# TONE at the TOP®

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

## SEC의 새로운 사이버보안 공시 규정: 이사회가 속도를 높이기 위해 해야 할 일


미국 증권거래위원회(SEC)의 새로운 사이버보안 공시 규정은 사이버보안이라는 상존하는 리스크에 대해 강력한 거버넌스의 중요성을 가중시킨다. NACD 기사는 사이버보안 공시 규정이 최근 확정된 점을 고려할 때 "규모를 막론하고 모든 상장 기업이 임박한 기한보다 앞서 규정 준수를 이행하기 위해 경쟁하고 있다"라고 언급했다. [1]

새로운 규정의 영향을 이해하고 규정 준수를 보장하기 위한 조치를 취하는 일은 조직의 최우선 과제가 되어야 한다. Tone at the Top 금번 호는 새로운 지침을 검토하고 기업의 사이버보안 노력에 내부감사가 할 수 있는 핵심적인 기여에 대해 논하고 있다. 또한 이사회 구성원의 새로운 책임과 기타 중요한 고려사항을 강조한다.

### 커져만 가는 위협

사이버보안은 컴퓨터, 네트워크 장치, 소프트웨어 및 데이터를 포함한 조직의 정보 자원을 무단 접근, 장애 또는 파괴로부터 보호하는 것이다. 그러나 사기꾼은 기술의 진보와 함께 사이버보안 공격을 일으킬 수 있는 새로운 방법을 찾아내기 때문에 모든 기업에서 사이버 리스크는 중요한 고려사항이 되었다.

사이버 침해로 인해 엄청난 비용이 발생할 수 있다. 시스코(Cisco) 연구에 응답한 민간 부문 사이버보안 리더 중 거의 60%가 최근 12개월 이내에 사이버보안 사고를 경험했다고 보고했으며, 타격을 입은 이들 중 41%의 피해 금액은 최소 $500,000였다. [2]

직접적인 금전적 피해 외에도 사이버 범죄와 공격은 기업의 업무 수행 능력을 저해하고 기업 및 고객의 기밀 데이터를 유출시키며 평판을 훼손시킬 수 있다.

이러한 점에서 지난 여름 SEC가 상장 기업이 중대한 사이버보안 침해사례를 보고하고 사이버보안 리스크 관리, 전략 및 거버넌스 실태에 대한 정보를 공시하도록 요구하는 새로운 규정(rules)을 발표한 것은 그리 놀랍지 않다. 이 규정은 2022년에 발표된 제안을 수정하여 확정한 것이다.

## 사이버 리스크의 영향

사이버 사고 및 위반이 조직에 가져온 부정적인 영향은 무엇인가?

| 영향 | 2021년 순위 | 2023년 순위 | 2023년 비중 |
|---|---|---|---|
| 운영 마비(공급망/또는 협력업체 생태계 포함) | 1 | 1 | 58% |
| 매출 손실 | 9 | 2 | 56% |
| 고객 신뢰 상실/브랜드 이미지 실추 | 4 | 3 | 56% |
| 평판 훼손 | 5 | 4 | 55% |
| 전략적 이니셔티브 자금지원 중단 | N/A | 5 | 55% |
| 기술적 무결성에 대한 신뢰 상실 | N/A | 6 | 55% |
| 인재 채용/유지에 미치는 부정적 영향 | 8 | 7 | 54% |
| 지적재산권 도용 | 2 | 8 | 54% |
| 주가 하락 | 2 | 9 | 52% |
| 벌금 | 7 | 10 | 52% |
| 경영진 교체 | 5 | N/A | N/A |

### 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/Tone**을 방문하여 무료 구독을 신청하세요.

**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

## 사이버보안 관리, 사고에 대한 공시 확대


SEC의 규정은 증권거래소법의 보고 요건에 따라 상장 기업의 사이버보안 공시를 강화하고 표준화하는 것을 목표로 한다. 새로운 규정은 리스크 관리, 전략, 거버넌스 및 중대하다고 간주되는 사이버보안 사고와 관련하여 기업이 반드시 보고해야 하는 내용을 강화하고 있다. 새 규정에는 다음과 같은 요구사항이 포함된다.

• 등록기업은 사이버보안 위협을 평가, 식별 및 관리하는 방법과 리스크가 비즈니스 전략, 운영 또는 재무 상태에 중대한 영향을 미쳤거나 합리적으로 중대한 영향을 미칠 가능성이 있는지 설명해야 한다. 또한 중대한 사이버보안 사고를 공시하고 사고의 성격, 범위 및 시기의 주요 측면을 설명해야 한다.

• 이사회가 사이버 리스크를 감시하는 방법과 경영진이 중대 리스크를 평가하고 관리하는 역할을 자세히 설명해야 한다. SEC는 이사회의 사이버보안 전문성 공시에 대해서는 제안된 요구사항을 채택하지 않기로 결정했다.

• 해외 비상장 기업에게도 동일한 규정이 적용되며, 외국 관할권에서 공개 또는 공시해야 하는 중대한 사이버보안 사고에 대한 정보를 증권거래소나 증권 보유자에게 반드시 제공해야 한다.

• 조직은 발생한 사이버 사고가 중대하다고 판단한 경우 일반적으로 4 영업일 이내에 8-K 양식(Form 8-K)을 제출해야 한다. (즉각적인 공시가 국가 안보나 공공 안전에 상당한 위험을 초래한다고 미국 법무부 장관이 판단하여 SEC에 서면 통보하는 경우 공시 지연이 허용될 수 있다.)

## 이사회의 핵심 고려사항

많은 조직은 현재 사이버 이벤트를 얼마나 잘 식별, 분석, 관리 및 복구하고 있는지 파악하기 위해 격차 평가를 수행하고 있다. IIA의 표준 및 전문 지침 담당 이사이자 CIA, CRMA, CISA인 조지 바햄(George Barham)은 새 규정에 따라 기존의 평가 프로세스가 4일이라는 처리기한을 지원할 수 있는지 여부를 경영진이 판단했는지 이사회가 보장해야 한다고 말했다. IT 팀이 사고를 식별하는 동안 재무, 법무, 규제담당 팀과 같은 다른 영역의 의견도 중대성 결정에 포함되어 포괄적인 관점을 확보해야 한다.

또한 이사회 구성원은 중대성이 정량적 요소와 정성적 요소를 모두 지니고 있음을 인식해야 한다. 바햄은 "이것은 금전적 영향 그 이상이다"라고 말했다. 또한 법적 및 규제상의 고려사항도 포함된다. 예를 들어, 회사가 유럽 연합에서 영업하는 경우 사이버 사고는 유럽 연합의 일반데이터보호규칙(GDPR)의 적용을 받을 수 있다. 예를 들어 사고가 영업 기밀이나 조직에 경쟁 우위를 제공하는 기타 정보의 유출과 관련된 경우 전략적 고려사항도 중대성 요소가 될 수 있다.
중대성 결정에는 투자자의 기업 분석에 영향을 미칠 수 있는 모든 고려사항이 포함되어야 한다고 바햄은 말했다.

규정의 106 항목은 이사회의 역할과 책임을 다루기 때문에 조직은 매년 10-K 양식을 작성하여 사이버보안 거버넌스를 문서화해야 한다. 예를 들어, 이사회 산하 감사위원회에 사이버 리스크를 검토할 책임이 있음을 보고할 수 있으며 경영진이 사이버보안 이슈를 감사위원회나 이사회에 보고하는 방법도 다룰 수 있다. 이사회의 책임의 일환으로서 이사진은 사이버보안 이슈를 담당하는 임원의 자격요건과 사이버 위협의 관리 및 경감 방식을 이해해야 한다.

## 내부감사의 기여

내부감사인은 널리 채택된 통제 프레임워크의 참조를 포함하여 사이버보안과 관련된 리스크를 경감하는 데 도움이 되는 핵심 내부 통제를 식별하고 검증하는 일을 담당하는 경우가 많다. 새로운 규정에 따라 조직의 거버넌스 기구와 최고경영진은 사이버보안 대응 및 복구 통제장치의 효과성과 효율성을 입증하기 위해 독립적이고 객관적이며 풍부한 지식을 바탕으로 한 보증을 확보해야 한다. 내부감사는 자체 직무 표준은 물론 널리 인정되는 통제 프레임워크, 특히 조직의 IT 및 정보 보안 부서에서 사용되는 통제 프레임워크를 준수하여 이러한 보증을 제공할 수 있다. 내부감사인은 사이버 리스크로부터 기업을 보호하는 최선의 방법을 결정할 때 자문을 제공할 수도 있다.

조직이 새로운 요구사항을 충족시킬 수 있는 방법을 결정할 때 최고감사책임자(CAE)와 내부감사 팀이 수행할 수 있는 구체적인 역할은 다음과 같다.

- 재무, 전략기획, 컴플라이언스 및 감사계획 관점에서 예상되는 SEC 규정의 영향에 대해 이사회, 최고경영진, 사이버보안 리스크 관리 리더에게 컨설팅 제공

새로운 규정 준수와 관련된 리스크 평가를 업데이트하고 요건 충족을 위해 조직을 대비시킴. 내부감사가 아직 사이버보안 리스크 평가에 관여하지 않은 경우 해당 프로세스에 대한 기여를 개시할 수 있음

- 조직이 새로운 규정을 준수할 수 있도록 현재의 사이버보안 통제가 적절하게 설계되어 효과적으로 운영되고 있는지 보고

사이버보안은 일반적으로 조직이 관리해야 하는 가장 큰 리스크 중 하나로 간주된다고 바햄은 지적했다. 따라서 내부감사가 이미 관심을 기울이고 있는 것은 확실하다. 이는 내부감사가 관련 리스크와 이러한 리스크의 경감에 필요한 내부 통제를 인식하고 있음을 뜻한다. 내부감사는 또한 이사회가 새로운 규정에 따라 사이버보안 거버넌스 책임을 충족시키는 데 필요한 정보와 통찰력을 제공할 수 있다. 경영진이 제공하는 관점 외에도 내부감사는 사이버 리스크의 관리 및 공시 방법에 대해 독립적이고 객관적인 관점을 제공할 수 있다. 사이버보안 리스크 및 규정을 감사계획에 포함시키도록 감사위원회에 조언하고 조직이 SEC 규정 준수를 어떻게 대비하고 있는지, 앞으로 얼마나 성실히 이행할 수 있는지 보고할 수 있다.

## 시한의 준수

사고 공시 규정(8-K 양식)은 연방관보(Federal Register)에 공고되고 나서 90일 후에(2023년 12월 18일) 발효된다(중소기업의 경우 최대 180일의 기간 허용). 10-K 양식의 공시는 2023년 12월 15일 이후 종료되는 회계연도의 연례 보고서부터 시작된다. NACD는 새로운 규정이 이사진의 자격요건을 규제하지는 않지만 "리스크 관리에서 이사회, CEO, 최고정보보안책임자(CISO)를 포함한 모든 리더십이 맡은 책임의 수위를 높였다"고 언급했다. 이사진은 새로운 책임을 수행하는 과정에서 사이버보안 문제를 다루기 위해 필요한 확신과 통찰력을 얻기 위해 내부감사에게 의지할 수 있다.

## 이사진을 위한 질문

**▷ 조직은 SEC의 새 규정을 준수할 준비가 되어 있음을 어떻게 확인하고 있는가?**
**▷ 사이버공격을 예방하거나 경감하기 위해 어떤 종류의 통제 수단이 마련되어 있는가? 이러한 수단은 얼마나 성공적이었는가?**
**▷ SEC의 새 규정을 충족시키기 위해 새로운 통제 또는 보고 절차가 마련되어 있는가? 마련되어 있다면 무엇인가?**
**▷ 최근 2년 동안 조직은 중대한 사이버 사고를 겪은 적이 있는가? 그러한 문제는 어떻게 해결되었으며 어떤 개선이 가능한가?**
**▷ 이사회가 사이버리스크 감시 책임을 이행할 때 내부감사로부터 어떤 종류의 검증이나 조언이 도움이 될 수 있는가?**

1 "Time Is of the Essence with SEC's Approved Cybersecurity Disclosure Rules," James Turgal, NACD, September 12, 2023.
2 Cisco Cyber Security Readiness Index: Resilience in a Hybrid World Cisco, March 2023.