감사위원회 및 감사의 역할_(3) 리스크 감독

김 유 경 상무
삼정KPMG 감사위원회 지원센터 리더
youkyoungkim@kr.kpmg.com

1. 리스크 감독의 중요성 및 감사기구의 역할

(1) 리스크 감독의 중요성

기업 리스크 관리의 중요성이 대두된 결정적 계기는 2008년 글로벌 금융위기라 볼 수 있다. 2000년대 중반부터 서브프라임 모기지론[1] 원리금을 상환하지 못하는 저소득자들이 점증하였고, 이러한 모기지론을 기초자산으로 하는 금융상품을 구매한 금융기관들이 막대한 손실을 입게 된다. 뉴욕 월가의 5대 투자은행이었던 베어스턴스(Bear Stearns) 및 리먼브라더스(Lehman Brothers)가 파산하였고, 메릴린치(Merrill Lynch)는 뱅크오브아메리카(Bank of America)에 매각되었다. 미국발 금융위기는 비단 미국 뿐 아니라 전세계적인 장기 경기침체의 원인이 되었다. 금융위기 이후 비로소 많은 기업들이 상시적 리스크 관리의 중요성을 인식하기 시작하였고, OECD 기업지배구조 위원회는 2009년에 "기업지배구조와 금융위기(Corporate Governance and the Financial Crisis)" 라는 제목의 연구보고서를 공표하기도 하였다.

기업이 연루될 수 있는 각종 리스크 중 가장 대표적인 것은 아마 분식회계로 인한 리스크일 것이다. 분식회계는 선량한 투자자들의 금전적 손실 및 기업명성 추락을 넘어 극단적으로는 기업을 파산에 이르게까지 할 수 있다. 2000년대 초 미국 엔론과 월드컴, 2011년 일본 올림푸스, 2015년 일본 도시바, 2016년 우리나라 대우조선해양 등 최근 십 수 년 간 대규모 부정회계 사건이 잇따라 발생하였다. 자본주의의 선구자인 미국, 성실·정직한 경제의 표상이었던 일본은 물론 개발도상국 단계를 지나 자본주의가 정착되었다고 여겨졌던 우리나라까지, 여러 경제대국들에서 경영활동에 대한 체계적·공식적 보고로서 '기업의 언어' 라고 불리는 재무제표에 대한 리스크 관리, 즉 재무감독 조차 제대로 이루어지지 않고 있었다는 사실은 많은 사람들에게 충격을 안겨주었다.

한편, 올 9월 S사의 배터리 충전 시 화재 발생 위험으로 인한 스마트폰 대량 리콜 사태, 사망·반영구적 폐 손상 등 약 1,500명의 피해자를 낳은 O사의 가습기 살균제 사건은 제품 안전에 관한 리스크 관리의 실패 사례이다. 해외 사례로는 미국 내 세 번째로 큰 자산규모를 지닌 웰스파고(Wells Fargo) 은행이 2011년부터 고객의 동의 없이 고객의 개인정보를 이용해 2백만 개 이상의 허위 계정을 생성하여 왔던 것이 9월 초에 발각되었는데, 이는 적절한 내부통제 및 리스크 관리의 부재가 재앙적인 결과를 초래할 수 있음을 보여준다. 그 외 국내 대기업집단의 총수가 횡령·배임·탈세 등 혐의로 기소 및 처벌된 다수의 사건들은 리더십의 갑작스러운 부재로 인한 혼란은 물론 기업 이미지를 심각하게 훼손시키는 오너리스크이다. 또한 최근에는 해킹·개인정

1) Subprime mortgage loan(비우량주택담보대출): 신용등급이 낮은 저소득층에게 주택을 담보로 주택 구입자금을 대출해 주는 금융상품

보 유출과 같은 사이버 리스크를 대비해야 한다는 목소리가 높아지고 있다. 국내에서는 2014년 초 은행·카드사 등 금융회사에서 대량의 고객 정보가 유출되어 사회적으로 큰 파장이 있었다. 이와 같이 기업의 명성훼손 뿐 아니라 심한 경우 기업의 존폐에까지 영향을 미칠 수 있는 리스크 요소는 회계투명성, 소비자 안전, 지배주주 및 임원의 도덕성, 사이버 보안 등 매우 광범위하다.

(2) 감사기구의 리스크 감독 역할

리스크 감독은 해당 업무를 전담하는 리스크관리위원회만이 수행하여야 하는가? 감사품질센터[2], 유럽 회계사연합[3], 호주 공인회계사협회[4]는 2013년에 발간한 보고서[5]에서 리스크 감독 및 관리는 감사위원회의 중대하고 어려운 임무 중 하나이며, 리스크(관리)위원회가 존재할 경우 동일한 이사를 두 위원회에 동시에 배치하는 등 감사위원회와 리스크(관리)위원회 간 긴밀한 협력이 필요하다고 하였다.

국내 실태를 보더라도 별도의 리스크관리위원회 설치를 의무화하기 보다는 감사기구가 리스크 감독 역할까지 담당하는 것이 현실적일 것으로 보인다. 한국기업지배구조원의 조사에 따르면, 2013년 사업연도 말 기준 국내 유가증권시장 상장사 694사 중 리스크관리위원회를 설치한 회사는 49사로, 비율로는 7.06%에 불과하였다[6]. 이 중 대부분이 금융지주사, 보험사, 증권사, 은행 등 금융회사였다[7]. 반면, 2013년 말 기준 유가증권시장 상장사 694사의 감사기구 설치 현황을 살펴보면, 감사위원회를 설치한 기업은 261사(37.6%), 감사를 두고 있는 기업은 433사(62.4%)로, 유가증권시장 상장사는 모두 감사기구를 보유하고 있었다[8]. 이러한 제도적 현실과 감사기구에게 상법상 업무감독권한을 부여한 법적 환경을 감안할 때, 리스크관리위원회가 별도로 존재하지 않는 경우, 일반적으로 리스크 감독의 역할을 감사기구가 담당한다는 것에 동의하는 것으로 보인다.

아래의 표에서 보듯이, 해외의 경우에도 리스크관리위원회가 별도로 설치된 금융기관을 제외하고는 리스크 감독의 역할을 감사위원회가 가져가는 것이 일반적인 것으로 나타나고 있다. 노스 캐롤라이나 주립대학교가 2014년 가을에 미국 기업 CFO 등 재무 담당 임원 1,093명을 대상으로 수행한 조사[9]에 따르면, '이사회가 리스크 감독에 대한 공식적인 책임을 산하위원회에 위임한다면 어느 위원회가 가장 적합한가?' 라는 질문에, 상장회사 및 매출액 10억 달러 이상의 대규모 기업들의 경우 감사위원회라고 답한 비율이 리스크(관리)위원회라고 답한 비율보다 높게 나타났다.

---

2) Center for Audit Quality, CAQ
3) Federation of European Accountants, FEE
4) Institute of Chartered Accountants in Australia, ICAA
5) CAQ·FEE·ICAA, "Global Observations on the Role of the Audit Committee", 2013.
6) 한국기업지배구조원, 김선민·엄수진 연구원, "리스크 관리에 관한 규준 및 국내 유가증권시장 상장사의 리스크관리위원회 도입 현황", CG Review Vol.75, 2014.08.
7) 리스크관리위원회를 설치한 비금융회사는 케이티앤지, 사조산업, 남해화학이었음
8) 오덕교, "2014년 지배구조 평가 및 실태 분석-유가증권시장 상장기업을 중심으로", 선진상사법률연구 통권 제67호, 2014.07.
9) North Carolina State University, "2015 Report on the Current State of Enterprise Risk Oversight", 2015.02.

[표 1] 미국 기업의 리스크 감독 업무 이관 현황

표본그룹 / 답변	전체 표본	대규모 기업 (매출액 $10억 이상)	상장회사	금융기관	비영리법인
감사위원회	50%	56%	53%	38%	58%
리스크위원회	24%	29%	31%	41%	7%
집행위원회(주1)	14%	4%	4%	9%	15%

(주1) Executive Committee

2015년 KPMG ACI(Audit Committee Institute)에서 발간한 자료에 의하면, 해외 선진국에서는 일상적이고 정형화된 프로세스로 정착된 '회계감독' (Integrity of financial statement)을 넘어 감사위원회의 역할이 '리스크 감독' (Risk Oversight)로 이행하고 있다고 언급하고 있다.

"Audit committees today deal with a broad range of issues, and accompanying risks, that go beyond financial statements, reporting and internal controls over financial reporting – their traditional areas of responsibility."

(Audit committee trends "What's changing and how audit committees are responding, KPMG ACI 2015)

본고에서는 감사기구의 리스크 감독 의무를 다룬 법규를 살펴보고, 최근 선진국 감사위원회가 리스크 감독 업무에 할애하는 시간이 증가하고 있는 실태를 소개할 예정이다.

2. 감사기구의 리스크 감독 역할 관련 법규

OECD의 "Risk Management and Corporate Governance" (2014), ISO[10]의 "ISO 31000: Risk management — Principles and guidelines" (2009), COSO의 "Enterprise Risk Management — Integrated Framework " (2004) 등 리스크 관리와 관련해 기업들이 일반적으로 참고할 수 있는 글로벌 지침들은 이미 다수 존재한다. 국내에서는 금융회사 지배구조 모범규준이 마련되기 전까지는 금융감독원, 금융투자협회, 전국은행연합회 등에서 금융회사들을 대상으로 한 리스크 관리 모범규준을 공시하고 있었다. 본고는 그러나 보편적인 기업 리스크 관리보다는 기업 내에서 '감사기구'가 리스크 관리·감독과 관련해 기여할 수 있는 역할을 다룬 법규들에 초점을 맞추고자 한다.

10) International Organization for Standardization(국제표준화기구): 각국 163개의 표준제정·연구기관을 회원으로 보유한 독립적인 비정부기구로서, 과학·기술·시장경제 등 분야에서 지식 협력을 위해 1946년 설립됨

(1) 국내 법규

우선, 우리나라 법률이나 모범규준 상에서는 감사(위원회)의 리스크 관리 의무를 명시하고 있지는 않다. 올해 8월 1일부터 시행된 금융회사의 지배구조에 관한 법률(이하 '금융사 지배구조법')은 금융회사의 위험관리위원회 설치[11], 위험관리기준 마련[12], 위험관리책임자의 임면[13] 의무를 명시하고 있다. 금융회사 지배구조 모범규준에서도 보상위원회에 위험관리위원회 소속 이사를 1인 이상 참여하게 하여 보상체계에 위험 관리측면이 충분히 다루어질 수 있도록 하여야 한다[14]고 정하였지만 감사(위원회)의 리스크 감독 책임을 직접적으로 명시한 조항은 없다.

(2) 해외 법규

이와 달리 미국, 영국 등 선진국에서는 감사위원회에 리스크 관리 또는 감독의 책임이 있다고 표명하고 있다. 미국 뉴욕증권거래소(이하 'NYSE') 상장규정 섹션 303A.07에서는 감사위원회의 부가적인 의무를 나열하고 있는데, 비록 리스크 평가 및 관리의 주된 혹은 유일한 담당자가 감사위원회는 아니지만 리스크 평가·관리 프로세스 및 해당 프로세스를 규정한 지침을 검토하는 업무 등은 감사위원회가 담당하는 것이 바람직하다고 적시하고 있다. 영국의 기업지배구조 모범규준에서도 이사회 또는 이사회 내 리스크(관리)위원회가 존재하지 않거나 리스크 관리 업무 책임자에 대해 특별히 따로 정하지 않은 경우, 회사의 내부통제 및 리스크 관리 시스템을 검토해야 할 책임은 감사위원회에 있다고 하였다.

[표 1] 감사위원회 및 감사의 리스크 감독 역할 관련 해외 법규

미국 NYSE 상장규정 Section 303A.07 "감사위원회의 추가 의무"
(b) 감사위원회는 다음 사항을 명문화된 헌장에 포함하여야 함: (iii) 감사위원회의 의무와 책임 - 증권거래법 10A-3(b)(2), (3), (4), (5)항 및 다음 사항을 포함하여야 함: (D) 리스크 평가 및 리스크 관리 관련 정책에 대해 논의; 논평: 상장회사의 리스크 노출 수준에 대해 평가 및 관리 하는 것은 CEO 및 임원들의 임무이지만, 이것이 다루어지는 프로세스를 명시한 지침 및 정책에 대해서는 감사위원회가 논의하여야 한다. 감사위원회는 상장회사의 주요한 재무 리스크 노출, 경영진이 그러한 리스크 노출에 대한 감시 및 통제를 위해 행한 조치에 대해 논의해야 한다. 감사위원회는 리스크 평가 및 관리를 책임지는 유일한 기구일 필요는 없으나, 앞서 언급했듯이 리스크 평가 및 관리를 이행하는 프로세스를 명시한 지침 및 정책에 대해 논의하여야 한다. 다수의 회사들, 그 중 특히 금융회사들이, 감사위원회가 아닌 다른 기구나 절차를 통해 그들의 리스크를 평가 및 관리하고 있다. 이러한 회사들이 활용하는 프로세스는 감사위원회에 의해 보편적인 방식으로 검토되어야 하지만, 감사위원회가 해당 프로세스를 완전히 대체할 필요는 없다.
영국 기업지배구조 모범규준
C.3.2. 감사위원회의 주요 역할 및 책임은 명문화된 위임사항(terms of reference)에 명시되

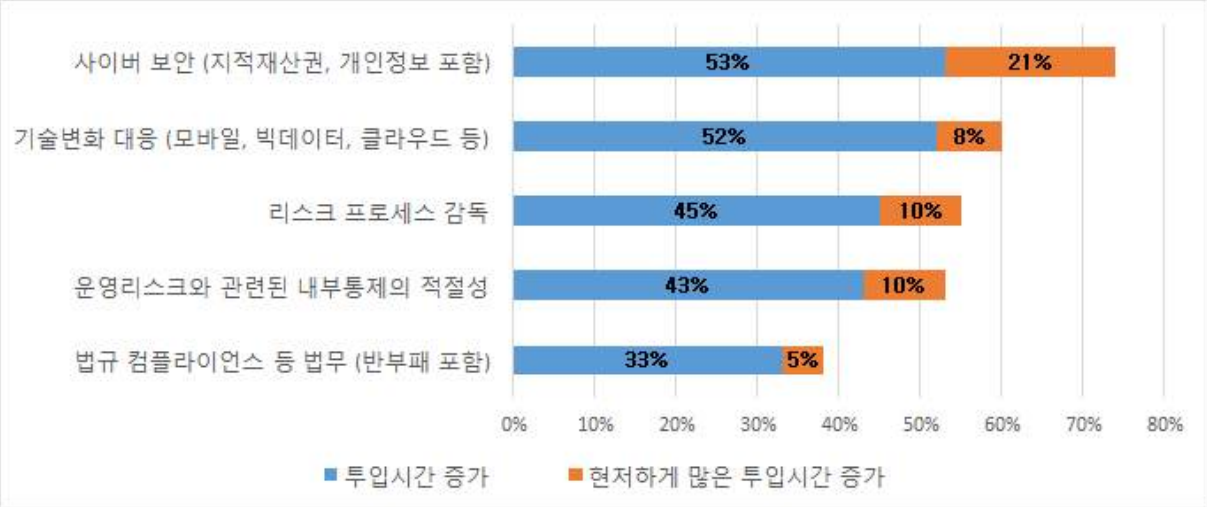
11) 금융사 지배구조법 제16조(이사회내 위원회의 설치 및 구성) 제1항, 제21조(위험관리위원회)
12) 금융사 지배구조법 제27조(위험관리기준)
13) 금융사 지배구조법 제28조(위험관리책임자의 임면 등)
14) 금융회사 지배구조 모범규준 제11조 제2항

어야 하며 다음 사항을 포함해야 함: (중략) • 회사의 내부 재무통제를 검토하고, 사외이사로 구성된 별도의 이사회 내 리스크 위원회나 이사회의 의무로 명시되지 않는 한, 회사의 내부통제 및 리스크 관리 시스템도 검토하여야 함;

3. 감사기구의 리스크 감독 역할 강화 동향

또한 2015년 Global ACI의 "2015 KPMG ACI Global Survey"에 따르면, 글로벌 감사위원회의 주요 어젠다 중 최근 들어 검토 및 의사결정에 투입시간이 증가한 안건 상위 4개가 리스크 감독과 관련된 것이었다.

[그림 1] 2015년 글로벌 감사위원회 주요 어젠다[15] 중 투입시간이 증가한 안건 Top 5



상기 그래프가 보여주는 바와 같이 최근에는 사이버 보안의 중요성에 대한 공감대가 확산되고 있다. 올해 5월, G7 국가들은 일본에 회동하여 금융산업 사이버 공격에 대한 보안을 강화하는 방안을 논의하였다. G7 국가 간 사이버 보안에 관한 협약은 금년 10월에 초안이 나올 것으로 예상되고 있다. 뿐만 아니라 미국 증권거래위원회(SEC) 위원장 메리 조 화이트(Mary Jo White)는 G7 회동과 같은 달에 열린 로이터 금융규제 회담(Reuters Financial Regulation Summit)에서 "사이버 보안 이슈는 금융 시스템이 당면한 최대 리스크다"라는 발언을 하였다.

아울러, 올 들어 미국 공인회계사협회(American Institute of Certified Public Accountants)는 재무제표 위주인 기존의 사업보고서 외에 회사의 사이버 보안에 관한 별도의 보고서를 외부감사인이 작성하도록 하는 방안을 추진하고 있다. 사이버 보안 보고서에는 회사의 사이버 리스크 관리 프로그램 실태, 동 프로그램의 공정성·효과성에 대한 경영진의 확인, 이에 대한 외부감사인의 감사의견 등이 포함된다.

15) Global ACI, "2015 KPMG ACI Global Survey"

이러한 세계적 트렌드를 고려할 때, 감사위원회가 사이버 보안 이슈를 논의하는 데 할애하는 시간이 증가하고 있는 실태는 긍정적인 현상으로 볼 수 있다. 특히 사이버 보안 보고서를 외부감사인이 작성하는 것이 보편화된다면, 다른 지배기구보다 외부감사인과의 커뮤니케이션이 잦은 감사위원회가 사이버 리스크 감독을 상시적으로 담당하는 것이 바람직하다. 감사위원회가 이에 대한 책임의식을 보유하고 사이버 보안 정책 및 프로그램의 실효성에 대한 실태파악이 되어있어야 외부감사인과의 시너지 효과를 기대할 수 있을 것이기 때문이다.

4. 결론

"금융기관을 제외하고 감사위원회와 리스크관리위원회를 구분해야 할 필요는 없다고 생각한다. 내가 속한 감사위원회에서는 리스크 관련 문제가 위원회 활동 시간의 50% 정도를 차지하고 있다."

상기 내용은 영국 이동통신 업체 보다폰(Vodafone Group Plc)의 사외이사이자 감사위원장인 닉 랜드(Nick Land)가 KPMG ACI와의 인터뷰에서 발언한 것이다. 실제로 보다폰은 이사회 내에 '감사위원회'가 아닌 '감사 및 리스크 위원회(Audit and Risk Committee)'를 운영하고 있다. 보다폰은 동 위원회의 목적이 '충분한 공시, 효과적인 내·외부감사, 내부통제 시스템·경영 리스크·컴플라이언스 활동에 대한 감독을 포함한 재무보고의 적절성 뿐 아니라 기업지배구조의 건전성을 제고하는 것'이라고 표명하고 있다.

빠르게 발전하는 과학기술, 소비자 권리·안전 관련 소송 발생의 증가, 날로 교묘해지는 사이버 공격, 지진·화산폭발 등 자연재해, 최근 증가하고 있는 불특정다수에 대한 테러위협 등 기업이 맞닥뜨릴 수 있는 리스크는 나날이 그 종류가 다양해지고 있을 뿐 아니라 심각성도 중해지고 있다. 독자적인 리스크관리위원회를 설치하여 리스크 관리를 전담하게 하는 것이 이상적이라 볼 수 있으나, 별도의 위원회를 신설하는 데 자원이 상당히 소요되기 때문에 기업 입장에서는 리스크관리위원회 운영이 현실적으로 쉽지 않은 일이다. 앞서 말했듯 우리나라 유가증권시장은 전체 상장사가 감사기구를 보유하고 있는데다, 감사 및 감사위원은 대개 재무적인 전문성까지 갖추고 있기 때문에 기업이 겪을 수 있는 잠재적 리스크를 예측하는 데 있어 유의미한 역할을 할 수 있을 것으로 기대된다.

기업이 직면할 수 있는 다양한 리스크 별로 대응 시나리오를 마련하고 임직원을 대상으로 주기적인 리스크 예방 교육을 실시하는 등 리스크 감독 업무에 대해 감사기구가 전적으로 책임을 맡거나 적극적으로 관여한다면, 감사(위원)로서의 독립성·전문성과 결합되어 기업지배구조의 건전성과 기업의 리스크 대응능력을 제고하는 데 기여할 수 있을 것이다. 기업의 자발적인 노력으로 이러한 목적이 달성되는 것이 가장 바람직할 것이나, 미국·영국처럼 상장규정이나 기업지배구조 모범규준에 감사(위원회)의 리스크 감독 의무를 명문화하는 것도 고려해 볼 만 하다.