TONE at the TOP®

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

이사진이 2024년에 고려해야 할 리스크

사이버보안과 인적 자본은 전 세계 6대 지역에서 기업이 현재 직면해 있거나 향후 마주하게 될 리스크를 파악하기 위해 실시된 설문조사에서 주요 리스크로 식별되었다. 세계내부감사인협회(IIA) 산하 내부감사재단(Internal Audit Foundation)에서 발행한 리스크 인 포커스(Risk in Focus) 2024는 내부감사 리더들을 대상으로 조직의 현재 리스크 환경(그림1 참조)과 감사계획에서 중점을 두고 있는 영역에 대해 설문조사를 실시했다. 또한 향후 3년 동안 어떤 리스크가 가장 심각해질 것인지 예측하도록 요청했다.

Tone at the Top 이번 호에서는 이를 통해 식별된 주요 리스크 중 일부를 다루고 있다. 이사회가 새롭게 부상하는 위협을 고려할 때 내부감사는 거버넌스 노력에서 중요한 파트너가 될 수 있다. "내부감사인은 리스크에 대해 선제적으로 접근하고 있다"고 IIA의 국제협력관계 부사장이자 CIA, CRMA, CCSA인 자비에 팔레아토(Javier Faleato)는 말했다. "내부감사인은 기업의 여정과 함께 하며 기업이 올바른 길을 택할 수 있도록 돕고 있다."

사이버보안 리스크를 바라보기

최근 몇 년 동안 사이버 범죄자의 수법이 더욱 교묘해짐에 따라 많은 이사회에서 사이버보안 전문성을 갖추기 위해 노력하고 있지만 기술적인 전문용어로 이루어지는 논의가 실제 비즈니스 운영에 어떻게 적용될 수 있는지 결정하기 어려울 수 있다. 내부감사는 매개체 역할을 하여 사이버위협과 잠재적인 비즈니스 리스크를 연결하는 독특한 위치에 있다고 팔레아토는 말했다. 내부감사 리더는 조직에 영향을 미치는 새로운 사이버보안 전개 양상 및 보안사고와 이것이 리스크 관리와 전략적 계획수립에 미치는 영향에 대해 이사회를 업데이트 시켜줄 수 있다. 내부감사를 통해 사이버보안과 관련된 거버넌스 프로세스의 효율성도 검토할 수 있다.

팔레아토는 "내부감사의 역할은 무엇이 효과가 있고 무엇이 효과가 없는지 이사회가 인식하게 해주는 것이다"라고 말했다.

백분율로 본 지역별 상위 리스크

현재 귀하의 조직이 직면한 상위 5대 리스크는 무엇인가?

감사 영역	전 지역 평균	아시아태평양	중남미	아프리카	북미	중동	유럽
사이버보안	73%	66%	75%	58%	85%		84%
인적 자본	51%	59%	44%	39%	65%	47%	50%
사업 연속성	47%	61%	47%	52%	36%	53%	38%
규제 환경 변화	39%	35%	48%	32%	43%	33%	43%
디지털 파괴(Digital Disruption)	34%	30%	38%	33%	36%	32%	33%
재무 유동성	32%	21%	33%	47%	28%	38%	26%
시장 변화	32%	47%	26%	21%	41%	26%	30%
지정학적 불확실성	30%	28%	42%	25%	28%	16%	43%
거버넌스/기업 보고	27%	24%	18%	36%	16%	45%	22%
공급망 및 아웃소싱	26%	27%	16%	19%	36%	28%	30%
조직 문화	26%	23%	26%	34%	21%	30%	20%
부정행위(Fraud)	24%	22%	30%	46%	9%	26%	13%
커뮤니케이션/평판	21%	18%	22%	27%	21%	28%	12%
기후 변화	19%	22%	22%	19%	12%	10%	31%
보건 안전	11%	12%	8%	10%	17%	9%	13%
인수합병(M&A)	6%	4%	3%	3%	8%	10%	8%

그림1

출처: Risk in Focus 2024

주: IIA의 리스크 인 포커스 글로벌 서베이, n=4,207. 백분율은 해당 영역을 5대 상위 리스크 중 하나로 평가한 사람을 보여줌. 파란색 음영은 해당 지역에서 리스크가 가장 높은 5개 영역임

내부감사팀은 회사가 관련 위협을 경감하는 데 필요한 모든 조치를 취하고 있는지에 대한 통찰력을 제공할 수도 있다. 설문조사에 따르면 내부감사팀은 전반적으로 감사계획 수립 시 사이버보안을 예전보다 강조하고 있는 것으로 나타났다. 사이버보안은 오랫동안 리스크 인 포커스의 우려사항으로 1위를 차지해 왔지만 과거 감사팀은 이 영역에 그에 상응하는 시간과 노력을 투자하지 않았다. 올해 설문조사에 따르면 사이버보안은 일반적으로 감사팀의 다른 관심영역보다 훨씬 주목받고 있다. 이사회는 내부감사팀이 사이버보안 이슈를 해결하기 위한 충분한 자원을 확보할 수 있도록 보장함으로써 이들이 계속해서 적절한 초점을 유지하도록 보호할 수 있다.

불행히도 대부분의 조직에서 가장 큰 사이버보안 취약성은 인적 요소이다. 직원은 피싱 이메일이나 사이버 범죄자에게 액세스를 부여하도록 설계된 점점 더 교묘해지는 기타 사기계획의 표적이 된다. 이사진은 사이버보안과 관련해 최고경영진의 태도가 얼마나 중요한지, 그리고 이사회가 어떤 긍정적인 영향을 미칠 수 있는지 명심해야 한다. 팔레아토는 이사진이 사이버보안의 중요성을 인지하고 이를 위해 노력하고 있다는 사실을 직원들이 알게 되면 사이버 안전 프로토콜을 무시할 가능성이 낮아질 수 있다고 말했다. 예를 들어 피싱 공격 캠페인에 대한 사내 교육에 이사진이 참석하고, 내부감사의 지원과 함께 몸값을 요구하는 공격 시나리오에 이사회 차원에서 참가하는 것을 고려해 볼 수 있다고 그는 권고했다.

세계내부감사인협회 소개

세계내부감사인협회(IIA)는 전 세계 230,000명 이상의 회원에게 서비스를 제공하고 전 세계적으로 185,000명 이상에게 공인내부감사사(CIA) 인증을 수여한 비영리 국제 전문가 협회이다. 1941년에 설립된 IIA는 표준, 인증, 교육, 연구 및 실무적 지침 분야에서 내부감사직종의 리더로 전 세계적으로 인정받고 있다. 자세한 내용은 **theiia.org.** 참조.

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.

번역: 이은주(CIA)

- 삼성전자 내부감사팀 근무
- SC제일은행 내부감사부 근무
- 한국씨티은행 내부감사부 근무
- 2003~한국외국어대학교 통번역대학원 영어과 졸업
- 한-영 통역사, 제조, 금융, IT, 법률 등 다양한 분야의 한-영 통역사 활동

기업의 가장 중요한 자산에 대한 거버넌스

직원의 능력과 전문성은 기업의 성공에 필수적이다. 조직은 인적 자원, 다양성, 형평성 및 포용성(DEI), 인재의 관리와 유지가 핵심 우려사항이라는 것을 알고 있지만 많은 경우 이러한 영역에 쏟는 노력이 유의미한 결실을 맺고 있는지 측정하는 방법을 모르거나 확신하지 못하고 있다. 새로운 세대의 직원에 대한 기대치가 변하고 원격 및 하이브리드 근무에 대해 논쟁이 계속됨에 따라 대화가 더욱 복잡해졌다.

이해관계와 불확실성을 고려할 때 이사회에는 명확한 정보와 조언이 필요하다. 내부감사는 이사회에게 가장 가치 있는 인적 자원 지표를 결정하고 전략 및 거버넌스 관점에서 이해하기 쉽게 복잡한 핵심 성과 지표(KPI)를 제시하는 데 도움이 된다. 예를 들어, 내부감사는 이사회가 변화하는 문화적 규범과 기대에 맞게 인적 자본 및 다양성 전략을 정렬시키는 데 활용할 수 있는 직원 만족도 측정을 포함하여 광범위하고 통찰력 있는 기업 정보에 접근할 수 있다.

새롭게 부상하는 리스크에 대비

리스크 인 포커스 2024는 내부감사 리더들에게 조직이 앞으로 3년 후에 직면하게 될 리스크의 순위를 매기도록 요청했다(그림 2 참조). 당연히 사이버보안이 현재나 앞으로나 1위였다. 그러나 디지털 파괴는 현재 5위에서 2위로 상승했고, 기후 변화는 14위에서 5위로 급등했다. 각 영역에서 이사가 고려해야 할 사항은 다음과 같다.

3년 후 예상되는 리스크 순위 변화

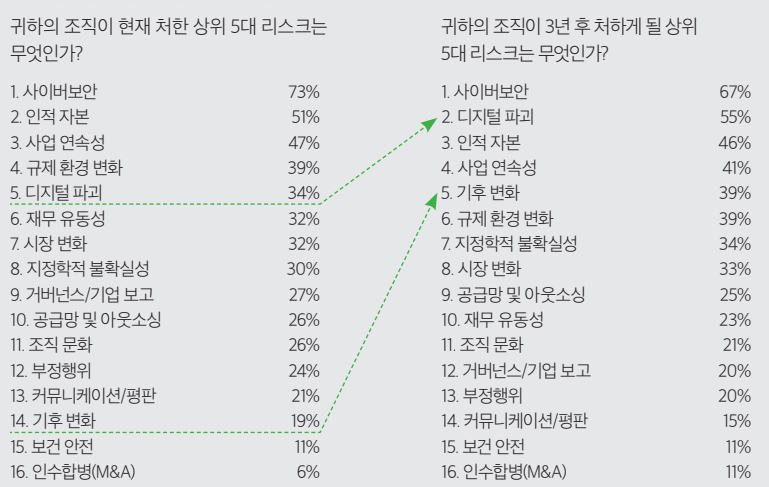

그림2 IIA의 리스크 인 포커스 글로벌 설문조사, n=4,207. 해당 영역을 조직의 상위 5대 리스크 영역 중 하나로 꼽은 비율

디지털 파괴. 어떤 신기술이 단기적으로 가장 큰 영향을 미칠지 알 수는 없지만, 생성형 인공지능(AI)이 그중 하나일 가능성이 높다. 생성형 AI로 잘 알려진 첫 번째 사례인 챗GPT(ChatGPT)는 출시 후 몇 달 만에 약 1억 명의 사용자를 확보했다.[1] 전반적으로 AI, 특히 생성형 AI는 사업 운영 방식을 변화시킬 것이다. 내부감사는 AI가 제공할 수 있는 주요 리스크뿐만 아니라 엄청난 기회를 이사회가 이해하는 데 도움이 된다고 팔레아토는 말했다. 생성형 AI에 대한 초기 대중의 열광적인 반응 이후 관련된 윤리적, 법적 문제에 대해 많은 의문이 제기되었다. 여기에는 개인정보보호 및 기밀유지, 원본 자료의 투명성 부족, 지적 재산권 문제와 정보의 정확성과 관련된 리스크가 포함된다. 기술이 진보하고 이용이 늘어남에 따라 내부감사는 이사회에 리스크와 장점을 알리고 이를 관리하는 방법에 대해 조언을 제공할 수 있다.

기후 변화. 이 영역에 대한 기업의 보고는 오랫동안 자진 보고로 이루어졌지만 규제기관이 새로운 규정을 발표하거나 제안함에 따라 빠르게 변하고 있다. 여기에는 EU 지속가능성보고표준(ESRS), 미국 증권거래위원회(SEC)의 기후변화 관련 공시 제안, 국제지속가능성기준위원회(ISSB)의 새로운 지침은 물론 호주, 캐나다, 인도, 브라질, 싱가포르 및 캐나다의 규정이 포함된다. 내부감사는 이 영역과 관련된 몇 가지 새로운 개념에 대해 이사회에 업데이트를 제공할 수 있다. 예를 들어, 조직은 재무 리스크와 관련하여 중대성의 개념을 오랫동안 이해해 왔지만 이제는 이중 중대성(Double Materiality)의 개념에도 익숙해져야 한다.

이 개념은 조직의 재무적 가치와 조직이 전 세계에 미치는 영향 모두에 있어 기업의 공시가 얼마나 중요한지 설명한다. "이중 중대성이라는 발상은 재무 이외에 기업이 세계에 미치는 영향이 중대할 수 있으므로 기업의 수익에 미치는 영향 외의 이유로 공개할 가치가 있다는 인식에서 비롯된다[2]."

팔레아토는 "이중 중대성 보고에 대한 결정의 기저에 자리잡은 가정사항에 대해 검증을 제공하기 위해 이사회가 신뢰할 수 있는 사람들이 필요할 것이다"라고 말했다. 조직, 비즈니스, 프로세스에 대해 깊은 지식을 갖고 있는 내부감사인은 철저하고 신뢰할 수 있는 검증을 제공할 수 있다.

"그린워싱(Greenwashing)"은 이사회가 숙지해야 할 또 다른 개념이다. 이는 조직의 기후 변화 정책이나 조치에 대해 과장 또는 허위 주장을 하는 것을 말한다. 그린워싱으로 의심을 받으면 조직의 평판에 상당한 영향을 미칠 수 있다. 특히 크고 다양한 이해관계자 그룹이 환경 보고의 투명성 제고를 요구하고 있다는 점을 고려하면 더욱 그렇다. 내부감사는 조직이 보고하는 기후 관련 정보에 대해 검증을 제공함으로써 신뢰도를 높일 수 있다. 내부감사는 이러한 모든 주제를 이사회 안건으로 발의하고 이사진이 이를 해결하기 위해 필요로 하는 맥락을 제공할 수 있다.

리스크의 상호연결성

리스크 인 포커스 2024에서는 리스크의 상호연결성, 즉 한 리스크가 다른 리스크를 유발하고 심지어 증폭시킬 수도 있는 방식을 강조했다고 팔레아토는 지적했다. 그 예로, 사이버보안 사고는 일반적으로 IT 팀이나 직접적인 타격을 입는 직원에게만 골치 아픈 일이 아니다. 다른 부정적인 영향 중에서도 고객, 협력업체 또는 기타 이해관계자가 관련된 경우 조직의 브랜드나 공급망 관계에 부정적인 영향을 미칠 수 있는 경우가 많다. 팔레아토는 "리스크를 단절된 사건으로 볼 수는 없다"라고 말했다.

내부감사는 이사회가 직면한, 겉으로는 관련 없어 보이는 다양한 리스크의 점들을 연결하고 그를 이해하는 관점을 제공할 수 있다. 팔레아토는 이사회나 감사위원회가 내부감사 리더와 정기적으로 만나 리스크 관리, 컴플라이언스 우려, 비즈니스 기회 및 프로세스 효율성에 대해 논의할 것을 권고했다. 팔레아토는 "우리는 이 모든 분야에서 비즈니스 파트너가 될 수 있다"라고 말했다. "이것이 이사회를 위해 우리가 지니는 커다란 가치이다."

이사진을 위한 질문

- 이사회는 환경, 사회 및 거버넌스(ESG) 정보 공시 규정에 어떻게 대비하고 있는가?
- 어떤 규정이 조직에 영향을 미치고 있거나 앞으로 미칠 것으로 예상되는가?
- 비즈니스 파트너나 가치 사슬의 다른 구성원에게 ESG 정보를 제공해야 하는가?
- 조직은 전략적 의사결정에 사용하기 위해 신뢰도 높은 ESG 정보를 생성할 수 있는가?

1 "챗GPT는 가장 빠르게 성장하는 사용자 기반 기록을 수립했다 - 분석가 노트" Hu, K., Reuters, Feb. 2, 2023
2 '이중 중대성(Double materiality)': SEC의 기후 계획 논쟁에 개입될 가능성이 있는 새로운 법적 개념, Engler, H., Reuters, April 12, 2022.