

# 전사적 리스크 관리 - 통합 프레임워크

## Enterprise Risk Management – Integrated Framework

---

### Executive Summary

September 2004



## 경영자 개요

전사적 리스크 관리의 기본 전제는 모든 회사가 이해관계자에게 가치를 제공하기 위해 존재한다는 것이다. 그런데 모든 회사는 불확실성에 직면해 있으므로, 경영자의 과제는 이해관계자의 가치를 증가시키기 위해 수용할 수 있는 불확실성의 정도를 결정하는 것이다.

불확실성은 잠재적으로 가치를 감소 또는 증가시킬 수 있는 리스크와 기회를 동시에 제공한다. 전사적 리스크 관리의 경영자가 불확실성으로 인한 리스크와 기회를 효과적으로 다룰 수 있도록 함으로써 기업가치 향상에 기여한다.

기업 가치는 경영자가 성장, 목표이익 및 이와 관련된 리스크 간의 최적 균형을 바탕으로 전략과 목표를 수립하고, 기업의 목표를 달성하기 위해 자원을 효율적이고 효과적으로 배치할 때 극대화된다. 전사적 리스크 관리의 내용은 포함한다.

- **리스크 선호도와 전략의 정렬** – 경영자는 전략적 대안을 평가하고 관련 목표를 수립하며 이에 따른 리스크 관리 메커니즘을 개발하는 과정에서 회사의 리스크 선호도를 고려한다.
- **리스크 대응의 강화** – 전사적 리스크 관리의 리스크를 식별하고 리스크 대응방안(리스크 회피, 감소, 공유, 수용)을 선택할 수 있는 정교한 방법을 제공한다.
- **예상하지 못한 운영상의 손실 감소** – 기업은 잠재적인 사건을 식별하고, 대응방안을 수립할 수 있는 향상된 능력을 갖게 되어, 예상치 못한 일의 발생과 그로 인한 비용 및 손실을 감소시킬 수 있다.
- **복합적·전사에 걸친 리스크의 식별과 관리** – 모든 회사는 조직의 각기 다른 부문에 영향을 미치는 수많은 리스크에 직면해 있는데 전사적 리스크 관리의 상호 연관되어 있는 리스크에 대한 효과적인 대응과 복수의 리스크에 대한 통합된 대응을 가능하게 한다.
- **기회 포착** – 경영자는 모든 잠재적 사건을 고려함으로써 기회를 식별하여 혁신적으로 실현할 수 있게 된다.
- **자본 배분의 개선** – 경영자는 확실한 리스크 정보를 통해 자본 수요를 파악하고 효과적으로 자본을 투입할 수 있게 된다.

이러한 전사적 리스크 관리의 고유특성은 경영자가 회사의 성과 및 수익성 목표를 달성하고 자원 손실을 예방하는 데 도움을 준다. 또한, 전사적 리스크 관리의 효과적인 보고체계 수립 및 법과 규제 준수를 통해 회사 명성의 손상이나 그에 따른 손해를 피할 수 있도록 한다. 즉, 전사적 리스크 관리의 회사가 추구하는 목표에 도달하는 과정에서의 위험과 예상치 못한 사건을 감소시킬 수 있도록 도와준다.

### 사건 – 리스크와 기회

사건은 부정적/긍정적인 영향 또는 두 가지 영향을 동시에 줄 수 있다. 부정적인 영향을 주는 사건은 가치 창출을 방해하거나 현존하는 가치를 감소시킬 수 있는 리스크를 의미한다. 반면에 긍정적인 영향을 주는 사건은 부정적인 영향을 상쇄하거나 새로운 기회를 의미한다. 기회란 사건이 발생하여 가치를 창출하거나 보존하면서, 목표 달성에 긍정적인 영향을 미칠 가능성이 있다. 경영자는 기회를 전략 또는 목표 수립 프로세스로 돌려 보냄으로써 기회포착을 위한 실행계획이 수립된다.

### 전사적 리스크 관리 정의

전사적 리스크 관리는 가치 창출 또는 보존에 영향을 미치는 리스크와 기회를 다룬다. 전사적 리스크 관리의 정의는 다음과 같다.

*전사적 리스크 관리는 회사목표 달성에 대한 합리적인 확신을 제공하기 위해 이사회, 경영자 그리고 모든 직원에 의해 만들어지며, 전략 수립과 기업전반에 적용되며, 회사에 영향을 주는 잠재적 리스크를 식별하고 해당 리스크를 리스크 선호도 내에서 관리하기 위해 설계된 프로세스이다.*

위의 정의는 다음과 같은 기본적 개념을 반영한다. 전사적 리스크 관리는:

- 회사 전체적으로 계속적으로 진행되고 있는 프로세스이다.
- 조직의 모든 계층에 속한 사람들에 의해 만들어진다.
- 전략 수립에 적용된다.
- 모든 계층과 구성 단위를 통한 기업 전반에 적용되고, 전사 차원에서의 리스크 포트폴리오 (portfolio)관점을 포함한다.
- 발생시 회사에 영향을 미치는 잠재적 사건을 식별하고, 리스크 선호도 내에서 리스크를 관리하도록 설계되어 있다.
- 회사 경영자와 이사회에 합리적인 확신을 제공할 수 있다.
- 상호 연관성 있는 다양한 범주에서 목표 달성이 가능토록 설계되어 있다.

위의 정의는 다소 광범위한데 그 이유는 이와 같은 정의가 조직, 산업 및 각 분야에서 전반적으로 적용 가능한 원리를 제공하면서, 회사 또는 다른 조직이 리스크를 다루는 방법에 대한 기본적인 핵심 개념을 제공하기 때문이다. 그리고 특정 회사의 목표 달성에 직접적으로 초점을 맞추고 있으며 전사적 리스크 관리의 효과성을 정의하기 위한 기본토대를 제공한다.

## 목표 달성

회사가 수립한 미션과 비전의 범위 내에서, 경영자는 전략적 목표를 수립하고, 전략을 선택하며 해당 전략과 정렬되고 회사 전반에 걸쳐 단계적으로 수행될 목표를 설정한다. 이러한 전사적 리스크 관리의 프레임웍(framework)은 아래 네 가지 범주로 설명된 회사의 목표를 달성하도록 설계되어 있다.

- **전략** – 회사의 미션과 정렬되어 있는 가장 높은 수준의 목표
- **운영** – 회사의 자원을 효과적이고 효율적으로 사용하는 목표
- **보고** – 보고의 신뢰성을 갖는 목표
- **준수** – 회사에 적용되는 법과 규제준수의 목표

회사 목표의 범주화는 전사적 리스크 관리가 구분되어 있는 각 측면에 초점을 맞출 수 있게 한다. 이와 같이 구분되지만 일부분 겹쳐있는 범주들은—특정 목표는 하나 이상의 범주에 속할 수 있다—회사의 서로 다른 필요사항을 설명하고, 해당 경영진이 직접적인 책임을 져야 함을 암시한다. 또한 범주화는 각각의 목표 범주에서 기대될 수 있는 것들이 서로 구별되도록 한다. 일부 회사에서 사용되는 또 다른 범주인 자원의 보호(safeguarding of resources)도 이와 같은 맥락에서 설명된다.

보고의 신뢰성 및 법과 규제의 준수에 관련된 목표들은 회사의 통제 내에 있기 때문에 전사적 리스크 관리가 해당 목표 달성에 관한 합리적 확신을 제공할 수 있을 것으로 기대된다. 반면에 전략적 목표와 운영 목표의 달성은 항상 회사 통제 내에 있는 것이 아니라 외부 사건에 의해 영향을 받는다. 전사적 리스크 관리는 경영자와 감독 책임이 있는 이사회가 기업이 목표 달성을 위해 어느 수준으로 운영되고 있는지를 적절한 시기에 인식할 수 있도록 하여, 합리적 확신을 갖도록 해준다.

## 전사적 리스크 관리의 구성요소

전사적 리스크 관리는 여덟가지의 상호 연관되는 구성요소로 이루어져 있다. 이 요소들은 경영자가 기업을 운영하는 방법으로부터 도출되고 관리 프로세스로 통합된다. 이 요소들은 다음과 같다.

- **내부 환경(Internal Environment)** : 내부 환경은 조직의 분위기를 포함하고 회사 조직원이 리스크와 통제를 검토하고 다루는 방법의 토대를 이룬다. 또한 리스크 관리 철학과 리스크 선호도, 조직 구성원의 도덕성, 윤리가치 그리고 환경을 포함한다.
- **목표 수립(Objective Setting)** : 목표는 경영자가 목표 달성에 영향을 미치는 잠재적 사건들

을 식별하기 전에 존재해야 한다. 전사적 리스크 관리는 경영자가 목표를 수립하는 프로세스를 제대로 가지고 있고, 선택된 목표가 회사의 미션을 지원하고 미션과 정렬되어 있으며 리스크 선호도내에 있음을 보증한다.

- **사건 식별(Event Identification)** : 회사의 목표 달성에 영향을 줄 수 있는 내부나 외부 사건은 식별되어야 한다. 목표에 긍정적인 사건은 기회, 부정적인 사건은 리스크라고 정의한다. 식별된 기회는 경영자의 전략 또는 목표수립 프로세스로 전달되어 다시 고려된다.
- **리스크 평가(Risk Assessment)** : 리스크는 그것들이 어떻게 관리되어야만 하는지를 결정하기 위한 토대로서 리스크 발생 가능성과 영향도를 고려하여 분석되며, 고유 리스크와 잔여 리스크에 대해 평가가 수행된다.
- **리스크 대응(Risk Response)** : 경영자는 리스크 대응방안—회피, 수용, 감소 또는 공유—을 선택하는데, 대응방안은 발견된 리스크들을 회사의 리스크 허용한도와 리스크 선호도내에 있게 하기 위한 실행계획을 개발하는 것이다. .
- **통제 활동(Control Activity)** : 정책과 절차가 리스크 대응이 효과적으로 수행된다는 것을 보증하기 위해 수립되고 수행된다.
- **정보와 의사소통(Information & Communication)** : 관련 정보는 조직 구성원이 적절하게 자신의 책임을 수행할 수 있도록 정해진 시간 내에 적절한 형태로 인식, 파악, 의사소통 된다. 효과적인 의사소통은 발생하여 조직의 상하좌우로 순환한다.
- **모니터링(Monitoring)** : 전사적 리스크 관리의 모든 것은 모니터링되며 필요에 따라 수정된다. 모니터링은 상시 모니터링, 독립 평가 또는 두 가지의 조합으로 수행된다.

전사적 리스크 관리는 한 구성요소가 오직 그 다음 요소에만 영향을 주는 순차적인 프로세스는 아니다. 대부분의 구성 요소가 서로 다른 요소에 영향을 줄 수 있고 실제로 영향을 주고 있는 다각적이고 반복적인 프로세스이다.

### 목표와 구성요소간의 관계

기업이 달성하려고 노력하는 목표와 목표 달성을 위해 필요한 전사적 리스크 관리의 구성요소는 상호 밀접한 관련이 있다. 이 관계는 큐브의 형태의 3차원 매트릭스로 표현된다.

네 가지 목표의 범주 (전략, 운영, 보고, 준수)는 수직열에, 여덟 가지 구성요소는 수평행에, 회사 조직은 3차원 측면에 나타나 있다. 이것은 회사의 단계별 조직이 네 가지 목표로 분류된 자신의 목표 달성을 위해 여덟 가지 요소의 프로세스로 리스크를 관리한다는 것을 의미한다.

## 효과성

회사의 전사적 리스크 관리가 효과적인지 여부는 여덟 가지 구성요소가 존재하고 각 요소들이 효과적으로 기능을 수행하는가에 따라 판단된다. 그러므로, 구성요소들은 효과적인 전사적 리스크 관리에 관한 기준이 된다. 여덟 가지 구성요소들이 존재하는 동시에 적절하게 기능을 수행하기 위해서는 중대한 취약점이 없어야 하고 리스크는 회사의 리스크 선호도 내에 존재해야 한다.



전사적 리스크 관리가 네 가지 목표 범주에 대해 효과적으로 운영되면, 이사회와 경영자는 그들이 회사의 전략과 운영 목표가 달성된 정도를 이해하고 있고 회사의 보고가 신뢰성 있으며 회사에 해당되는 법과 규제가 준수되고 있다는 합리적인 확신을 가질 수 있다.

여덟 가지 구성요소는 모든 회사에서 동일하게 적용되지는 않는다. 예를 들어, 중소기업의 경우, 대기업에 비해 정형화와 구조화가 많이 되어 있지 않을 수 있다. 그럼에도 각각의 구성요소들이 존재하고 그것들이 적절히 상호 작용하는 한 중소기업도 효과적인 전사적 리스크 관리 체계를 구축할 수 있다.

## 한계

전사적 리스크 관리는 중요한 효익을 제공하지만, 한계도 존재한다. 위에서 언급된 사항뿐만 아니라, 의사결정에서의 인간판단에 오류가 존재한다는 사실, 리스크에 대한 대응과 통제 수립은 관련된 비용과 이익을 고려해야 한다는 사실, 단순한 실수 또는 판단착오와 같은 인간의 한계로 인해 오류가 발생할 수 있다는 사실, 두 사람 이상의 공모에 의해 무력화될 수 있다는 사실, 경영자가 전사적 리스크 관리 결정을 무시할 수 있다는 사실 등은 한계로 지적된다. 이러한 한계는 이사회와 경영자가 회사 목적 달성에 대한 절대적 확신을 가질 수 없도록 한다.

## 내부 통제 포함

내부 통제는 전사적 리스크 관리에 통합되는 일부분이다. 전사적 리스크 관리 프레임워크는 더욱 확고한 개념화와 관리 도구를 형성하면서 내부 통제를 포괄하고 있다. 내부 통제는 내부 통제-통합 프레임워크에서 정의되고 설명된다. 당 프레임워크는 오랜 기간 검증되었고, 현행 규칙·규제·

## 경영자 개요

---

법을 토대로 하고 있기 때문에 내부 통제에 대한 정의와 프레임워크로 계속 유효하다. 그런데 내부 통제-통합 프레임워크 중 일부만을 당 프레임워크에서 다루고 있으므로 전문이 이 프레임워크에 대한 참조로 활용될 수 있다.

### 역할과 책임

회사의 모든 구성원은 전사적 리스크 관리에 대해 어느 정도 책임을 가지고 있다. CEO는 궁극적인 책임을 지고 소유권(ownership)을 가져야 한다. 한편, 다른 관리자들은 회사의 리스크 관리 철학을 지지하고, 리스크 선호도 준수를 장려하며, 리스크 허용한도에 부합하는 책임 범위 내에서 리스크를 관리한다. 또한, 리스크 책임자, 재무 담당자, 내부 감사인 그리고 다른 구성원은 중요한 역할을 수행한다. 다른 회사 구성원은 정해진 지침과 프로토콜을 따르며 전사적 리스크 관리를 수행해야 하는 책임이 있다. 이사회는 전사적 리스크 관리에 대한 감독 기능을 수행하고, 회사의 리스크 선호도를 파악하고 이에 동의한다. 고객, 벤더, 비즈니스 파트너, 외부 감사인, 규제기관, 재무 분석가는 전사적 리스크 관리에 영향을 미치는 유용한 정보를 제공한다.

### 당 보고서의 구조

본 보고서는 두 권으로 되어 있다. 제1권은 경영자 개요(Executive Summary)와 프레임워크(Framework)를 포함하고 있다. 프레임워크(Framework)은 모든 경영층과 각각의 조직이 전사적 리스크 관리의 효과성을 평가하고 강화하는데 사용하는 지침을 제공하면서, 전사적 리스크 관리를 정의하고 원리와 개념을 설명한다. 본 경영자 개요(Executive Summary)는 최고 경영자, 상위 경영진, 이사회 멤버, 규제기관을 대상으로 하는 높은 수준의 개관이다. 제2권인 적용 기법(Application Techniques)은 프레임워크 요소들을 적용하는 데 유용한 기법의 예시를 제공한다.

### 당 보고서의 이용

본 보고서의 결과로서 제안된 행동은 다음 각 주체들의 위치와 역할에 따라 달라진다.

- **이사회** - 이사회는 상위 경영진과 회사의 전사적 리스크 관리의 상황에 대해 논의하고 필요에 따라 감독기능을 수행한다. 이사회는 전사적 리스크 관리 메커니즘(mechanism)을 통해 회사의 전략이나 목표와 관련된 가장 중요한 리스크가 평가되고 있다고 확신해야 하며, 경영진이 전사적 리스크 관리 모니터링에 어떻게 참여하고 있으며, 어떤 행동을 취하고 있는지를 파악해야 한다. 또한, 이사회는 내부감사인, 외부감사인, 고문(advisor)들로부터 정보를 취득해

야 한다.

- **최고 경영자** – 이 연구는 최고경영자가 회사의 전사적 리스크 관리 능력을 평가해야 한다고 권고한다. 프레임웍(framework)을 사용하면, 최고 경영자는 운영 및 재무 부문의 핵심 관리자와 함께 필요한 부분에 관심을 집중할 수 있다. 접근 방법의 하나로써 최고경영자가 사업본부장 및 주요 직원들과 함께 전사적 리스크 관리의 능력 및 효과성에 대한 평가를 논의할 수 있을 것이다. 초기 단계에서는 형식에 상관없이, 어느 정도 수준의 평가가 필요한가와 해당 평가를 진행시키는 방법에 대해 결정해야 한다.
- **기타 구성원** – 관리자와 기타 구성원들은 이 프레임웍의 관점에서 그들의 전사적 리스크 관리 책임을 어떻게 수행할지 고려하고, 전사적 리스크 관리 강화 방안을 고위 경영진과 논의해야 한다. 그리고 내부 감사인은 전사적 리스크 관리에 대한 그들의 관심의 폭을 넓혀야 한다.
- **규제기관** – 당 프레임웍은 전사적 리스크 관리가 할 수 있는 것과 그 한계를 포함하여, 전사적 리스크 관리에 대한 공유된 관점을 갖도록 유도할 수 있다. 규제기관은 규정, 지도 또는 검사를 수행할 때, 그들이 감독하는 회사에 대한 기대치를 수립하기 위하여 당 프레임웍을 활용할 수 있다.
- **전문가 집단** – 규칙제정 및 재무관리 지침, 감사, 관련 토픽을 제공하는 전문가 집단은 당 프레임웍의 관점에서 자신들의 기준과 지침을 고려해야 한다. 개념과 전문용어의 다양성이 제거되면, 모든 부문들은 이익을 얻을 수 있다.
- **교육기관** – 이 프레임웍은 미래에 어느 분야가 더 발전할 수 있는지 파악하기 위해 학계의 연구, 분석의 주제가 될 수 있다. 당 보고서가 공통으로 이해되어 받아들여진다는 가정하에, 해당 개념과 용어는 대학 교육과정에서 인용될 수 있다.

상호 이해의 전제 하에 모든 관계자들은 공통된 언어로 말함으로써 더욱 더 효과적으로 의사소통 할 수 있게 된다. 경영진은 표준에 의거하여 전사적 리스크 관리 프로세스를 평가하고, 프로세스를 강화하며 설정된 목표를 향하여 나아갈 수 있게 하는 위치에 서게 될 것이다. 앞으로의 연구는 이러한 토대를 더욱 강화시킬 것이다. 그리고 입법기관과 규제기관은 전사적 리스크 관리의 혜택, 한계와 함께 이를 더욱 잘 이해할 수 있을 것이다. 모든 관계자들이 공통된 전사적 리스크 관리 프레임웍을 사용한다면, 이러한 집합적으로 강화된 효익이 현실화될 것이다.