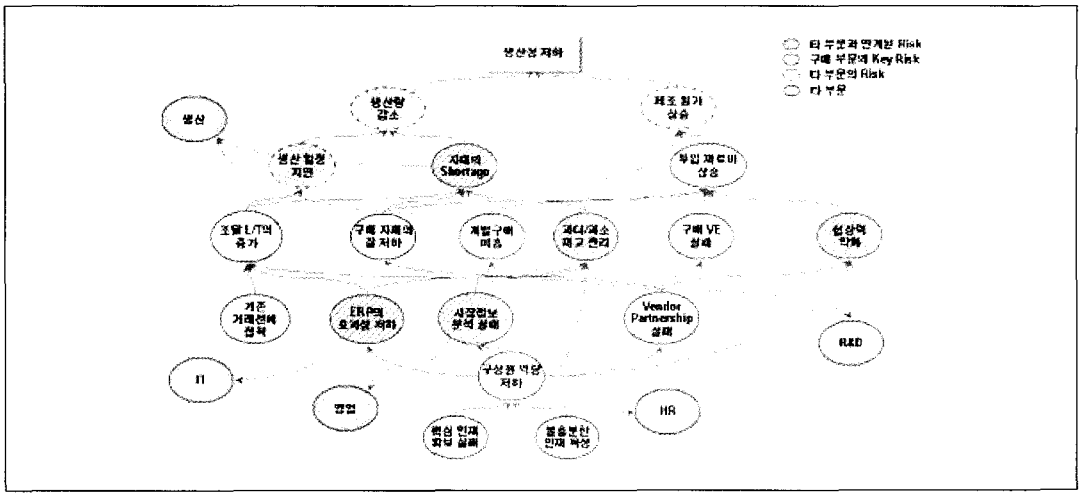
업이라고 할 수 있다.

여기서 인과관계도를 작성하는 목적은 전사 목표(Objective)의 달성을 저해할 수 있는 잠재적으로 발생 가능한 모든 리스크를 파악하기 위해서이다. 특히 발생 가능한 리스크를 나열하는 데 그치지 않고 각 리스크 간의 인과관계까지 파악하는 일은 매우 중요하다. 개별 리스크가 어떤 위치를 차지하고 있는지 각 리스크의 유기적 관계를 입체적으로 파악함으로써, 어떤 리스크 요인이 전사 목표 달성에 가장 애로(Bottleneck) 요인으로 작용할 수 있는지를 직관적으로 이해할 수 있기 때문이다(〈그림 4〉 참조).

리스크 식별 과정에서 전사 목표를 저해할 수 있는 모든 잠재적인 리스크 요인을 포함하고 이를 효과적으로 보여 주기 위해서는 두 가지 작업을 먼저 수행해야 한다. 첫째는 리스크 식별 단위를 적절히 구분하는 것이고, 둘째는 리스크 범주를 확정하는 것이다.

먼저 리스크 식별 단위를 살펴 보자. 리스크 식별 단위의 구분으로는 사업부별 구분과 기능별 구분의 두 가지 대안을 생각해 볼 수 있다. 사업부별 구분은 전사 목표를 사업부별 목표로 분해한 후, 각 사업부별 목표 달성을 저해하는 리스크 요인을 찾아내는 과정을 거친다. 반면 기능별 구분은 전사 목표를 달

〈그림 4〉 Risk Causal Map의 예 (구매부문)



성하기 위한 각 기능별 목표를 규명한 후, 이를 저해하는 리스크 요인을 찾아낸다. 두 가지 방법 모두 장·단점이 존재하지만, 사업부별 구분의 경우 사업부간에 목표와 리스크 요인이 크게 다르지 않을 가능성이 커서 효과성 측면에서 다소 의문의 여지가 있다. 반면 기능별 구분의 경우에는 각 기능별로 목표가 뚜렷이 구분되고, 이에 따라 리스크 요인의 차이도 명확히 나타나는 장점이 있다.

다음으로는 각 기업이 속해 있는 산업별 특성에 따라 리스크 범주를 확정한다. BASF는 ▲통화 ▲산업/규제 ▲공급 등 8개의 범주로, Cisco는 ▲M&A ▲정치 ▲규제 ▲기술 ▲재난 등 10개의 범주로 나누어 자사의 리스크를 식별하고 있다. ERM을 도입하고자 하는 주류 기업들 역시 Anheuser-Busch, Diageo, Heineken, Kirin Brewery 등 선진 주류 기업들에 대한 벤치마킹을 통해 그들이 어떤 리스크를 관리 대상으로 삼고 있는지를 살펴 보는 작업이 필요하다. 그들과 자사의 차이점을 비교함으로써, 자사가 식별한 Risk Pool의 적정성을 검증해 볼 수 있다. 이처럼 기업 내의 리스크를 구조화하여 구체적인 범주로 확정하고 이를 전 구성원들과 공유함으로써, 의사소통에 필요한 리스크 관리의 공통 언어(Common Language)를 마련할 수 있다.

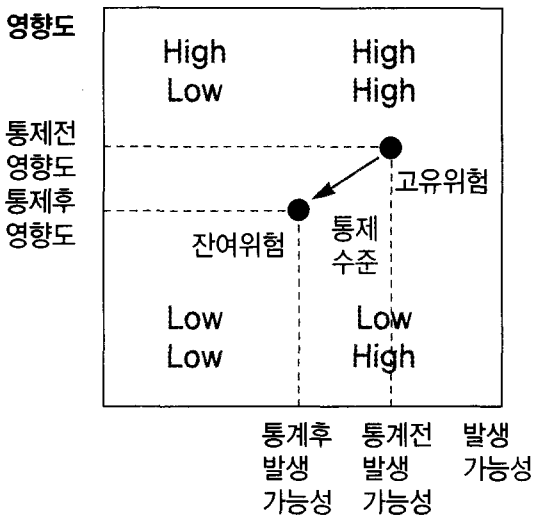
마지막으로 리스크 요인을 실제로 식별하기 위한 활동으로서, 앞에서 구분해 놓은 리스크 식별 단위별로 목표와 프로세스를 규명하고 각 프로세스간 업무 흐름을 파악한다. 그리고 각 프로세스별 활동 속에서 벌어질 수 있는 리스크 요인을 찾아내고 리스크 요인간의 인과관계를 파악하여, 각 리스크 식별 단위별로 인과관계도를 완성한다. 인과관계도를 작성할 때는 각 리스크가 목표와 얼마나 직접적인 관계를 지니고 있는지를 보여 주기 위해 리스크 요인의 계층(Hierarchy)을 제대로 표현해 주는 것이 중요하며, 리스크 식별 단위를 기능별로 구분한 경우에는 기능 내의 리스크 요인이 타 기능의 리스크 요인과 어떻게 연결되는지를

밝히는 것에 유의해야 한다.

● 2단계 : 리스크의 평가

1단계의 리스크 식별 단계에서 잠재적으로 발생 가능한 리스크를 모두 찾아낸 후에는, 그 중에서 전사 차원에서 우선적으로 관리해야 할 리스크를 선정하기 위해 리스크의 평가를 수행한다. 리스크의 평가는 먼저 해당 리스크가 조직의 목표 달성에 얼마나 큰 영향을 미치는지를 나타내는 영향도(Impact)와 해당 리스크의 발생 빈도를 나타내는 발생가능성(Frequency)을 이용하여 고유 리스크(Inherent Risk)를 구한다. 그리고 나서 각 고유 리스크의 영향도와 발생가능성을 줄이기 위한 기업의 통제수준(Control Level)을 감안하여 잔여 리스크(Residual Risk)를 평가한다(〈그림 5〉 참조).

〈그림 5〉 리스크의 평가과정



이와 같이 고유 리스크→통제수준→잔여 리스크를 순차적으로 구하는 이론적 접근법은 논리적으로 명쾌한 구조를 지니고 있고, 각 리스크 요인별로 통제수준에 대한 정보를 세세하게 분석함으로써 향후 대응 방안 설계를 용이하게 할 수 있다는 장점이 있다. 그러나 평가 과정이 복잡할 뿐 아니라, 현실 속에서 구성원들이 인식하고 있는 리스크는 잔여 리스크이므로 고유 리스크만을 따로 떼어내어 평가하는 것이 오히려 평가 과정에 왜곡을 가져올 수도 있다.

따라서 이를 극복하기 위한 현실적인 대안으로, 통제 후의 영향도와 발생가능성을 기준으로 잔여 리스크를 직접 평가하는 방법을 생각해 볼 수 있다. 이 경우에도 평가자들이 리스크 요인별로 점수를 부여한 후에, 이 리스크 요인간의 서열을 다시 한 번 살펴 보며 순위와 점수를 재조정하는 작업을 거침으로써 평가 과정에서의 Bias를 최소화시킬 필요가 있다.

● 3단계 : KRI의 도출

2단계에서 전략 차원의 평가와 운영 차원의 평가를 거쳐 중점관리 대상 리스크를 확정한 후에는, 이 리스크를 제대로 측정할 수 있는 KRI를 도출하는 작업과 KRI가 높은 리스크에 대한 적절한 조치를 취하는 단계가 남아 있다. 먼저 KRI의 도출을 위해서는 중점 관리 대상 리스크가 발생하는 구체적인 원인을 파악해야 하는데, 이를 위해 세부 인과관계도를 작성한다. 중점 관리 대상 리스크의 개수 만큼 작성된 세부 인과관계도는, 3단계에서 KRI를 도출하는 작업과 4단계에서 리스크별 대응 방안 수립의 기초 자료로 활용된다. 개별 리스크의 발생 원인을 제대로 찾아내지 못할 때에는 도출된 KRI와 대응 방안은 무의미하므로, 3단계와 4단계 작

업 이전에 구성원들과의 충분한 워크샵을 통해 합의를 이루는 과정은 매우 중요하다.

만약 리스크 평가를 연중 지속적으로 수행할 수 있다면 KRI를 따로 선정할 필요가 없을 것이다. 매일의 리스크 평가 결과에서 나온 중점 관리 대상 리스크에 대한 대응 활동만을 수행하면 되기 때문이다. 그러나 이와 같은 리스크 평가는 시간과 비용이 매우 많이 소요되기 때문에, 1년에 1~2번 밖에는 실시할 수 없다는 한계를 지니고 있다. 따라서 기업을 위기에 빠뜨릴 수 있는 리스크에 대한 대비책을 마련하고자, 리스크의 발생 가능성을 사전에 측정하고자 하는 것이 KRI의 도입 목적이다.

KRI를 선정하는 원칙은 ▲관리 중요성 ▲조기 경보 가능성 ▲측정 가능성 등의 3가지로 요약할 수 있다. 첫째, 관리 중요성 원칙은 목표 달성을 저해하는 핵심 리스크 요인을 중심으로 지표를 선정해야 함을 말한다. 이 관리 중요성 원칙이 충족되기 위해서는, 먼저 리스크 식별 단계의 산출물인 각 기능별 리스크 인과관계도와 중점 관리 대상 리스크별로 심층 분석한 세부 인과관계도가 제대로 작성되어 있어야 한다. 앞 단계의 작업이 충실히 수행되지 않고서는, 전사의 목표부터 일선 구성원들의 행위(Activity)로 인해 야기될 수 있는 리스크를 연결하는 데 일관성을 확보할 수 없기 때문이다. 관리 중요성이 높은 KRI를 선정함으로써 기업은 리스크 관리의 타당성(Validity)을 제고할 수 있고, 구성원들 역시 자신의 업무가 얼마나 리스크에 노출되어 있는지를 알게 됨으로써 경각심을 일깨우고 동기 부여를 꾀할 수 있다.

둘째, 조기 경보 가능성 원칙은 리스크 발생 정도를 측정하는 후행 지표(Lagging Indicator)는 물론이고 향후 리스크의 발생 가능성을 사전에 알려 줄 수 있는 선행 지표(Leading Indicator)를 찾아내야 함을 말한다. 여기서 후행 지표는 리스크 요인을 직접 평가할 수 있는 지표를 중심으로 선정하고, 선행 지표는 리스크 요인별 세부 인과관계도상에서 주요 원인을 평가할 수 있는 지표를 중심으로 선정한다. 이를 통해 리스크 요인별로 원인과 결과를 입체적으로 관리할 수 있고, 특히 리스크 발생 원인을 사전에 제거할 수 있는 효과를 누릴 수 있다.

셋째, 측정 가능성은 비용이나 노력이 덜 소요되는 지표를 중심으로 선정함으로써 리스크 관리의 효율성을 제고해야 한다는 의미이다. 여기서 한 가지 주의해야 할 것은, 각 지표가 사업부별 혹은 측정 시점별로 일관성을 확보함으로써 비교가능성을 제고할 수 있어야 한다는 점이다. 지표는 개별적으로 지니는 의미보다는 다른 사업부와의 비교를 통해 자원 투입의 우선순위를 결정하거나, 기간별 비교를 통해 리스크 노출 정도의 변화를 파악할 수 있어야 하기 때문이다.

이렇게 선정한 KRI는 조기 경보 시스템(Early Warning System : EWS)을 활용해 관리해야 한다. EWS를 구축하기 위해서는 KRI별로 ▲Who ▲How ▲When 등 3가지 요소가 포함되어야 한다. 즉 리스크 요인별로 KRI를 산출하고 이에 대한 대응 방안을 수립하는 리스크 관리 주체를 임명하고(Who), 리스크 요인별로 KRI의 산식과 평가 척도 및 측정 방식 등에 대해 합의하며(How), 리스크의 측정 및 보고 주기를 결정하는(When) 작업이 그것이다.

여기서 EWS란 반드시 IT를 활용한 시스템을 말하는 것은 아니며, 위기의 징후를 미리 감지하여 이를 해당 의사결정자나 위원회 등에 보고함으로써 이에 대한 대응책을 준비할 수 있는 체계를 의미하는 것이다. 따라서 리스크를 측정하고 보고하는 데 드는 시간과 노력이 과도하다는 판단이 들 때에만 IT로 구현하는 것이 합리적이다. IT는 문제를 보다 쉽게 해결해 줄 수 있는 하나의 도구는 될 수 있어도, 그 자체로서 문제를 해결해 줄 수는 없다는 사실을 잊지 말아야 할 것이다. 일단 수작업으로 조기 경보 시스템을 운영하여 이의 효과성을 기업 내부에서 검증한 후, 이를 보다 효율적으로 운영하기 위해 IT의 도입 여부를 결정하는 것이 바람직하다. 효과성을 검증하지도 않은 채 IT 시스템부터 도입했다가, 제대로 활용도 하지 않은 채 썩히는 경우가 얼마나 많은지 한 번 상기해 볼 일이다.

● 4단계 : 대응 방안 수립

이제는 마지막으로 위기 발생 가능성을 높이고 전략 목표 달성에 걸림돌이 될 수 있는 리스크를 줄이기 위한 행동을 시작해야 할 때이다. 이와 같은 리스크에 대한 대응 방안 수립은 역시 2단계의 리스크 평가 결과를 기초로 하여 이루어지게 된다.

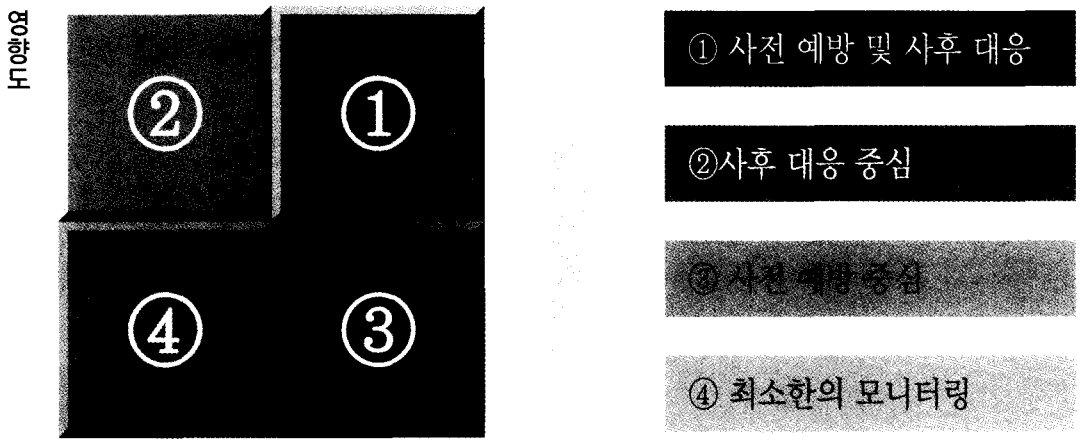
먼저 발생가능성도 높고 영향도도 높은 ① 분면의 경우, 사전 예방과 사후 대응을 동시에 실시해야 한다는 측면에서 이 영역에 포함된 리스크들을 중점 관리 대상 리스크라 부를 수 있다. 최고경영자를 중심으로 하는 회의체에서 리스크를 주기적으로 모니터링하여 대응 방안을 수립하고, 즉각적인 대응이 필요한 리스크에 대해서는 중요성에 따라 CRO(Chief Risk Officer) 혹은 최고경영자의 의사결정으로 조치를 취하게 된다.

발생가능성은 낮지만 영향도가 높은 ②분면의 리스크들에 대해서는 주로 사후 대응 차원에서 컨틴전시 플랜 등을 수립하여 리스크 발생시 피해 발생을 최소화시키기 위한 대비책을 마련한다. ③분면의 경우 영향도는 낮지만 발생가능성은 높은 리스크로서, 이 리스크들에 대해서는 주로 발생 빈도를 감소시키기 위한 사전 예방 활동에 힘을 기울인다. 마지막으로 ④분면의 경우 영향도와 발생가능성이 모두 낮은 영역으로서, 이는 비용-효익 측면에서 볼 때 수용 가능한 리스크라고 볼 수 있으므로 최소한의 모니터링이 가능한 수준의 리스크 관리 자원을 배치하면 될 것이다(〈그림 6〉 참조).

전사 차원의 리스크 관련 최고 의사결정은 CEO를 중심으로 하는 리스크 관리위원회나 이사회에서 수행하는 것을 유력한 방안으로 생각해 볼 수 있다. 다만 이들은 상설 조직이 아니므로, 평소에는 CRO가 리스크 관리 전담 팀을 이끌면서 일상적인 리스크 모니터링 및 대응 활동을 수행하게 된다. CRO는 전사 차원의 리스크 모니터링을 수행하다가 리스크 관련 중요 사안이 돌출할 경우에는, 즉각적인 대응이 가능하도록 리스크 관리위원회의 소집을 제안할 수 있다.

CRO나 리스크 관리 조직의 성격을 어떻게 규정하느냐도 하나의 이슈가 될 수 있는데, 이는 결국 기업 내에서 ERM의 위상을 어떻게 규정할 것인가의 문제와 연결된다. 어떤 경우든 ERM이란 결국 전략 수행의 이면에 숨겨진 리스크를 놓치지 않고 잘 관리

〈그림 6〉 리스크별 대응방안의 수립



하는 것이라고 볼 수 있기 때문에, CRO는 전략 수립 부서와 긴밀하게 협업하는 것이 필요하다. 만약 독립된 CRO를 설치하기 어려운 경우에는 전략 수립 부서에 추가적인 모니터링과 대응 방안 수립 기능을 부여하여 리스크 관련 최고 의사결정을 지원하는 것이 바람직할 것으로 판단된다.

5. ERM을 통해 무엇을 얻을 것인가?

기업이 ERM을 통해 얻을 수 있는 효과를 요약하면 크게 두 가지이다. 첫째, 기존에 인식하지 못하고 있던 리스크를 인식하고 관리하는 것이다. 둘째, 기존에 알고 있던 리스크를 개별적으로 대응하는 차원을 넘어서 전사 관점에서 공유하고 통합적으로 대응하는 것이다.

그러나 이미 대부분의 주류 기업들이 신생기업이 아닌 이상, 비록 통합적이지는 못하지만부서별로 체계적이든 비체계적이든 어느 정도의 리스크 관리는 수행하고 있을 것이다. 따라서 ERM 도입 초기에 전혀 모르던 새로운 리스크를 찾아낸다는 것은 결코 쉽지 않은 일이다. 이는 ERM을 도입하면 기업을 한 순간에 망하게 만들 수도 있는 엄청난 리스크를 찾아내고 대응책을 마련해 줄 것으로 기대하던 경영자에게는 실망스런 일일 수도 있다.

하지만 우리가 정기적으로 종합 검진을 받는 이유가 어디에 있는가? 평소에 부분적으로나마 건강 관리를 하기 때문에 아무런 병이 발견되지 않은 것을 두고 종합 검진의 효과를 부정할 수는 없지 않는가? 대신 종합 검진을 받은 후에는 작은 증상이라 할지라도 이를 전체적인 관점에서 살펴 보며 종합적인 개선 방안을 찾을 수 있기 때문이다.

ERM도 마찬가지이다. 개별 부서 차원에서 모르고 있던 잠재 리스크를 인식하기 위해서는 기본적으로 리스크를 찾아낼 수 있는 구성원들의 안목(Intelligence)이 높아져야 한다. 하지만 ERM을 도입한다고 해서 갑자기 없던 역량이 생겨날 수는 없는 일 아닌가? 이는 보다 장기적인 관점에서 학습을 통해서 조직의 리스크

관리 역량을 높일 때에야만 가능한 일이다.

대신 전사 차원의 관점에서 볼 때는 매우 중요한 리스크가 개별 부서 혹은 사업부만의 대응으로 인해 더 크게 번질 수도 있는 가능성을 차단할 수도 있고, 반대로 전사 차원에서 보면 별 것 아닌 리스크에 대해 지나친 노력의 투입을 조정해 주는 것이 ERM을 통해 얻을 수 있는 단기적인 효과라고 할 수 있을 것이다. 실제로 개별 부서 혹은 사업부의 리스크를 전사 차원의 포트폴리오로 구성해 보면, 리스크간의 상쇄 혹은 증폭으로 인해 리스크 관리의 우선 순위가 바뀔 수도 있다.

리스크 관리에도 왕도는 있을 수 없다. 리스크 관리에 기업들이 관심을 쏟는 것은 반가운 일이지만, ERM 역시 한 때의 열풍으로만 끝나지 않을까 하는 우려가 먼저 앞서는 것도 사실이다. 도입하자마자 큰 성과를 낼 것으로 기대했다가, 기대했던 효과를 보지 못했다고 금방 집어 치우는 우를 범하지는 말자. 초우량 기업들의 리스크 관리도 알고 보면 오랜 기간 동안 조금씩 조금씩 진화해 온 결과이다. 리스크 관리 체제를 확립하고 구성원들의 리스크 마인드를 제고하다 보면, 어느 순간 리스크 관리가 기업 경영에 체화되어 있을테고 결국 그것이 기업 목표의 달성 가능성을 높여 줄 수 있는 주춧돌이 될 것이다.

[참고 문헌]

- 고재민, "ERM 도입을 위한 실무 가이드(Ⅰ)(Ⅱ)", 〈LG 주간경제〉 제781 · 784호, 2004.
- 김종호, "전사적 위험관리 : 개념과 사례", LG경제연구원, 2004.
- Thomas L. Barton, William G. Shenkir, Paul L. Walker, "Making Enterprise Risk Management Pay Off", Prentice Hall Publishing, 2002.
- "Enterprise Risk Management : An Analytical Approach", Tillinghaust - Towers Perrin Publication, 2000.
- Robert Simons, "How Risky Is Your Company", HBR, 1999.