제107호 | 2021년 10월

TONE — at the — TOP®

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

OnRisk 2022 : 핵심 리스크에 대한 신속한 통찰

COVID-19 팬데믹과 그로 인한 많은 혼란은 조직이 직면한 다양한 리스크와 불확실성을 이해해야 할 필요성에 대해 중대한 경종을 울렸다. 세계내부감사인협회 (IIA)의 보고서 OnRisk 2022 : 리스크에 대한 이해, 정렬, 그리고 최적화를 위한 가이드 (OnRisk 2022: A guide to Understanding, Aligning and Optimizing Risk)는 조직 거버넌스의 주요 이해당사자 (이사회, 최고경영진, 최고감사책임자 (CAE))의 의견을 수집하여 현재 조직에 관련성이 가장 높은 리스크에 대한 정렬상태를 판단하고 (71페이지 박스 참조), 리스크를 처리하는 최선의 방법에 대한 관점을 얻었다. "이사회는 이 보고서를 통해 자신의 조직에 해당되는 문제점이나 우려사항과, 더 큰 관심이 필요한 영역에 대해 대화를 시작할 수 있습니다"라고 오랜 경력의 CEO이자 공기업 및 민간기업 이사인 크리스타 스틸 (Christa Steele)은 말했다.

이 보고서의 주요 관찰내용을 검토한 결과, 조직에 대한 주요 위협뿐만 아니라 이러한 위협을 처리하는 데 방해가 될 수 있는 몇 가지 장애물이 드러났다.

핵심 영역의 현저한 격차

OnRisk 2022는 응답자들이 특정 리스크가 조직에 얼마나 관련성이 있다고 생각하는지와, 이러한 리스크를 해결할 수 있는 조직의 능력에 대한 믿음 사이에 존재하는 상당한 격차를 포함하여 몇 가지 주요 관찰결과를 제공하고 있다 (70페이지 차트 참조). 이는 개인의 지식, 조직의 능력, 리스크별 관련성에 대해 응답자들이 부여한 등급을 분석하여 결정되었다. 등급은 각 리스크 영역에서 최고 등급 (7점 척도에서 6 또는 7)

을 부여한 응답자의 비율을 기반으로 하였다.

핵심 관찰내용은 다음과 같다

조직이 리스크를 관리하려면 그에 충분한 능력이 있어야 한다. 놀랍게도, 세 응답자 그룹 모두에서 사이버보안이 조직에 관련성이 가장 높은 리스크로 식별된 가운데 OnRisk 2022는 사이버보안이 조직과 매우 관련이 있다고 생각하는 이들 (87%)과 조직이 이 영역에서 출중한 능력을 보유하고 있다고 생각하는 이들 (42%) 사이에 45포인트 차이가 있음을 발견했다. 다른 리스크 영역에서도 눈에 띄는 관련성-능력 격차가 나타났다. 팬데믹으로 인해 자격을 갖춘 인재를 관리하는 일의 가치가 강조된 반면, 인재 관리에서는 46포인트의 관련성-능력 격차가 발견되었다. 응답자들이 향후 3~5년 동안 관련성이 증가할 것으로 예상하는 일부 리스크는 문화 (36포인트), 파괴적 혁신 (34포인트), 경제 및 정치적 변동성 (32포인트)을 포함하여 모두 관련성-능력 격차가 컸다.

여러 리스크 영역에서 리스크 관련성과 조직의 능력에 대한 임원진, 이사진 및 CAE의 응답에 유의미한 차이가 있었다. 조직의 능력과 리스크 관련성에 대한 이해당사자의 견해가 일치할 때 보다 쉽게 강력한 리스크 관리를 달성할 수 있기 때문에, 이러한 차이는 문제가 된다

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

세계내부감사인협회 소개

세계내부감사인협회 (IIA)는
전세계 170여개국에서
20만 명 이상의 회원들을 위해 봉사하는
감사직 종사자들의 단체이다.
IIA는 내부 감사직의 최고 수호단체이자
세계적으로 인정받는 표준의 주창자로서,
주요 연구와 교육을 실시하고 있다.

IIA 주소

1035 Greenwood Blvd. Suite 149 Lake Mary, FL 32746 USA

무료 구독

www.theiia.org/tone을 방문하여 무료 구독을 신청하세요.

독자 피드백

질문 및 의견은 다음 주소로 보내주세요 Tone@theiia.org

이사진을 위한 질문

≫우리 조직은 준법 및 재무 외에 어떤 리스크에 직면해 있는가?

≫우리 조직은 COVID-19 팬데믹으로 드러난 새로운 과제를 다루는 전사적 리스크 평가를 수행하였는가?

≫우리 조직은 직면한 리스크에 대처할 수 있는 능력을 갖추고 있는가?

≫우리 이사회는 우수한 거버넌스를 위해 필요한 전사적 리스크 관리 (ERM) 관점을 수용하고 있는가?

리스크 관련성과 관련하여 임원진보다 (50%) 더 많은 이사진이 (77%) 파괴적 혁신을 관련성이 높은 리스크로 택했으며, 이는 조사 대상 3개 그룹 중 리스크 관련성 등급에 있어 가장 큰 격차였다. 사이버보안의 경우 응답자는 조직의 능력에 낮은 점수 (42%)를 부여했을 뿐만 아니라 관련성 정도에 대해서도 동의하지 않았다. CAE (97%)는 이사진 (87%) 또는 경영진 (77%)보다 관련성이 높은 리스크로 사이버보안을 택했다. CAE (77%)는 또한 이사진 (60%) 및 최고경영진 (67%)보다 공급업체 및 벤더 관리 리스크가 더 관련성이 있다고 언급했으며, 이사진 (63%) 또는 최고경영진 (67%)보다 경제 및 정치적 변동성에 대해 더 걱정하고 있었다 (80%).

조직의 능력에 대한 평가에서 고위경영진은 여러 리스크 영역에서 더 자신감을 보이는 경향이 있었다. 한 가지 예외는 파괴적 혁신으로, 고위경영진의 20%만이 조직의 능력을 높게 평가했으며, 이것은 이사진 (43%)과 비교하여 모든 능력 중 가장 낮은 평가였다. 또한 이것은 두 그룹 간에 능력에 관한 가장 큰 격차였다.

이사회는 인재 관리 및 환경 지속가능성 (각각 20포인트 차이), 조직 거버넌스 (13포인트)와 관련된 리스크를 관리하는 조직의 능력에 대해 고위경영진보다 신뢰도가 낮았다. 각각의 경우 이사회는 CAE와 더 가깝게 일치했다.

ESG 고려 사항에 대한 인식의 차이가 있었다. 이 보고서에서는 세 개의 관련 리스크 영역인 환경 지속가능성, 사회적 지속가능성 및 조직 거버넌스로 세분화하였다.
그 중 응답자들은 조직 거버넌스가 다른 두 개보다 관련성이 훨씬 높다고 생각했다. 투자자와 규제 기관 사이에서 이 리스크 영역에 대한 관심이 높아짐에 따라, 이사회는 조직에서 모든 문제를 이해하고 적절하게 처리하고 있음을 확인하기 위해 ESG 리스크 관리에 대한 내부감사의 검토를 요청할 수 있다.

새로운 리스크 관리 기회

팬데믹은 재무 및 준법 리스크를 넘어선 영역에서 검증 (Assurance)을 얻어야 할 필요성에 대한 인식을 높였다. 외부감사는 주로 이러한 영역에 초점을 맞추지만 내부감사는 이사회 및 경영진의 지원으로 더 넓은 권한을 가질 수 있다. 스틸은 "여기에는 지정학적, 운영, 재무, 준법 및 법적, 문화적 리스크를 포함한 광범위한 리스크가 포함됩니다."라고 말했다. 팬데믹에 비추어, OnRisk 2022 응답자는 운영 및 전사적 리스크에 대해 더 큰 검증을 얻을 수 있는 기회에 관심을 표명했으며 리스크를 사전에 해결해야 할 필요성에 대해 새롭게 인식했다.

스틸은 내부감사가 조직에 대한 거시적 관점을 가지고 있다고 언급했다. "그들은 길을 내려다보고 모퉁이를 돌 수 있습니다."라고 그녀는 말했다. 또한 "세상이 데이터로 넘쳐나는 시기에 이사회에 어떤 정보가 올라와야 하는지에 대한 통찰력을 제공할 수 있습니다." 그런 다음 모든 이해당사자는 동일한 사실 기반의 데이터를 이용하여 가장 필요한 곳에 리스크 관리 자원을 집중할 전략을 식별할 수 있다.
스틸은 감사계획이 조직의 전략적 이니셔티브를 반영할 수 있도록 CAE가 임원회의에 배석할 것을 권고했다. 내부감사 서비스의 확장된 이용은 사이버보안, 인재 관리 및 조직 거버넌스와 같은 관련성이 높은 리스크 영역에서 이사회에 가치를 추가할 수 있는데 이 영역들은 팬데믹으로 인해 더 큰 관심을 받고 있다.

이사진을 위한 다음 단계

팬데믹으로 인해 조직은 리스크 관리 이슈를 면밀히 살펴보고 개선점을 모색해야 했다. 리스크 영향의 범위와 강도가 증가함에 따라 내부감사부서는 의사 결정을 위한 독립적이고 객관적인 검증을 제공하여, 위협을 식별하고 완화하기 위한 지속적인 노력의 핵심 파트너가 될 수 있다. 이사회가 다음 단계를 고려함에 따라, OnRisk 2022는 많은 회사를 괴롭힐 수 있는 문제 영역에 대한 로드맵과 이사회가 자신들의 관련성–능력 격차를 고려하기 위해 사용할 수 있는 모델을 제공한다.

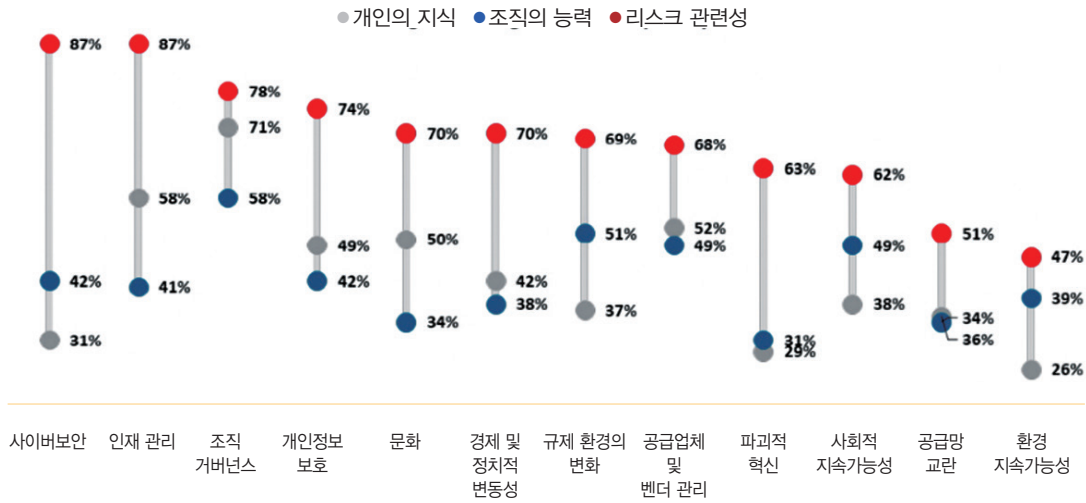
방법론 : OnRisk 접근법

OnRisk 방법론은 90개 조직에서 이사회 구성원 30명, 최고경영진 30명, CAE 30명을 정성적으로 인터뷰한다. 이 연구는 조직이 직면한 리스크에 대한 강력한 시각을 제공하고 리스크 관리 리더의 응답을 바탕으로 객관적인 데이터 분석과 주관적인 통찰력을 모두 허용한다.

인터뷰에서 응답자들은 다음 3개 영역에서 12개의 주요 리스크를 평가하도록 요청받았다 : 각 리스크에 대한 개인 의 지식, 각 리스크를 처리할 수 있는 조직의 능력에 대한 인식, 각 리스크가 조직에 미치는 관련성에 대한 견해.

리스크 영역 별 평균 등급

7점 척도에서 6~7점 등급을 부여한 비중



주 : OnRisk 2022 인터뷰 질문: 나는 다음의 리스크 각각에 대해 얼마나 잘 알고 있는가? 다음의 리스크 각각은 귀사에 어느 정도로 관련이 있는가? 전사적 리스크를 처리함에 있어 귀사의 전반적인 능력은 어떠한가? 응답자들은 7점 척도 (1 : 전혀 아니다, 7 : 매우 그렇다)에서 등급을 선택할 수 있었다. 전체 응답자의 수 = 90명

ONRISK 2022의 주요 리스크

2022년에 조직에 영향을 미칠 수 있는 광범위한 위협 목록에서 12개 리스크를 선택하고 이사진, 최고경영진 및 CAE와의 심층 인터뷰를 통해 검토했다. 여기에는 관련 우려사항을 요약하는 질문과 함께 OnRisk 2022 응답자가 지정한 등급을 기반으로 결합된 리스크 관련성 순서로 표시하였다.

사이버보안 : 조직은 운영 중단 및 평판 손상을 야기할 수 있는 사이버 위협을 관리할 준비가 되어 있는가?

인재 관리 : 원격 근무 전환과 다이내믹한 노동 조건을 고려할 때 조직은 목표 달성에 필요한 인재를 식별, 획득, 교육 및 유지하는 데 어려움을 겪을 수 있는가?

조직 거버넌스 : 거버넌스 (규칙, 관행, 프로세스 및 통제)가 목표 달성을 향상시키거나 방해하는가?

개인정보 보호 : 점점 더 복잡하고 역동적인 국제 규제 환경에 비추어 조직은 민감한 데이터를 적절하게 보호하고 제반 준거 법규를 준수하고 있는가?

문화 : 원격 및 유연 근무 제도의 등장을 감안할 때 조직은 모든 직원의 바람직한 행동을 유도할 사내문화, 인센티브 및 조치를 이해, 모니터링, 관리하는가?

경제 및 정치적 변동성 : 조직은 역동적이며 잠재적으로 불안정한 경제 및 정치 환경에서 관련 도전과제와 불확실성을 모니터링하고 해결하고 있는가?

규제 환경의 변화 : 엄격한 규제 여부에 관계없이, 조직은 역동적이고 모호한 규제 환경에서 리스크를 해결할 준비가 되어 있는가?

공급업체 및 벤더 관리 : 조직은 유익한 제3자 관계를 개발하고 모니터링할 수 있는 준비를 얼마나 갖추고 있는가?

파괴적 혁신 : 조직은 파괴적 혁신에 적응 및/또는 그를 활용할 수 있는가?

사회적 지속가능성 : 조직은 개인과 커뮤니티에 미치는 직간접적인 영향을 이해하고 관리할 수 있는가?

공급망 교란: 조직은 현재 및 미래의 공급망 교란에 적응하는 데 필요한 유연성을 구축했는가?

환경 지속가능성 : 조직은 환경 영향을 안정적으로 측정, 평가 및 정확하게 보고할 수 있는가?

간단 여론 조사

우리 이사회는 조직이 직면한 리스크의 관련성에 대해 최고경영진의 견해와 :

- 항상 정렬되어 있다
- 자주 정렬되어 있다
- 드물게 정렬될 때가 있다
- 한번도 정렬된 적이 없다
- 모름

www.theiia.org/Tone 사이트를 방문하여 응답하고, 다른 사람들의 응답도 확인하세요.

간단 여론 조사 결과

귀사의 이사회에는 사이버보안 전문성을 갖춘 멤버가 있습니까?

출처: Tone at the Top 2021년 8월 설문조사