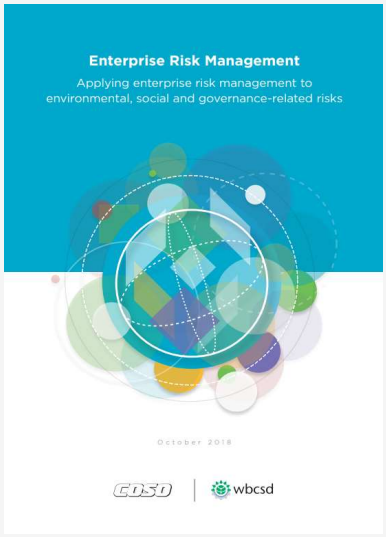
전사적 리스크 관리(ESG 관련 리스크에 ERM적용하기)

-K-Risk 발간편집위원회 역-



목차

※ 본 기사는 좌측 문헌의 단순 번역기사로서 K-Risk의 견해를 반영하는 것은 아니다.

K-Risk

※ 상기 이미지를 클릭하면 원문 다운로드가 가능합니다.

1. ESG 관련 리스크에 대한 거버넌스 및 문화

서론

거버넌스(gorvernance)는 기업, 정부 또는 다자간 기관에 관계없이 기업의 전반적인 효율성을 보장하는 시스템 및 프로세스이다. 효과적인 거버넌스는 조직의 목표를 설정하는 데 필요한 감독, 구조 및 문화, 목표를 추구하는 수단 및 관련 리스크를 이해하는 능력을 제공한다.

COSO ERM(Enterprise Risk Management) 프레임워크는 강력한 감독을 포함한 거버넌스가 조직에 대한 전체 리스크 범위를 효과적으로 식별, 평가 및 해결하기 위한 전제 조건임을 강조한다. ESG 관련 리스크를 거버넌스 구조, 시스템 및 프로세스에 통합시키는 것은 조직적 사일로 효과, 수량화 문제 및 조직적 편향과 같은 리스크를 관리하는 데 있어 많은 조직이 직면한 문제를 극복하는 데 중요하다.

이 장은 거버넌스와 문화에 대한 COSO ERM 프레임워크 구성요소와 5가지 관련 원칙에 관한 것이다.

❶ 이사회 리스크 관리 : 이사회는 전략을 감독하고 경영진이 전략 및 비지니스 목표를 달성할 수 있도록 지원하는 거버넌스 책임을 수행한다.

❷ 운영 구조 설정 : 조직은 전략 및 비지니스 목표를 추구하기 위해 운영 구조를 설정한다.

❸ 원하는 문화를 정의한다 : 조직은 기업이 원하는 문화를 특징짓는 행동을 정의한다.

❹ 핵심 가치에 대한 헌신을 보여준다. : 조직은 기업의 핵심 가치를 보여준다.

❺ 유능한 인적자원을 발굴하고 유지한다. : 조직은 전략 및 비지니스 목표에 따라 인적 자본을 구축하기 위해 최선을 다한다.

이 장에서는 리스크 관리 및 지속 가능성 실무자가 ESG 관련 리스크를 ERM 거버넌스 및 문화에 통합하는 데 도움이 되는 조치들을 간략하게 설명할 것이다.

- □ 조직의 필수적인 혹은 자발적인 ESG 관련 요구 사항 매핑 또는 정의
- □ 기업의 문화와 핵심 가치에 ESG를 포함시킬 수 있는 기회 고려
- □ ESG 관련 리스크에 대한 이사회의 인식을 높이는 방법 알림.
- □ 운영 구조, ESG 관련 리스크에 대한 리스크 소유자, 보고 라인, 전사적 ERM 및 전략적 계획 프로세스를 매핑하여 감독, 협업 개선 영역 식별
- □ 조직 전체의 협업 기회 구성
- □ 통합을 촉진하기 위해 고용 및 인재 관리에 ESG 관련 기술, 역량 및 지식 포함

ESG에 대한 감독 및 거버넌스

각 조직은 감독 및 거버넌스에 대해 고유한 접근 방식이 있다. 2016년에 발행된 남아프리카 기업 지배구조에 관한 King IV 보고서(King IV 보고서)는 불평등, 기후 변화, 급진적 투명성, 급속한 기술 및 과학 발전과 같은 ESG 관련 비지니스 및 사회 변화의 맥락에서 좋은 지배 구조를 정의하는 것에 대한 관점을 제공한다. King IV 보고서는 윤리적 문화, 우수한 성과, 효과적인 통제 및 정당성을 포함하는 결과를 추구하는 이사회에 의한 윤리적이고 효과적인 리더십에 대한 원칙을 기반한 접근 방식을 제공한다.

ESG 관련 리스크 거버넌스를 지원하는 데 도움이 될 수 있는 King IV 보고서 권장 사항은 다음과 같다.

- 규정된 이사회 위원회로 사회 및 윤리 위원회를 설립한다.
- 거버넌스 프로세스에서 이해관계자의 역할을 대단히 중요하게 강조하고 있다. 이사회는 이해관계자의 정당하고 합리적인 요구, 이익 및 기대를 고려하는 동시에 이사회와 회사가 자신의 행동과 공개에 대해 책임을 지도록 하는 이해관계자의 역할을 인식해야 한다.
- 기회 및 리스크 관리에 중점을 두고 있으므로 리스크 위원회에 특정 리스크와 관련된 기회를 식별하는 역할을 부여한다.
- 이사회가 전략 계획 과정에서 특별한 기회에 주의를 기울일 것을 요구한다.

ESG 관련 리스크 관리 책임

종종 상호 연결된 ESG 관련 리스크는 장기적으로 서서히 진행되어 효과적인 관리가 어렵다. 그러나 이러한 리스크가 조직의 성과에 미치는 잠재적 영향은 상당하므로 이를 관리하는 조직의 책임은 다른 비지니스 리스크와 다르지 않다. ESG 문제가 기업의 사회적 책임 또는 지속 가능성 부서와 같이 별도로 관리되는 경우에도 ESG 관련 리스크를 조직의 핵심 ERM 구조 및 프로세스에 통합하는 것은 기업과 이사가 책임을 다할 수 있도록 지원하는 데 중요하다.

이 섹션에서는 ESG 관련 리스크와 관련하여 기업의 책임을 초래할 수 있는 규제 및 자발적 ESG 관련 의무에 대해 간략히 설명한다.

리스크 관리 및 지속 가능성 관련 실무자가 고려해야 할 질문들:

- 기업이 과거에 ESG 관련 사고로 재정 및 운영 분야에서 평판 문제를 겪은 적이 있는가?
- 기업 시장의 ESG 관련 규정, 요구 사항 또는 의무는 무엇인가? 이러한 규정, 요구 사항 또는 의무를 준수하지 않을 때 발생하는 리스크가 있는가?
- 경영진에게 관련 규정, 요구 사항 또는 책임이 어떻게 전달되고 운영되는가?
- 기업은 미션, 비전, 핵심 가치 또는 장기 전략에 있어 ESG 관련 리스크를 어떻게 다루는가?
- 기업은 ESG와 관련하여 어떤 정책이나 방법을 갖고 있는가?

규제가 있는 책임

많은 국가에서 재무, 보건, 안전 및 환경 규제 관련 기관은 ESG를 잘못 관리한 회사의 임원이나 직원에게 민사 및 형사처벌을 내릴 수 있다. 예를 들어, 2015년 두 명의 전 Quality Egg LLC(미국 기반

소비재 회사) 임원이 2010년 살모넬라 발병 당시 취한 조치에 대해 형사상 책임이 부과되었다. 그들은 계란 시설이 오염될 리스크가 있다는 사실을 알고 있었다. 그 결과 회사 680만 달러 임원, 10만달러의 벌금이 각각 부과되었다.

기업은 규제나 벌금이 집행되지 않는 경우라 할지라도 ESG 리스크를 관리하지 못하면 재정적 영향을 받을 수 있다. 예를 들어 음식으로 인한 질병에 대한 공포 이후 치폴레의 시장 가치가 하락했다거나, 여성 체조선수들에 대한 의사의 성적 학대 혐의로 미시간 주립 대학이 소송 합의금으로 5억 달러를 지불해야 했다는 예 등이 이에 해당한다.

관리 기관은 관리하는 기관의 장기적 이익을 보장해야 한다. 이 중 일부는 기업 리스크에 대한 일상적 관리이다. 잠재적으로 중대한 리스크와 마찬가지로 ESG 문제는 기업 리스크 평가 및 공개에 포함되어야 한다. 일부 관할 구역의 리스크 공개 요건에 대한 개요는 부록 II를 참조하라.

특정 ESG 관련 요구 사항도 많은 관할 구역에서 나타나고 있다. 이러한 규정 중 일부는 의무인 반면 다른 규정은 기업이 ESG를 관리하는 방법을 공개할 요구 사항이다. 이러한 규정 중 많은 부분이 고위 경영진에게 적용되는 시행 조항이다(표 1.1 참조).

1단계 대 2단계 이사회 구조

1단계 이사회는 주주를 대신하여 경영진과 그 결정을 감독한다(미국, 영국 및 호주에서 일반적).
2단계 시스템에서 관리 이사회의 상임이사는 회사의 목표를 결정하고 실행하는 반면, 감독 이사회의 비상임 이사는 다른 당사자를 대신하여 결정을 모니터링한다 (유럽에서 더 일반적임).

지침

조직의 필수 또는 자발적 ESG 관련 요구 사항 매핑 및 정의

자발적 책임

기업의 규제 요구 사항 외에도 경영진과 이사회는 기업의 자발적 규범이나 의무를 알고 있어야 한다. 여기에는 지속 가능성, 인권, 천연 자원, 공급망 및 상품, 개인 정보 보호, 환경 정책 또는 회사의 약속이 포함될 수 있다. 이들 중 일부는 CEO가(예: UN Global Compact 또는 PRI) 결정하며 자발적이지만 기업이 책임을 질 수 있는 약속을 해야 한다. 원칙이나 요구 사항을 준수하지 않는 회사는 평판이 손상되고 주주, 고객, NGO 또는 지역사회의 감시를 받을 수 있다. 보통 채택되는 일부 자발적 프레임워크 및 약속은 부록 III을 참조하라.

CDSB 및 Ecodesk와 협력한 보고서 교환, WBCSD는 2017년 보고 교환 (reportingexchange.com)을 시작했다. 60개국 이상에서 요구하는 기업 지속 가능성 보고를 위한 글로벌 리소스이다.

표 1.1: ESG 관련 규정의 예

규제	범위	시행
지침 2014/95EU (비재무 보고에 관한 유럽 연합 지침)	약 6,000개의 대기업(상장 기업, 은행, 보험 회사 및 공익 단체 포함)이 사회 및 환경 문제를 운영하고 관리하는 방식에 대한 EU의 특정 정보(예: 환경 보호 및 인권 존중)공개 요구 법률.	보고 연도 2017년까지 완전한 보고 준수가 필요하다. 회사가 소재한 국가는 시행에 대한 책임이 있다. 요건 위반은 조치 자체에 대한 위반으로 간주된다.
도드-프랭크 1502 (분쟁 광물 규칙)	미국 법률에 따라 SEC 제출자는 제조 또는 계약된 제품에 콩고 민주 공화국 또는 인접 국가에서 생산되는 분쟁 광물(예: 탄탈륨, 주석, 금 또는 텅스텐)이 포함되어 있는지 여부를 공개해야 한다.	발행인은 성실하게 준수하지 않을 경우 18조(1934년 교환법)의 적용을 받는다. 미준수에 대한 법적 의미 외에도 발행자는 인권 운동가, 비정부 기구(NGO), 소비자 또는 기타 시장 세력으로부터 분쟁이 없음을 증명하라는 압력을 받을 수 있다.
1900년 Lacey법	야생 동물, 어류 및 식물을 불법적으로 채취, 소유, 운송 또는 판매하는 것을 금지하는 미국 보존법.	경범죄 위반은 최대 1년의 징역형에 처할 수 있다. 또한 기업의 경우 USD$ 200,000, 개인의 경우 USD$ 100,000의 벌금이 부과된다. 중범죄는 회사에 대해 최대 5년의 징역과 위반 건당 USD$ 500,000, 개인에 대해 USD$ 250,000이 부과될 수 있다.
법률 2010-788 (Grenelle II 법칙)	직원 500명 이상, 매출 1억 유로 이상의 상장 및 비상장 기업이 사회, 환경 및 경제 지표에 대한 제3자 검증 보고가 포함된 통합 보고서를 발행하도록 요구하는 프랑스 법률.	회사는 이해 관계자의 요청에 따라 정보를 생성해야 한다. 2015년 및 2017년 추가 법률은 보고 요건을 강화하고 이사회가 ESG 정보를 이해 당사자에게 보고하지 않을 경우 벌금 및 책임을 부과한다.
현대판 노예법 2015	희생자 보호를 위한 조항을 포함하여 노예제, 노예 상태, 강제 노동 및 인신매매 문제를 해결하기 위해 고안된 영국 법률	직접적인 처벌은 없지만 영국 정부는 조직이 준수하도록 요구하는 금지 명령에 대해 고등 법원에 소송을 제기할 수 있다.
2007년 국가 온실가스 및 에너지 보고법(NGER법)	특정 회사가 이 프레임워크에 따라 온실 가스 배출, 에너지 생산 및 에너지 소비에 대한 정보를 보고하고 배포하도록 요구하는 호주 연방법.	NGER 법의 의무를 따르지 않을 경우 회사와 임원에게 최대 USD$ 220,000의 벌금이 부과될 수 있다. 심각한 범죄는 형사 처벌의 대상이다.

또한 기업이 따르기로 한 다수의 자발적인 부문, 지역별 코드 또는 표준이 있다. 예를 들어, 방글라데시에 있는 업체에 일을 맡기는 의류 회사는 방글라데시 협정에 참여할 수 있다. 이는 해당 지역에 있는 공장의 건물 안전 및 작업 조건을 목표로 한다. 또한, 지속 가능한 팜유에 관한 원탁회의(RSPO)에 속한 단체는 지속 가능한 팜유 제품의 생산, 조달, 재정 및 사용을 발전시켜야 한다. 해산물 분야의 경우, MSC(Marine Stewardship Council)와 ASC(Aquaculture Stewardship Council)는 양식업자, 해산물 가공업체, 소매 및 식품 서비스 회사, 과학자, 환경 보호 단체 및 소비자를 위한 환경 지속 가능성 및 사회적 책임에 대한 표준 및 인증을 제공한다.

기업 문화에 ESG 인식 포함

COSO ERM 프레임워크는 문화를 "경영진과 직원의 결정에 영향을 미치고 조직의 사명, 비전 및 핵심 가치를 반영하는 긍정적이고 부정적인 리스크에 대한 태도, 행동 및 이해"로 정의된다. 미션, 비전, 핵심 가치 및 전략을 종합하면 독립체가 존재하는 이유, 엔터티, 수행 의도 및 수행 방법을 설명한다. 이러한 요소는 통찰력을 제공하고 동기를 부여하며 기업이 성장하고 목표를 달성함에 따라 앞으로 나아갈 방향을 제시한다. 따라서 ESG 요소를 미션, 비전 및 핵심 가치에 포함시키면 "ESG 의식적" 행동과 결정을 나타내는 문화를 육성하는 데 도움이 될 수 있다.

포장, 생체 재료, 목조 건축 및 종이의 재생 가능한 솔루션을 제공하는 글로벌 리더인 Stora Enso는 지속 가능성을 ERM에 통합하기 위한 기업 지배 구조의 중요성을 보여주었다. 스토라 엔소의 "Do Good for the People and the Planet"이라는 목표는 지속 가능성의 중요성을 나타낸다. 지속 가능성은 투자자 제안 및 전략의 기본이다. 또한, 재생 가능 제품의 생산 및 판매, 지역 산림 소유자로부터 목재 구입, 공장에서 생산된 전기 판매, 글로벌 규모의 물류 관리와 같은 Stora Enso의 모든 운영 및 활동 전반에 걸친 의사 결정에 필수적이다.

리더십 교체, 합병 및 인수, 예상치 못한 사건에서 얻은 교훈, NGO 캠페인의 부정적 홍보, ESG 문제에 대한 조사 저널리즘 또는 소비자 압력과 같은 특정 이벤트는 문화 변화의 촉매제가 될 수 있다. 이러한 이벤트는 기존 문화에 도전하거나 위협할 수 있으며 조직이 해당 문화를 수정하거나 강화할 수 있는 기회를 제공할 수 있다.

지침

기업의 문화와 핵심 가치에 ESG를 포함시킬 수 있는 기회 고려

ESG 문화 강화 및 통합을 위한 몇 가지 고려 사항은 다음과 같다.

- 조직의 사명, 비전 및 핵심 가치가 ESG 관련 리스크를 해결하는가?
- 조직 리더의 어조가 ESG에 대한 기대치를 전달하는가?
- 경영진은 조직의 사명, 비전, 핵심 가치 및 전략을 수행하는가?
- 기업이 올바른 인재를 고용하고 있으며 선택 과정이 비지니스 요구를 반영하는 포괄적이고 재능 있는 인력을 구축하는 과정과 양립하는가?
- 기업은 중요한 ESG 문제에 대한 성과를 향상시키는 지표와 보상을 연결하는가?
- 기업이 현지 지식을 반영하는 ESG 정보를 고려하여 결정을 내릴 수 있는 팀과 직원에 어떤 권한을 주고 있는가?
- 조직의 문화와 우선순위가 일치하는 직원의 행동을 장려하는가?

지속 가능성을 기업 문화에 포함시키는 방법에 대한 자세한 내용은 경영진을 위한 가이드의 조직 문화의 지속 가능성을 참조하라.

이사회 단계에서의 ESG

COSO ERM 프레임워크에 따라 이사회는 "회사 전략을 감독하고 경영진이 전략 및 비지니스 목표를 달성할 수 있도록 지원하는 거버넌스 책임을 수행한다." 이러한 책임은 조직을 감독하는 모든 이사회에 해당된다.

리스크 관리 및 지속 가능성 실무자가 고려할 질문:

- 이사회는 기업 전략 및 목표에 영향을 미칠 수 있는 ESG 리스크를 인지하고 있는가?
- 중요한 ESG 관련 리스크가 조직 내에서 이사회의 주의를 끌도록 하는 단계적 확대 경로가 있는가?
- 이사회는 ESG리스크를 평가하는 데 필요한 정보를 알고 있는가?
- 이사회는 ESG의 의미를 이해할 능력이 있는가?
- ESG 리스크 관련 소위원회가 있는가?
- 이사회는 기업의 통제 및 관리에 대해 중요한 ESG 리스크와 자원을 정기적으로 확인하는가?
- 이사회는 ESG 리스크의 거버넌스를 포착하는가?
- 이사회는 ESG 리스크에 대해 정기적으로 보고서를 받는가?
- ERM 및 ESG에 대한 이사회 구성원의 기대치는 무엇인가?

전체적인 리스크를 감독하려면 이사회가 비지니스 전략 또는 목표를 위협할 수 있는 ESG 관련 리스크를 통해 조직을 안내할 적절한 이해, 적절한 정보와 경험 및 전문성을 갖추어야 한다.

지침

ESG 관련 리스크에 대한 이사회의 인식을 높이는 방법 안내.

이를 위해 이사회는 관련 ESG 문제와 이를 관리하는 기업의 접근 방식에 대해 브리핑을 요구할 수 있다. 보다 성숙한 ESG 프로그램을 가진 조직은 중대한 ESG 문제 또는 리스크를 모니터링하고 보고하기 위해 이사회 또는 위원회 수준에서 특정 역할을 정할 수 있다. 이사회 차원에서 ESG 리스크 인식을 강화하기 위한 접근 방식은 표 1.2에 설명되어 있다.

표 1.2: 이사회의 ESG 관련 리스크 인식 제고를 위한 접근법

접근	설명	예
이사회 헌장에 ESG 관련 리스크 또는 문제에 대한 참조 포함	경우에 따라 ESG 관련 리스크를 감독하는 이사회(또는 위원회)의 책임을 설명하기 위해 공식적으로 위임된다. 헌장 또는 참조 조건에서 ESG 문제에 대한 특정 참조는 이사회 수준에서 ESG 통합에 대한 명확한 방향을 제공한다.	Stora Enso에는 헌장에 다음 의무를 포함하는 지속 가능성 및 윤리에 대한 소위원회가 있다. •지속 가능성 및 윤리와 관련하여 Stora Enso의 활동 및 평판에 중대한 영향을 미칠 수 있는 법적 성격을 포함하는 문제 검토 •Stora Enso의 비지니스 활동 및 성과에 중대한 영향을 미칠 수 있는 사회, 정치, 경제 및 환경 동향 검토
ESG 관련 리스크 및 쟁점에 중점을 둔 이사회 위원회 구성	ESG에 중점을 둔 별도의 위원회를 구성하여 ESG 리스크를 감독할 명확한 권한을 줄 수 있다. 이 위원회는 리스크 또는 감사 위원회에서 관리하는 거버넌스 리스크와 함께 환경 및 사회적 리스크와 같은 ESG 리스크 선택을 관리할 수 있다. 감사 위원회와 같은 다른 위원회는 온실가스 배출 또는 인권 보고 및 공개와 같은 ESG 리스크의 특정 측면에 초점을 맞출 수 있다.	국제 제지 및 포장 회사인 Mondi plc는 지속 가능한 개발 소위원회와 감사 위원회에 리스크를 감독하는 책임을 분담한다. 지속가능발전위원회는 건강, 안전, 환경 리스크를 관리하고 감사위원회는 회사의 나머지 리스크를 관리한다.

표 1.2: 이사회의 ESG 관련 리스크 인식 제고를 위한 접근법(계속)

접근	설명	예
ESG 관련 지식 또는 전문성을 갖춘 이사를 이사회 또는 관련 위원회에 임명	이사회는 회사의 가장 중요한 ESG 문제를 이해하고 이사회나 관련 위원회에 알리기 위해 전문가 관점에서 접근해야 한다. (예: ESG 위원회 또는 감사 위원회). 일부 이사회는 특정 ESG 경험이 있는 이사를 임명할 수 있다. 이사회에 지속가능 전문가가 있는지 여부와 상관없이 기업은 이사가 기업의 ESG 문제와 관련하여 최소한의 역량을 갖추어야 하는지를 고려해야 한다.	2017년 ExxonMobil은 대기 과학자이자 Woods Hole Oceanographic Institutionf의 전 사장 겸 이사를 13명으로 구성된 이사회에 추가했다. Conoco Phillips 및 GM을 포함한 다른 회사들도 최근 이사회에 ESG가 있는 이사를 추가했다.

리스크 관리 및 지속 가능성 실무자는 이사회를 위한 정보를 준비하고 (예: 조직의 ESG 성과를 반영하는 KPI 및 지표) 어떤 커뮤니케이션 채널을 사용해야 하는지, 얼마나 자주 정보를 제공해야 하는지 결정함으로써 이사회 차원에서 ESG관련 리스크 인식을 높이는 데 중요한 역할을 할 수 있다. 또한 실무자는 조직의 내부 기능을 활용하여 ESG 관련 리스크에 대해 개별 이사회 구성원 또는 위원회에 관점을 제공할 수 있다. 이 때 전문적인 제3자의 의견이나 관점을 얻을 수도 있다.

"모든 이사나 고위 경영진이 'ESG 전문가'가 될 수는 없지만 이사와 적절한 회사 직원은 회사가 당면한 주요 ESG 문제에 대해 스스로 교육하고 중요하거나 심각한 리스크를 내포하는 문제에 대해 편안하게 대화할 수 있어야 한다."

Wachtell, Lipton, Rosen 및 Katz

ESG에 대한 이사회 인식 개선에 대한 추가 지침은 UNEP 통합 거버넌스를 참조하라. 지속 가능성을 위한 새로운 거버넌스 모델, NACD의 거버넌스 과제 2017: 이사회의 ESG 감독, 기업 지속 가능성 활동에 대한 감독(이사 핸드북 시리즈, 2014-2015), Ceres 2018 보고서 시스템 규칙: 이사회 거버넌스가 지속 가능성 성과를 주도하는 방법 또는 Eccles와 Youman의 2015년 작업 문서 기업 거버넌스의 중요성: 주요 청중 및 중요성에 대한 설명.

관리 단계에서의 ESG

이사회는 궁극적으로 조직의 장기적 성공에 대해 책임을 지며 의사 결정 및 관리 활동을 CEO에게 위임한다. CEO는 리스크 관리의 운영 활동을 수행하는 경영진에게 명령 사슬을 위임하는 회사 경영진에게 위임한다. ERM 프로세스 전반에 걸쳐 조직의 다양한 역할 중 일부의 예는 부록 V에서 찾을 수 있다.

리스크 관리 및 지속 가능성에 대해 실무자가 고려해야 할 질문:

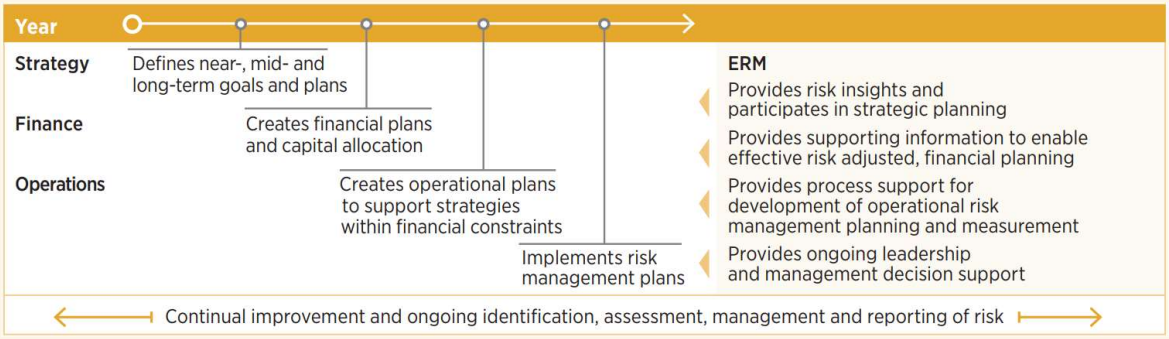
- ERM 프로세스에 대한 감독이 명확하게 정의되고 구현되었는가?
- 리스크와 지속 가능성에 운영 및 전략적으로 통합된 프로세스가 있는가?
- 지속적인 프로세스 개선이 공동으로 개발되고 모니터링되는가?
- ERM 프로세스가 ESG를 리스크 관리에 연결하는가?
- 어떤 이해관계자의 이익이 기업의 장기적 성공에 중요한지에 대한 합의가 있는가?
- ERM이 주요 비지니스 프로세스, 보고 및 메트릭에 포함되어 있는가?
- 경쟁업체와 동료는 ESG 관련 리스크를 식별, 관리 및 공개하기 위해 무엇을 하는가?
- ERM 실무자는 ESG에 대해 교육을 받았는가? 또는 그 반대도 마찬가지인가?

ERM 구조, 프로세스 및 지속적인 개선

조직은 ERM을 컴플라이언스 프로세스, 1년에 1회 활동 또는 연간 주기로 수행할 활동 체크리스트로만 접근해서는 안 된다. ERM은 지속적이고 반복적이며 일상적인 비지니스 프로세스에 내장되어 기업이 새로운 위협과 기회를 인식하고 앞서 나갈 수 있도록 한다.

그럼에도 불구하고 조직에는 일반적으로 ERM에 대한 정해진 일정이 있다. 이는 부분적으로 의무와 예산 주기, 전략 계획 프로세스 및 연례 총회와 같은 기타 전략적 및 규제적 이정표에 의해 결정된다. 지속 가능성 실무자는 관련 ESG 주제 전문가가 연례 설문 조사 또는 워크숍에 포함되고 ESG 관련 리스크가 전략 계획 및 운영 논의에 포함될 수 있도록 종단 간 리스크 관리 프로세스 및 전략적 계획 주기를 이해해야 한다. 전략적 계획 및 운영 주기의 예와 ERM이 이를 지원하는 방법은 그림 1.1에 나와 있다.

그림 1.1: 전략적 계획 및 운영 주기

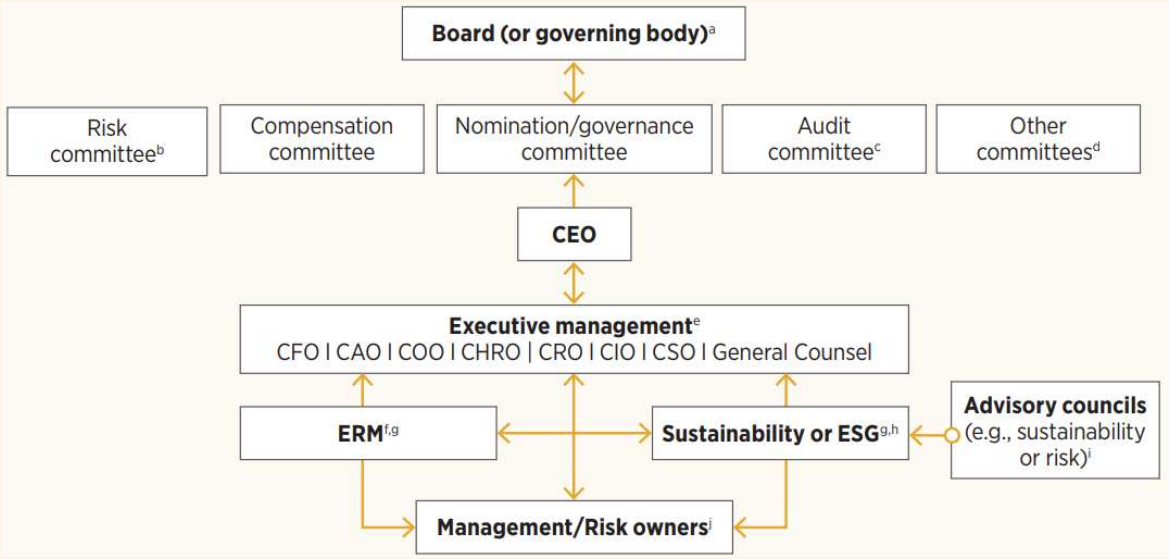


리스크 관리 및 지속 가능성 실무자는 조직의 운영 구조, 보고 라인 및 프로세스를 매핑하여 ESG-ERM 감독 및 협업을 강화할 수 있는 영역을 구분해야 한다. 경우에 따라 ESG 관련 리스크가 예기치 않게 구체화될 수 있으며 적절한 리스크와 해당 전문가를 신속하게 찾아 적절한 대응책을 마련해야 한다. 그림 1.2는 거버넌스 구조의 예와 리스크 관리 및 지속 가능성을 위한 몇 가지 주요 역할을 보여준다.

지침

운영 구조, ESG 관련 리스크에 대한 리스크 소유자, 보고 라인, (조직구조의 수직) 끝에서 끝까지 ERM 및 전략적 계획 프로세스를 매핑하여 감독 및 협업 개선 영역 식별

그림 1.2: 거버넌스 구조의 예



a. 이사회는 ESG 관련 리스크 소유권에 대한 경영진의 접근 방식을 감독하고 적절한 경우 이의를 제기하고 ESG 리스크를 효과적으로 식별, 평가, 관리 및 모니터링하기 위한 프로그램이 있는지 확인할 책임이 있다.
b. 리스크 위원회는 기업 리스크 관리를 직접 감독한다. 리스크 위원회의 초점은 회사 전체, 감사위원회의 권한과 가용 자원을 넘어선 비재무적 영역까지이다. (예: 운영, 책임, 신용, 시장, 기술).
c. 감사 위원회는 이사회가 기업 지배 구조를 수행하고 기업의 재무 보고, 내부 통제, 리스크 관리, 내부 및 외부 감사 기능과 관련된 책임을 감독하도록 지원한다.
d. 일부 회사에는 ESG 관련 리스크를 식별, 모니터링 및 검토하기 위해 기능간 대표로 구성된 리스크 위원회 및 감사 위원회와 별도로 지속 가능성 위원회와 같은 추가 이사회 위원회가 있다.
e. 전략 계획 및 운영 담당자와의 연결은 지속 가능성을 새로운 전략 및 리스크 대응과 연결하는 데도 중요하다. 조직이 리스크와 관련 기회를 식별하고 더 잘 준비할 수 있도록 새롭고 새로운 ESG 관련 리스크에 대한 시기적절한 평가를 지원한다.
f. ERM 기능 또는 이사는 ERM 활동을 조정하고 통합하는 책임이 있으며 일반적으로 CRO 또는 기타 C-suite에 보고할 뿐만 아니라 통합적이고 체계적인 방식으로 전사적 리스크를 관리하는 프로세스를 이끌 것이다.
g. 지속가능성 책임자는 ERM 책임자와 긴밀한 관계를 유지해야 한다.
h. 지속 가능성 이사는 CFO, CSO 또는 COO에게 보고할 수 있으며 ESG 관련 활동 조정을 지원한다. 여기에는 메가트렌드 모니터링과 리스크 식별, 평가 및 모니터링이 포함된다.
i. 교차 기능 또는 다중 이해 관계자 자문 위원회(내부 또는 외부)는 ESG 문제 또는 기타 리스크의 특정 측면에 대한 관점을 제공할 수 있다.
j. 경영진이 기업 리스크를 집합적으로 '소유'하면서 특정 리스크를 적절하게 관리할 책임이 있는 담당자로 '리스크 소유자'를 지정하는 경우가 많다.

ERM이 최고 리스크 책임자(Chief Risk Officer)의 전적인 책임이 아닌 것과 마찬가지로 ESG 리스크 관리는 지속 가능성 실무자만의 책임이 아니다. 모든 경영진은 전략 및 의사 결정에 영향을 미치는 중대한 ESG 리스크를 명확히 설명할 수 있어야 한다. 표 1.3은 ESG 전문가일 수도 있고 아닐 수도 있는 ESG 관련 리스크에 대한 리스크 소유자의 예를 제공한다.

표 1.3 : ESG 관련 리스크에 대한 리스크 소유자의 예

기업 단계 리스크	ESG 요소	관련 리스크 소유자	리스크 소유자 지원
원자재 가격 상승 리스크	기후변화 규제에 따른 에너지 비용 상승으로 인한 가격 변동	공급망 부사장	최고 지속 가능성 책임자 지속 가능성 분석가(에너지)
작업 중 부상 또는 사망 리스크	보건 및 안전 관련 고려 사항	환경보전 안전관리자	현장 관리자
공급망의 ESG 문제에 대한 불충분한 커뮤니케이션으로 인한 평판 손상 리스크	인권에 대한 공급망 투명성 강화에 대한 압력	최고 조달 책임자	최고 지속 가능성 책임자

협업과 통합을 향해

지침

조직 전체에서 협업 기회 만들기

새로운 트렌드와 세력으로 인해 복잡해짐에 따라 조직은 리스크에 더 잘 적응하고 탄력적으로 대처해야 한다. 이를 지원하기 위해 조직 전체의 리스크 관리에 대한 협업 및 통합은 리스크 관리 및 지속 가능성 실무자가 ESG 문제를 논의하기 위한 공통 언어를 찾고, 리스크 소유권에 대한 공동 책임을 정하고, 이를 해결하기 위한 보다 혁신적인 솔루션을 개발하는 데 도움이 될 수 있다. 통합 접근 방식에서 리스크 관리 및 지속 가능성 실무자는 다른 주제 전문가와 함께 기능 간 리스크 위원회와 같은 공식적인 파트너십으로 작업할 수 있다. 이 접근 방식에서는 재무, 환경, 거버넌스, 기술, 사회적 또는 기타 모든 리스크가 하나의 프로세스의 일부로 간주된다.

일부 대기업에서는 리스크 및 컴플라이언스 기능을 ESG 문제(특히 인권)를 관리하는 기능과 연결한다. 이러한 변화는 조직의 평판을 보호하고 리스크를 완화하려면 보다 조정되고 통합된 대응이 필요하다는 인식의 확산으로 나온 것이다. 이런 기능을 결합하면 조직이 직면한 리스크와 이러한 리스크가 전략적 우선순위를 제공하는 능력에 어떤 영향을 미칠 수 있는지 더 잘 볼 수 있다. 이러한 새로운 변화의 일부는 활동가들이 소셜 미디어를 사용하여 자신의 입맛에 맞지 않는 단체를 배척하고 정부가 기업에 책임을 묻도록 하는 데 초점이 맞춰진 데 기인한다.

기술, 능력 및 지식 활용

지침

통합을 촉진하기 위해 고용 및 인재 관리에 ESG 관련 기술을 포함한다.

ESG에 ERM을 적용하려면 기업 전반에 걸쳐 전문가와 실무자의 다분야 접근 방식이 필요하다. 어떤 경우에는 외부 전문 지식이 필요할 수도 있다. 지속 가능성 실무자는 이해 관계자의 기대치, 잠재적인 환경 및 사회 관련 리스크와 기회, 그리고 이러한 리스크를 가장 잘 피하거나 활용할 수 있는 방법에 대해 지식을 갖고 있다. 리스크 관리 실무자는 리스크 식별, 평가 및 우선순위 지정, 대응 구현 및 효율성 추적에 대한 지식과 기술을 보유하고 있다.

표 1.4는 리스크 관리 및 지속 가능성 실무자의 일부 기술, 능력 및 지식을 강조한다. 이러한 기술을 이전하거나 공유하면 ESG 통합을 지원할 수 있다. 조직은 이러한 ESG 리스크 관련 기술, 역량 및 지식을 채용 및 인재 관리에 포함시키는 것을 고려해야 한다.

표 1.4 : 이전하거나 공유할 수 있는 기술, 능력 및 지식의 예

리스크 관리 실무자	지속 가능성 실천가
• 전사적 ERM 프로세스와 ERM 및 전략적 활동의 타이밍에 대한 지식 • 중대한 리스크에 대해 고위 경영진 및 이사회(또는 위원회)에게 전달 경로 • COSO와 같은 ERM 프레임워크와 리스크의 재무, 운영 및 전략적 영향을 이해하는 데 능숙하다. • 광범위한 리스크 환경에 대한 이해 • ESG 관련 리스크에 활용할 수 있는 재무 리스크(예: 시나리오 계획, Monte Carlo 시뮬레이션)을 평가하는 데 사용되는 도구 또는 접근 방식을 배포하는 기능 • 이익, 손실 및 자본 할당 측면에서 영향을 평가하는 기술	• ESG 관련 메가트렌드 및 이러한 메가트렌드가 다른 리스크나 영향을 어떻게 악화시킬 수 있는지 이해 • 비지니스 및 사회에 대한 ESG 문제에 대한 이해를 지원할 수 있는 널리 인정되는 프레임워크에 대한 지식 • 회사의 탄소 인벤토리에 대한 자세한 지식 및 관련 리스크를 줄이거나 완화하기 위한 수단과 같은 ESG 관련 리스크에 대한 기술적 이해 • 경영진 및 이사회에 ESG 문제 및 관련 비지니스 리스크를 제시할 수 있는 리더십 능력 • ESG 문제(주주, 고객, 직원, 노동조합, NGO)에 대한 광범위한 이해 관계자 환경 및 우선순위에 대한 지식 • 리스크를 완화하거나 가치와 기회를 포착하기 위해 현재 시행 중인 ESG 이니셔티브에 대한 이해

리스크를 식별하고 관리하는 리스크 관리, 지속 가능성 및 기타 기능은 공통의 목적을 구축하고 이들의 복합적인 기술, 능력 및 지식이 그 목적에 부합할지 이해해야 한다. 기업은 다음과 같이 회사 전반에 걸쳐 리스크 또는 ESG 관련 모범 사례를 공유하기 위한 교육 프로그램을 개발할 수 있다.

- 비지니스 전반에 걸친 리스크 및 대응
- 효과적인 완화 전략
- 교훈
- ERM 인증 또는 교육
- 리스크 평가에 사용되는 도구 및 자원