TONE at the TOP®

최고경영진, 이사회, 감사위원회에 거버넌스 관련 주제에 대한 간결한 정보를 제공

이사회가 ERM 감독에 대해 알아야 할 사항

오늘날의 불확실한 경영 환경에서 이사회 구성원들은 리스크 감독을 강화해야 한다는 요구를 받고 있다. 다양한 이해관계자들은 이사회가 끊임없이 변화하는 리스크 환경을 감독하는 데 있어 점점 더 적극적인 역할을 수행하기를 기대하고 있다.

조직이 직면한 리스크에는 지정학적 혼란, 사이버보안 우려, 신기술의 영향, 공급망 문제, 노동력 부족, 심각한 기상 현상 등이 포함되며, 이는 몇 가지 예에 불과하다. 하버드 로스쿨 기업거버넌스 포럼(Harvard Law School Forum on Corporate Governance)의 「리스크 관리와 이사회(Risk Management and the Board of Directors)」에 따르면, "기업 리스크 관리는 단순히 기업 경영진의 사업 및 운영상 책임이 아니라, 이사회의 감독 책임에 명확히 포함되는 거버넌스 및 전략적 이슈이다."

해당 보고서는 또한 위기가 발생할 때 법원과 규제기관이 이사회의 감독 활동과 이사회의 대응에 주목하고 있다고 덧붙인다. 이사들이 일상적인 리스크 관리에 직접 관여해서는 안 되지만, "모든 이사회의 감독 역할에는 적절한 이사회 위원회 활용을 포함하여 주요 기업 리스크 요인을 모니터링하는 데 대한 적극적인 참여가 포함되어야 한다"고 보고서는 설명한다.

이번 호에서는 전사적 리스크 관리(ERM) 감독과 관련한 이사회의 고려사항과, 이사회에 가치 있는 보증과 자문을 제공하는 내부감사의 역할을 살펴본다.

ERM 성숙도 판단

조직의 ERM 성숙도 수준에 대한 현실적인 평가는 현재 상황과 필요한 변화에 대해 이사회가 보다 깊이 이해할 수 있도록 해준다. PwC의 「이사를 위한 ERM 기본지침(Director's Guide to ERM Fundamentals)」에 따르면, 높은 수준에서 조직의 ERM 성숙도 단계는 다음과 같다.

- **초기 단계(Initial)**. 일부 비공식적인 관행은 존재하지만 공식적인 정책이나 프로세스는 없다. 조직은 문제가 발생하면 이에 대응하는 방식으로 움직인다.
- **발전 단계(Developing)**. 설계 또는 운영 측면의 일부 영역에서 효과적인 시스템과 프로세스가 존재한다. 접근방식은 사업 운영에 어느 정도 부합한다.
- **구축 단계(Developed)**. 공식 기준을 충족하기 위해 공식적인 프레임워크와 시스템이 내재화되어 운영되고 있다.
- **통합 단계(Integrated)**. 조직은 현재 및 신규 리스크에 대해 조정된 전략적이고 효율적인 대응을 가능하게 하는 통합적·협업적·고도화된 시스템과 프로세스를 갖추고 있다.
- **최적화 단계(Optimized)**. 시스템, 프로세스 및 문화가 전략적 우선순위와 잘 통합되어 있으며 이에 부합한다. 기술은 거버넌스, 리스크 관리 및 모니터링·보고를 강화하는 데 활용된다.

해당 지침서는 "ERM 프로그램이 성숙해질수록 이사회는 무엇이 효과적으로 작동하고 무엇이 그렇지 않은지에 대해 경영진에게 질문함으로써 지속적인 개선을 촉진할 수 있다"고 설명한다.

더 깊이 살펴보기

COSO의 전사적 리스크 관리-전략 및 성과와의 통합(Enterprise Risk Management-Integrating With Strategy and Performance) 경영진 요약본은 이사회가 ERM과 관련하여 경영진에게 제기할 수 있는 질문들을 제시하고 있으며, 여기에는 다음이 포함된다.

- 최고리스크관리책임자(CRO)뿐만 아니라 모든 경영진이 전략 선택이나 사업 의사결정 과정에서 리스크가 어떻게 고려되는지를 설명할 수 있는가?
- 경영진은 조직의 리스크 성향(risk appetite)와 그것이 특정 의사결정에 어떠한 영향을 미칠 수 있는지를 명확하게 설명할 수 있는가? COSO는 이에 대한 답변이 조직의 실제 리스크 수용 성향에 대한 통찰을 제공할 수 있다고 지적한다.
- 최고경영진은 리스크 관리 프로세스뿐만 아니라 조직 문화가 리스크 감수를 어떻게 촉진하거나 저해하는지에 대해서도 논의할 수 있는가?
- 경영진은 어떤 관점이나 기준을 사용하여 리스크 문화를 모니터링하고 있으며, 그것은 어떻게 변화해 왔는가? 조직 내부와 외부에서 변화가 불가피하게 발생하는 상황에서, 이사회는 경영진이 적절하고 시의적절하게 대응할 것이라는 확신을 어떻게 가질 수 있는가?

COSO의 사례집(Compendium of Examples)에는 거버넌스에 관한 구체적인 관찰 내용이 포함되어 있다. 그 사례 중 하나는 ERM이 의사결정을 개선하여 더 나은 성과를 창출하고, 기회를 확대하며, 부정적인 돌발 상황을 최소화하는 방법을 다루고 있다. 해당 사례에서 한 기업은 현재의 ERM 역량과 바람직한 ERM 역량을 보다 잘 이해하기 위한 노력을 기울이고 있다. 예를 들어 최고경영자(CEO)와 내부감사인은 사업부문과 함께 경영성과 검토 회의에 참석하여 성과 목표 달성 진행 상황을 추적하고, 리스크에 대한 이해가 목표 추구 방식에 어떠한 영향을 미치는지를 확인한다. 이러한 노력 덕분에 CEO는 사업 성과를 더욱 잘 이해할 수 있게 되었고, 내부감사인은 감사계획을 더욱 효과적으로 수립할 수 있게 되었다.

모범사례에 대한 지침

ERM 접근방식을 강화하고자 하는 조직은 여러 ERM 프레임워크 중에서 선택할 수 있다. 여기에는 COSO의 전사적 리스크 관리 통합 프레임워크(Enterprise Risk Management-Integrated Framework), ISO 31000 리스크 관리 표준(ISO 31000 Risk Management Standard), 그리고 미국 국립표준기술연구소의 리스크 관리 프레임워크(U.S. National Institute of Standards and Technology's Risk Management Framework)가 포함된다. Optro의 전사적 리스크 관리 기초(Enterprise Risk Management Fundamentals)에 따르면, 이러한 프레임워크들은 일반적으로 다음의 다섯 가지 핵심 구성요소를 공유한다.

- 기업 문화, 거버넌스 및 가치.
- 전략 기획, 목표 및 목표 설정.
- 리스크 관리 사이클.
- 모니터링 및 지속적 개선.
- 투명성, 커뮤니케이션 및 보고.

IIA의 3선 모델(Three Lines Model) 은 리스크 관리에 대한 이사회 감독을 위한 모범사례 모델로서, 핵심 역할들이 강력한 거버넌스를 지원하기 위해 어떻게 함께 작동하는지를 보여준다. 이 모델과 연계된 전사 및 비즈니스 프로세스 리스크 도구(Enterprise and Business Process Risks Tool)는 전사 수준 및 프로세스 수준에서 리스크를 식별·평가·관리·모니터링하기 위한 실용적이고 맞춤화 가능한 접근방식을 제공함으로써 조직이 체계적인 ERM 프로그램을 구현하고 관리하는 데 도움을 준다.

세계내부감사인협회 소개

세계내부감사인협회(IIA)는 전 세계적으로 265,000명 이상의 회원을 보유하고 있으며, 200,000개 이상의 국제공인내부감사사(CIA)® 자격을 부여한 비영리 국제 전문가 협회입니다. 1941년에 설립된 IIA는 전 세계 내부감사 분야의 표준, 자격인증, 교육, 연구 및 기술 지침을 선도하는 기관으로 인정받고 있습니다. 자세한 내용은 **theiia.org**에서 확인할 수 있습니다.

IIA 주소

1035 Greenwood Blvd.Suite 401
Lake Mary, FL 32746 USA

무료 구독

theiia.org/Tone을 방문하여 무료 구독을 신청하세요.

독자 피드백

질문이나 의견은 다음 이메일로 보내주세요:
Tone@theiia.org.

내부감사와의 협력

내부감사는 ERM을 강화하려는 이사회의 노력에 있어 가치 있는 협력자가 될 수 있다. 실제로 IIA는 ERM과 관련된 내부감사의 역할이 진화하고 있으며, 점점 더 많은 최고감사책임자(CAE)가 ERM에 대한 책임을 맡고 있다고 보고한다. IIA의 「북미 내부감사 현황 조사(North American Pulse of Internal Audit)」에 따르면, 내부감사 책임자 역할과 함께 ERM 프로그램에 대한 책임도 맡고 있다고 응답한 CAE의 비율은 2025년에 34%까지 증가하였다.

효과적인 리스크 관리 기능을 지원하는 핵심 요소 중 하나는 3선(Three Lines) 전반에 걸친 협력이다. IIA의 3선 모델(Three Lines Model)에 따르면 다음과 같다.

- **제1선(First Line)**: 리스크를 관리하는 경영진 및 운영 책임자.
- **제2선(Second Line)**: 리스크를 모니터링하고 감독하는 리스크 관리 및 컴플라이언스 기능.
- **제3선(Third Line)**: 조직의 목표 달성에 대해 독립적인 보증과 자문을 제공하는 내부감사.

이사회에 대한 기대사항

이사회의 핵심적인 리스크 관련 책임은 다음과 같다.

- 조직의 리스크 성향(risk appetite)과 리스크 허용범위(risk tolerance)를 설정하는 것.
- ERM 프레임워크를 승인하고 모니터링하는 것.
- 전략과 리스크 노출 수준을 정렬시키는 것.
- 리스크 문화와 내부통제를 감독하는 것.
- 신규 리스크와 핵심 리스크 영역을 모니터링하는 것.
- 역할과 책임이 명확하게 정의되고 유지되도록 보장하는 것.

- Diligent, 「현재와 미래의 리스크 관리에 대한 이사회 감독의 이해(Understanding Board Oversight of Risk Management Now and for the Future)」

IIA의 3선 모델은 "내부감사가 경영진으로부터 독립성을 유지함으로써 계획 수립과 업무 수행 과정에서 방해나 편향 없이 활동할 수 있도록 보장하지만, 독립성이 완전한 고립을 의미하는 것은 아니라는 점을 명확히 보여준다"고 Baker Tilly, Internal Audit Foundation, 그리고 Wolters Kluwer TeamMate가 공동 발간한 보고서 「타협 없는 협업: 내부감사, 리스크 관리 및 거버넌스 실무에 대한 실무자 관점(Collaboration Without Compromise: Practitioner Perspectives on Internal Audit, Risk Management, and Governance Practices)」은 설명한다. ERM을 포함한 여러 영역에서 확대되고 있는 내부감사의 책임은 거버넌스와 리스크 관리의 효과성을 독립적으로 평가하는 기능으로서 내부감사의 역할을 한층 강화할 수 있는 기회를 제공한다.

해당 보고서에 따르면 응답자의 90%는 제2선과 제3선 간의 협력이 다음과 같은

이점을 제공한다고 인식하고 있다.

- 리스크 커버리지의 향상.
- 중복 업무의 감소.
- 조직 전반의 연계성 강화.
- 이사회에 대한 커뮤니케이션 강화 및 보다 효율적인 보고.

보고서 응답자의 39%는 지난 5년 동안 내부감사 기능과 리스크 관리 기능의 통합이 확대되었다고 응답하였으며, 60%는 향후 5년 동안 이러한 수치가 더욱 증가할 것이라고 전망하였다. 보고서는 "정보 공유, 활동 조정, 우선순위 정렬을 통해 신중하게 설계된 이러한 접근방식은 이사회가 정보에 기반한 의사결정을 내릴 수 있도록 신뢰할 수 있는 정보를 제공하는 데 도움이 된다"고 설명한다.

명확한 시야

ERM은 무엇보다도 변화를 인식하거나 예측하고, 그러한 변화가 조직에 어떤 의미를 가지는지를 판단하는 활동이라고 할 수 있다. COSO는 변화에 대한 명확한 시야가 조직으로 하여금 새로운 투자를 해야 하는지, 아니면 사업을 축소해야 하는지와 같은 어려운 질문에 대해 건전한 의사결정을 내릴 수 있게 해준다고 설명한다. COSO는 "전사적 리스크 관리는 이사회가 리스크를 평가하고 회복탄력성(resilience)의 사고방식을 수용할 수 있도록 적절한 프레임워크를 제공한다"고 밝히고 있다.

기술과 ERM

인공지능(AI)이 ERM에서 더욱 큰 역할을 수행할 수 있는 잠재력은 매우 크다. Baker Tilly와 Internal Audit Foundation이 발간한 「고도화된 전사적 리스크 관리와 전략적 의사결정(Enhanced Enterprise Risk Management and Strategic Decision-Making)」에 따르면, AI를 자주 활용해 위험을 식별한다고 답한 응답자는 10명 중 1명 미만(6%)이었으며, 위험 관리 활동의 데이터 입력에 AI를 본격적으로 활용하고 있다고 답한 응답자도 3%에 불과했다.

통합 거버넌스·리스크 관리·컴플라이언스(GRC) 플랫폼은 ERM 프로세스를 지원할 수 있다. Baker Tilly와 Internal Audit Foundation의 ERM 성숙도 조사(ERM Maturity Survey)에 따르면, 응답자 중 이러한 플랫폼을 활용하고 있는 비율은 21%에 불과하다. 많은 조직의 ERM 프로그램은 워드프로세서 및 스프레드시트(59%) 또는 자체 개발 기술 도구(20%)와 같은 비교적 단순한 도구에 기반하고 있다.

「고도화된 전사적 리스크 관리」 보고서는 "디지털 전환이 운영 전반에 걸쳐 기술 의존도를 가속화하고 전략 자체를 재정의하고 있는 시대에 ERM이 이러한 변화 속도를 따라가지 못하는 것은 위험한 일이다"라고 경고한다.

이러한 점을 고려할 때 다음과 같은 사항이 중요하다.

- 서비스형 소프트웨어(SaaS)와 GRC 도구는 기본적인 ERM 프로그램을 강화하고, 전사적 차원에서 리스크에 대한 보다 심층적인 이해를 촉진할 수 있다. 이러한 도구는 데이터를 중앙집중화하고, 업무흐름을 자동화하며, 리스크 식별을 더욱 용이하게 함으로써 더 나은 의사결정을 가능하게 하고 리스크 노출을 최소화할 수 있다.
- 해당 보고서는 조직이 안전한 AI 활용에 대한 탐색 활동을 지원·촉진·모니터링하고, ERM 프로세스에서 AI를 활용할 수 있는 방안을 발굴할 것을 권고한다.
  보고서는 "협업 도구, 외부 리스크 스캐닝, 기능 간 통합, 그리고 첨단 기술의 도움을 받아 전통적인 ERM 접근방식에서 한 단계 발전하는 것이 모든 ERM 프로그램의 목표가 되어야 한다"고 강조한다.

"설문조사에 참여한 전 세계 전문가들 가운데 50%는 향후 2년간 글로벌 리스크 전망이 '불안정한(turbulent)' 상태 또는 '격변적인(stormy)' 상태가 될 것으로 예상하고 있으며, 이 비율은 향후 10년 전망에서는 57%로 증가한다." 반면, 리스크 환경이 안정적일 것이라고 예측한 비율은 1%에 불과하다.

- World Economic Forum, 「글로벌 리스크 보고서 2026(Global Risks Report 2026)」