# TONE — at the — TOP®

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

## 기존 리스크를 모니터링하기 위한 새로운 툴

*세계내부감사인협회(IIA)는 최근 내부감사인이 중요 이슈를 보다 효과적으로 다룰 수 있도록 지원하는 주제별 요건(Topical Requirements) 시리즈 중 첫 번째를 발표했다. IIA의 국제내부감사직무수행체계(IPPF)에 새롭게 추가된 구성 요소인 주제별 요건은, 감사 대상 주제 영역의 지배구조, 리스크 관리, 통제의 효과성을 평가할 때 내부감사 부서의 규모, 소유 구조, 위치와 관계없이 모든 내부감사기능이 동일한 감사 방법론을 적용하도록 보장한다.*

*주제별 요건은 내부감사기능의 업무 수준을 제고하고, 내부감사가 이사회와 조직에 제공하는 정보 및 인사이트의 가치를 높이는 기준선을 설정한다. 이번 Tone에서는 주제별 요건이 무엇이며, 그것이 이사회 구성원과 그들의 조직에 어떤 의미를 가지는지 살펴본다.*

## 만연해 있는, 고위험 우려사항

내부감사인은 프로세스와 의사결정을 개선하여 가치를 극대화할 수 있도록 독립적이고 객관적인 검증 및 자문을 제공한다. 감사인이 조직의 요구를 충족할 수 있는 지식과 역량을 갖추도록 하기 위해, IIA는 표준과 지침을 정기적으로 보완하고 업데이트한다. 주제별 요건의 도입은 IPPF 발전 프로젝트의 일환이며, 이 프로젝트에는 작년에 도입된 새로운 국제내부감사표준(Global Internal Audit Standards™)과 기타 국제 지침도 포함된다.

주제별 요건은 "자주 감사되는 글로벌 주제로서 일반적으로 위험이 높고 만연해 있는 주제"를 대상으로 한다. 주제별 요건은 성숙한 리스크 영역을 다루며, 확립된 모범 사례에 기반한 지침을 제공한다. 이달 초 사이버보안에 관한 요건이 발표되었으며, 나머지 7개의 주제별 요건은 개발 중에 있다.

## 예정된 주제별 요건

**향후 몇 년 내에 발표될 예정인 주제별 요건은 다음과 같다.**

| | |
|---|---|
| 사이버보안 | 반부패/뇌물 방지 |
| 제3자 관련 리스크 | 인사 관리 |
| 조직 문화 | 부정 리스크 관리 |
| 비즈니스 회복력 | 지속가능성/ESG |

**사이버보안은 첫 번째 주제별 요건으로 우선 채택되었으며,** 이는 대부분 또는 모든 활동에서 조직이 인터넷에 깊이 의존하고 있고, 웹 기반 경계를 보호할 필요성이 크기 때문이다.
내부감사인들은 사이버보안 이슈가 초래하는 위협을 잘 인식하고 있다. 가장 최근에 발간된 글로벌 IIA의 『Risk in Focus』 보고서에 따르면, 내부감사 리더들은 사이버보안을 현재 및 향후 1년간 가장 높은 리스크로 지목했을 뿐만 아니라, 향후 3년간 조직에 가장 큰 위협으로 남을 것으로 예상하고 있다.

응답자들은 인공지능(AI), 생성형 AI(GenAI), 기타 신기술과 관련된 리스크를 포함한 디지털 붕괴(Digital Disruption)라는 연관 주제에 대해서도 우려를 나타내고 있다. 이들은 디지털 붕괴를 현재 및 향후 1년 동안의 상위 5대 리스크 중 하위권에 두고 있으나, 향후 3년을 내다볼 때는 두 번째로 큰 리스크로 간주한다. 생성형 AI는 위협 및 취약점을 탐지하는 데 도움을 줄 수 있지만, 동시에 악의적 행위자들이 더 정교하고 효과적인 공격을 개발하는 것을 더 쉽게 만들 수도 있다.

## 주제별 요건의 활용

주제별 요건은 내부감사인이 만연해 있는 리스크 영역을 어떻게 다루어야 하는지 체계화한다. 주제별 요건은 다음과 같이 기능한다:

- 조직의 리스크를 완화하기 위한 내부감사기능의 기준선을 제시한다.
- 관련된 검증(Assurance) 업무에는 필수적으로 적용되며, 자문(Advisory) 업무에는 적용을 고려할 것이 권장된다.
- 주제별 요건의 적용 여부는 리스크 기반 감사계획에 따라 결정되어야 하며, 이는 최고감사책임자(CAE)가 계획을 수립할 때 리스크 평가가 핵심 요소임을 고려해, 조직의 전략, 목표 및 리스크 평가를 기반으로 판단되어야 한다고 규정하고 있다.
- 각 주제 영역별로 전 세계적으로 일관된 감사 접근 방식을 확립함으로써, 내부감사 서비스의 신뢰성과 그 결과의 일관성을 제고한다.
- 사이버보안 관련 검증 업무 수행에 필요한 기준을 제공한다.
- 조직 전반에 영향을 미치는 영역에 대해서는 전사 또는 조직 단위(Entity or Organizational Level)에서 적용되어야 한다.
- 조직이 최소한 인지하고 있어야 할 광범위한 리스크를 식별한다.
- 적절한 사이버 리스크 범위 설정과 일관성 있는 접근을 통해 내부감사 기능의 가치를 창출한다.
- 검증 업무에서 고려해야 할 모든 측면을 포괄하는 것을 의미하는 것은 아니며, 해당 주제에 대해 일관되고 신뢰할 수 있는 평가를 수행하기 위한 최소한의 요건만을 제시한다.

이 요건들은 내부감사인이 신중하게 판단하여 사용할 수 있도록 설계되어 있다. 이 요건들이 어떻게 활용될 수 있는지를 이해하기 위해, 내부감사 계획 수립 과정에서 사이버보안이 조직에 만연해 있거나 광범위한 리스크로 식별되었고, 해당 주제에 대한 감사를 수행하게 되는 상황을 가정해 보자. 이는 주제별 요건이 반드시 적용되어야 하는 명확한 사례에 해당한다. 그러나 모든 사례가 이처럼 분명하지는 않다. 예를 들어, 한 내부감사팀이 외상매입금(Accounts Payable) 감사를 수행하던 중, 웹 기반 구매요청 프로세스와 관련된 사이버 리스크를 발견했다고 가정해 보자. 비록 감사계획 수립 시 사이버보안이 조직 전체 수준의 리스크로 식별되지 않았더라도, 내부감사팀은 해당 주제별 요건을 보다 제한된 범위 내에서 적용할 수 있다. 이 경우 감사팀은 지배구조나 리스크 관리보다는 사이버보안 통제에 더 많은 시간을 할애할 수 있으며, 감사 범위를 특정 영역으로 한정한 사유를 명확히 문서화해야 한다.

### 세계내부감사인협회 소개

세계내부감사인협회(IIA)는 전 세계적으로 255,000명 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/Tone**을 방문하여 무료 구독을 신청하세요.

### 독자 피드백

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

## 사이버보안 지배구조, 리스크 관리 및 통제

앞서 언급한 바와 같이, 주제별 요건은 각 주제 영역에 대한 지배구조, 리스크 관리, 통제를 모두 포함한다. 지배구조 측면에서 내부감사인은 조직의 지배구조 프로세스가 사이버보안을 적절히 다루고 있는지를 평가해야 한다. 사이버보안 지배구조는 기업의 목적(Goal), 정책, 절차를 효과적으로 추진하기 위한 관련 목표(Objectives)와 전략을 정의한다.

요건의 커뮤니케이션 항목에서는 이사회가 사이버보안의 전략, 리스크, 목표, 통제와 관련해 어떤 자료를 제공받는지를 다루며, 전략적 계획이 사이버보안을 지원하는지를 검토한다. 또한 이 항목은 사이버보안 목적을 달성하기 위해 수립된 정책 및 절차, 역할과 책임, 이해관계자와의 소통, 그리고 사이버보안 목적을 달성하는 데 필요한 자원 요건도 포함한다.

사이버보안 리스크 관리 항목은 사이버 위협을 식별, 분석, 관리, 모니터링하는 프로세스의 필요성을 규정하며, 사이버 리스크에 대한 인지를 신속히 상부에 보고(Escalate)하는 프로세스를 포함한다. 주요 목적은 기업 차원의 리스크 관리 관점에서 사이버보안 리스크 관리가 우선순위로 다루어지도록 보장하는 것이다.

사이버보안 통제(Control)는 사이버 리스크를 완화하기 위해 정기적으로 평가되는 프로세스이다. 총 7가지 통제 프로세스가 있으며, 이는 사이버보안 감사를 수행할 때 내부감사인이 반드시 평가해야 하는 중요하고 기본적인 항목들을 포함한다.

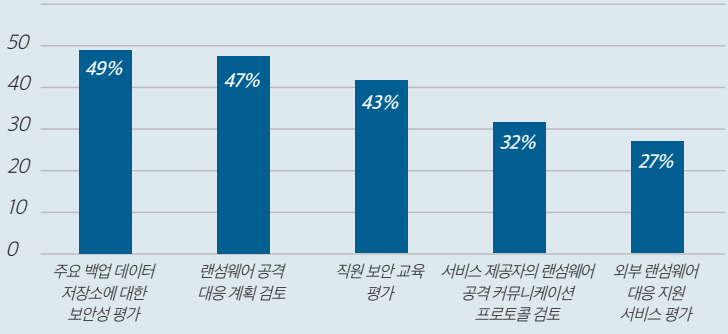
## 일반적이고 변화하는 리스크 해결

내부감사인은 깊이 있고 총체적인 지식을 바탕으로, 조직에 영향을 미칠 가능성이 높은 특정 리스크를 인식할 수 있는 독자적인 자격을 갖추고 있다. 아래 도표 "내부감사의 사이버보안 관여도"는 내부감사기능이 검증 및 정보 제공 측면에서 관여하고 있는 여러 영역을 보여준다. 전 세계의 내부감사 리더들과 다양한 산업 분야의 전문가들로 구성된 그룹에 의해 개발된 주제별 요건은 내부감사 직무의 수준을 한층 발전시키고, 감사인이 일반적이며 변화하는 리스크에 보다 효과적으로 대응할 수 있도록 해줄 것이다.

### 내부감사의 사이버보안 관여도

*인사 및 컨설팅 전문 기업 제퍼슨 웰스(Jefferson Wells)에 따르면, "내부감사팀이 정보보안을 독립적으로 평가하는 관행은, 내부감사팀이 자체적으로 수행하든, 제3자의 지원을 받아 수행하든, 매년 일관되게 유지되어 왔다."*

*그러나 특정 사이버보안 관련 감사업무에 내부감사팀을 활용하는 기업 비율을 보여주는 아래 도표는 많은 조직이 내부감사가 제공할 수 있는 정보와 자문을 충분히 활용하지 못하고 있다는 점을 나타낸다.*

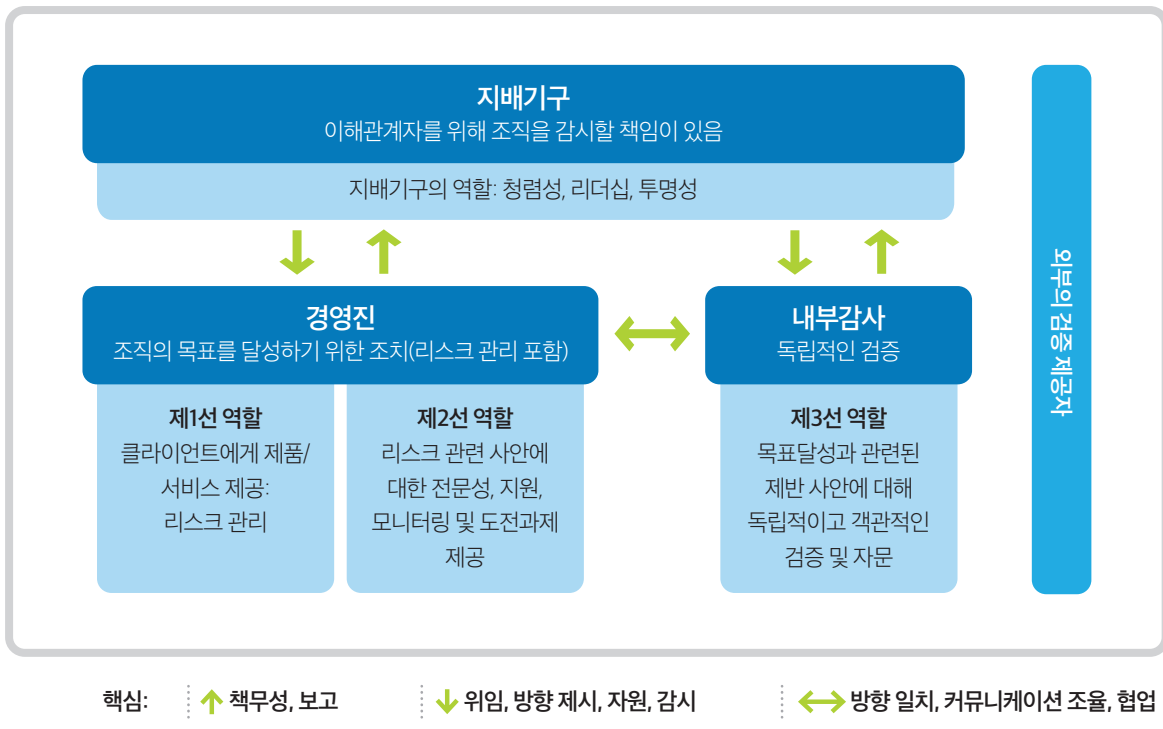



*Source: 2024 Internal Audit Priorities Annual Survey, Jefferson Wells.*

## 주제별 요건과 3선 모델의 연계

IIA는 주제별 요건을 개발하는 과정에서 3선 모델을 활용하였다. 요건에서 지배구조 및 감독 요소는 조직의 지배기구에 해당하고, 리스크 관리 요소는 제2선에, 통제 및 통제 프로세스 요소는 제1선에 해당하며, 내부감사기능은 제3선으로서 독립적인 검증을 제공한다.

### 세계내부감사인협회(The IIA) 3선 모델




## 이사진을 위한 질문

1. 우리 조직의 가장 큰 취약점은 무엇인가?
2. 어떤 유형의 사이버 공격이 우리 조직에 발생할 수 있는가?
3. 배후에 어떤 유형의 적대자가 있을 수 있는가?
4. 적대자의 목적은 무엇인가? — 사업 방해, 데이터 또는 정보 자산의 탈취, 금전적 대가 요구, 혹은 그 외의 다른 목적이 있는가?
5. 그들은 어떻게 공격을 수행할 수 있는가?
6. 우리는 공격 발생을 어떻게 감지할 수 있으며, 즉각적으로 대응할 준비가 되어 있는가?
7. 우리는 사이버보안 리스크 대응을 위해 내부감사가 제공할 수 있는 검증(Assurance) 및 자문(Advisory) 기능을 충분히 활용하고 있는가?
8. 우리 조직은 사이버보안에 인공지능(AI)을 활용하고 있는가? 활용하고 있다면 어떤 방식으로 활용하고 있는가? 활용하고 있지 않다면, AI 도입 가능성에 대해 고려해 본 적이 있는가?