Global Perspectives And Insights

글로벌 시대의 관점과 통찰력

–

3선 방어 모델 – 모든 조직의 성공을 위해 중요

번역자: 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 통역사활동

자문위원회
Nur Hayati Baharuddin, CIA, CCSA, CFSA, CGAP, CRMA – IIA 회원 – 말레이시아

Lesedi Lesetedi, CIA, QIAL – 아프리카 연맹 IIA

Hans Nieuwlands, CIA, CCSA, CGAP – IIA – 네덜란드

Karem Obeid, CIA, CCSA, CRMA
– IIA 회원 – 아랍 에미리트

Carolyn Saint, CIA, CRMA, CPA – IIA – 북미

Ana Cristina Zambrano Preciado, CIA, CCSA, CRMA
– IIA – 콜롬비아

과거 발간호
글로벌 시대의 관점과 통찰력 (Global Perspectives and Insights) 과거 발간호는 www.theiia.org/GPI 참조.

독자 피드백
질문이나 의견을 보내실 곳:
globalperspectives@theiia.org.

세계내부감사인협회 소개
세계내부감사인협회 (IIA)는 세계적으로 널리 인정받는 표준과 가이던스를 주창 및 교육하고, 자격인증을 제공하는 내부 감사직 종사자들의 단체이다. 1941년에 설립된 이래 오늘날 170여개국에서 20만 명 이상의 회원들을 위해 봉사하고 있다. 협회의 글로벌 본부는 미국 플로리다주의 레이크 메리 (Lake Mary)에 위치하고 있다. 보다 자세한 내용은 협회 웹사이트 참조 (www.globaliia.org).

주의
글로벌 시대의 관점과 통찰력 (Perspectives and Insights)에 피력된 견해는 기고자 개인 또는 고용주의 견해와 일치하지 않을 수 있음.

저작권
Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

들어가며

세계적으로 많은 조직이 팬데믹과 디지털 변혁, 경제적 불평등의 심화, 지정학적 변화, 세계화, 기후 변화 등의 난기류를 헤쳐나가는 동안 거버넌스의 중요성은 그 어느 때보다 커졌다. 지배 기구와 경영진은 업무 환경의 혼란, 시장의 변화 및 매출 손실에 대한 질문에 답을 찾기 위해 고심하고 있다. IIA의 3선 모델은 궁극적인 성공을 위해 혁신적인 방법을 뒷받침해줄 강력한 거버넌스를 추구하는 조직에게 시의 적절한 답을 제공한다.

3선 모델은 조직의 목표 달성을 지원하고, 강력한 거버넌스 및 리스크 관리를 촉진하는 최상의 구조를 파악하고, 프로세스를 설계하고, 책임을 분장하는데 도움이 된다. 또한 거버넌스의 3대 주체인 지배 기구, 경영진, 내부감사의 당위성을 설명해 준다. 동시에 거버넌스를 위해 필요한 주요 구성요소(책무성, 조치, 검증 및 자문)의 근본을 규명한다. 기본적으로 이것이 바로 거버넌스이다.

거버넌스는 왜 필요한가?

조직의 주인들은 지배 기구에게 조직의 관리를 맡긴다. 그러나 이사진은 대개 직접적인 관리활동을 하지 않고 다른 일에 종사하는 가운데 일년에 몇 번 모여, 지배 기구가 경영진에게 조치와 자원을 위임하도록 내버려둔다. 이는 조직의 주인을 실제로 일어나는 일로부터 분리시킨다. 인간의 본성, 주관적 성향, 사익 추구 경향, 불확실성, 리스크 및 심지어 부정행위로 인해 가중되는 복잡성을 고려할 때, 뚜렷한 질문이 떠오른다: 이사회는 어떻게 하면 실제로 일어나는 일에 대해 이해당사자에게 정직하게 보고할 수 있을까? 지배 기구는 경영진에게 물음으로써 어느 정도의 확신을 확보할 수 있지만, 궁극적으로 이들에게는 거버넌스의 근간인 독립적이며 객관적인 검증이 필요하다.

조직의 거버넌스는 구조, 규정 및 그를 지키기 위한 실무를 포함하여, 이해당사자의 이익을 보호하려는 노력을 참고한다. 거버넌스는 다음과 같은 이유에서 필요하다.

- **이해당사자들을 위해 조직은 종종 다른 이에 의해 감시된다.**
- **거버넌스 책임이 있는 이가 경영진이 수행하는 모든 일에 대해 직접적인 지식을 갖고 있는 것은 아니다.**
- **조직의 행동에 의해 영향을 받을 수 있는 미래 세대와 같이, 쉽게 파악되지 않는 이들을 포함하여 이해당사자 집단은 매우 다양할 수 있다.**
- **이해당사자들의 이해관계는 서로 다를 수 있고 변할 수 있다.**
- **인간은 믿을 수 없는 존재이거나, 편향되어 있거나, 이기적일 수 있다.**
- **운영은 복잡하고 완전히 이해하기 어려울 수 있다.**
- **매사에는 차이와 불확실성이 존재한다.**

거버넌스는 리더십, 투명성 및 진실성(Integrity)을 통해 이러한 도전과제를 해결하려는 시도로 이해될 수 있다. 거버넌스를 행사하기 위해 필요한 최소한의 요건은 다음에 대한 명확한 책임소재와 정렬이다:

- **조직의 성과를 위해 이해당사자에게 지니는 책무성**
- **리스크를 고려하는 가운데 목표를 달성하기 위한 조치 및 자원의 이용**
- **제반 중대 사안에 대해 관리 책임으로부터 독립적인 객관적 확인 및 검증**

성공적인 거버넌스는 이해당사자들에게 조직의 결정, 조치 및 성과가 조직이 뜻한 목적을 이룰 수 있는 방향으로 이루어져 있다는 확신과 믿음을 제공한다. 우리는 이해당사자들이 무조건적인 성공을 원하지는 않는다는 것을 알고 있다. 이들은 효율적이고, 윤리적이고, 지속가능

한 방식으로 성공을 달성할 것을 요구한다. 이들은 결과뿐만 아니라 행위, 행동, 스튜어드십 등에도 관심을 보인다. 독립적인 검증 없이, 이들의 귀와 눈으로 기능하는 내부감사 없이, 이해당사자나 지배 기구는 실제로 일어나고 있는 일을 어떻게 알 수 있을까?

3선 모델은 무엇인가?

3선 모델은 매우 단순한 프레임워크로, 이해하고 설명하기 쉬우며 심플한 모식도로 표현된다. 6대 핵심 원칙에 기반한 3선 모델은 조직의 성공 추구를 돕기 위해 효과적인 거버넌스에 필요한 역할을 고려하게 만든다. 이러한 역할 및 조직의 성취를 뒷받침하기 위해 각각의 역할이 상호 작용하는 방식을 보다 깊이 이해함으로써, 조직은 스스로에게 적합한 구조를 결정할 수 있다. 이 모델은 리스크를 관리하고 목표를 달성하기 위해 조직에게 필요한 구조와 프로세스를 구축하는 토대로서 조직의 특정한 목적, 환경, 문화, 자원 등과 함께 적용된다.

3선 모델의 대상은?

조직의 성공에 관심이 있는 모든 이는 3선 모델의 대상이다. 보다 구체적으로, 3선 모델의 수혜자는 거버넌스, 경영, 리스크 관리, 외부 검증을 담당하는 이들과 내부감사이다. 내부감사인은 핵심적인 관계에 대한 평가 및 내부감사가 성공에 기여하는 바를 증진시킬 수 있을 뿐만 아니라, 다음과 같이, 내부감사의 위상, 구조, 자원확보, 운영 방식에 영향을 미칠 수 있는 이들과 이 모델을 공유할 수 있다:

- **지배 기구 및 감사위원회**
- **내부감사와 긴밀히 협력하는 이들. 특히 경영진, 리스크 관련 부서, 외부감사인 및 기타 검증 제공자**
- **아웃소싱한 서비스 제공자**
- **규제당국. 특히 금융 부문 규제기관**
- **입법자, 정책 입안자, 선구적 사상가 (Thought Leader), 교육자 및 커리어 자문인**
- **관련 직종 및 업무활동의 표준 기구, 특히 외부감사, 리스크, 거버넌스, 회계, 재무 관리**
- **HR 및 채용 에이전시를 포함하여 내부감사인 고용 조직**
- **위의 당사자들에게 영향을 미치는 전국적, 지역적, 글로벌 단체와 개인**

3선 모델의 제정을 촉발시킨 것은?

2020년 7월 발표된 3선 모델은 20여년 전에 제정된 3선 모델을 숙고 끝에 개정한 것이다. 구 모델이 내부감사직무를 설명하는 심플한 방법으로 잘 알려졌고 널리 채택된 반면, 현대 조직에 대한 이해와 그 관행의 반영을 원하는 목소리가 점점 커지고 있었다.

IIA가 2019년 1월 구 모델의 리뷰를 시작한 가장 중요한 이유는 아마도 내부감사를 방어의 제3선으로 표현한 내용이 시대에 뒤떨어졌기 때문일 것이다. 국제직무수행방안(IPPF)에서 정의한 내부감사의 미션(리스크에 기반한 객관적 검증, 자문 및 통찰을 제공함으로써 조직의 가치를 증진하고 보호함)과 양립할 수 없게 된 것이다. 방어 라는 단어의 사용은 포커스를 지나치게 좁게 만들었다. 내부감사는 미래를 내다보고, 자문과 컨설팅을 제공하고, 나쁜 일을 미연에 방지하는 것 이상의 일을 한다.

구 모델을 비판하는 사람들은 리스크의 개념이 구시대적이라고 말한다. 선이라는 용어의 사용은 사일로(Silo)와 뛰어넘을 수 없는 경계선, 그리고 1선, 2선, 3선의 연쇄적인 작용을 암시한다. 구 모델의 모식도에서 감사위원회의 위치는 조직도 상의 저 멀리 어딘가에 동떨어져 있는 것처럼 보였다. '내부감사는 제3선이므로 나설 수 없다'고 말하는 것처럼 보였다. 중소 기업, 공공 부문 및 규제 대상이 아닌 조직에게는 내부감사가 해당하지 않

는 것처럼 보였다. 내부감사인은 소위 "흐릿한 경계선"과 최고감사책임자(CAE)가 내부감사 이외의 역할을 수행할 때 이것이 의미하는 바에 대해 혼란을 느껴왔다.

이 모델이 여전히 유효한지 판단하고 수년간 쌓여온 비판을 해결하기 위해 능력이 출중한 실무 그룹이 조직되었다. 전문가로 구성된 이 엘리트 팀의 임무는 각각의 도전과제를 신중하게 따져보고 관련된 모든 뉘앙스를 고려하는 것이었다.

구 모델과 같은 점

전세계 2,000 명 이상의 실무자들로부터 수집한 의견과 실무 그룹의 추가적인 연구에 이어, 보다 강력한 모델과 모식도가 등장했다. 신 모델과 구 모델은 다음과 같은 점에서 동일하다.

- IPPF와의 전적으로 일치함
- 권위 있음
- 모든 조직에 적용됨
- 조직이 중복, 격차 및 혼란을 피하는 가운데 리스크 관리를 뒷받침하는 자원과 업무활동을 기획하고 구조화할 수 있도록 고안됨
- 외부 당사자도 일부 고려대상이지만, 주로 조직 내부에 포커스를 맞춤
- 지배 기구, 경영진(리스크 관련 부서 포함) 및 내부감사의 관계와 각자의 역할을 고려함
- 인식 및 연속성을 위해, "3선"이라는 용어와 익숙한 순번 유지
- 단순하고 이해하기 쉬운 모식도로 보충됨
- 원칙에 기반함

달라진 점

3선 모델은 조직의 니즈와 환경을 일치시키기 위해, 원칙에 입각한 접근법을 장려한다. 분명, 모든 조직은 서로 다르고 모두에게 해당되는 접근법은 없다. 그에 따라 이 모델이 기반하고 있는 6대 원칙을 명확하게 정의하였다.

추가적인 중대한 변화는 "선"을 사용하는 대신, "역할"이라는 발상을 고취시키는 용어 사용에 있다. 핵심 역할을 정의하고 새로운 3선 모델의 핵심 역할 간의 관계를 기술하여 조율과 정렬이 조직의 일관성을 보장하고 사일로 현상을 방지하는데 필수적임을 확인한다.

가장 중요한 것은, 신 모델이 통제를 포함하여 거버넌스의 기본적인 구성요소로서 리스크 대응의 적정성 및 효과성을 검증할 필요성을 증가시킨다는 점이다. 이는 체계적이며 절제된 프로세스의 능숙한 적용, 전문성 및 내부감사가 제공하는 통찰을 통해 이루어진다.

원칙

3선 모델 소견서에 기술되어 있는 것처럼, 3선 모델의 원칙은 IPPF의 심장부에 있으며 성공적인 거버넌스가 어떻게 작용하는지 보여주고 있다.

원칙 1: 거버넌스

조직의 거버넌스는 다음을 가능하게 하는 적절한 구조 및 프로세스를 필요로 한다:

- **이해당사자를 위해 지배 기구가 진실성, 리더십 및 투명성을 통해 조직을 감시해야 할 책무성**
- **리스크에 기반한 의사결정[1] 및 자원의 사용을 통해 조직의 목표를 달성하려는 경영진의 조치 (리스크 관리 포함)**
- **명료성과 확신을 제공하고 철두철미한 질의와 통찰력 있는 커뮤니케이션을 통해 지속적인 개선을 유도할 수 있는, 독립적인 내부감사 부서의 검증[2] 및 자문**

원칙 2: 지배 기구의 역할

지배 기구는 다음을 보장한다:

- **효과적인 거버넌스를 위해 적절한 구조 및 프로세스가 마련되어 있음**
- **조직의 목표 및 업무활동은 이해당사자가 우선시하는 이익과 정렬되어 있음**

지배 기구는:

- **법적, 규제적, 윤리적 기대치가 충족됨을 보장하는 가운데 조직의 목표를 달성하도록 책임 및 자원을 경영진에게 위임한다.**
- **목표 달성 진척도에 대한 명료성 및 확신을 제공하기 위해 독립적, 객관적인 유능한 내부감사 부서를 설치하여 감시한다.**

원칙 3: 경영진과 제1선 및 제2선 역할

조직의 목표를 달성하기 위해 조치를 취해야 하는 경영진의 책임(리스크 관리 포함)은 제1선 및 제2선 역할로 구성된다.[3] 제1선 역할은 조직의 클라이언트에게 제품 및/또는 서비스를 전달하는 것과 가장 직접적으로 연관되어 있으며, 이를 가능하게 하는 지원 부서의 역할도 포함된다[4]. 제2선 역할은 리스크 관리를 지원한다.

제1선 및 제2선 역할은 합쳐지거나 분리될 수 있다. 제2선 역할의 일부는 전문가들에게 맡겨 제1선 역할 담당자들에게 필요한 전문성, 지원, 모니터링 및 의견을 보충하게 할 수 있다. 제2선 역할은 법규 및 허용가능한 윤리적 행위의 준수, 내부통제, IT 보안, 지속가능성, 품질보증(QA)과 같은 리스크 관리의 특정 목적에 집중될 수 있다. 제2선 역할은 전사적 리스크 관리(ERM)와 같이, 리스크 관리를 위한 더 넓은 소관 임무로 확대될 수도 있다. 그러나, 리스크를 관리할 책임은 경영의 범위 내에서 제1선 역할의 일부로 남아 있다.

---

1 리스크에 기반한 의사 결정: 분석, 기획, 조치, 모니터링 및 리뷰를 포함하는 프로세스를 고려하고, 불확실성이 목표에 미치는 잠재적 영향을 감안

2 보증: 독립적인 확인 및 확신

3 "제1선", "제2선" 및 "제3선"이라는 용어는 친숙함을 위해 원래 모델로부터 유지하였다. 그러나, "선"이 구조적 요소를 의미하는 것은 아니며, 역할을 구별하기 위해 사용되었다. 논리적으로는 지배 기구 역할도 "선"에 해당하지만 혼란을 피하기 위해 이 용어는 채택하지 않았다. 순번(제1, 제2, 제3)은 연쇄적인 작용을 의미하는 것으로 이해해서는 안된다. 그보다, 모든 역할은 동시에 작용한다.

4 일부는 지원 부서 (HR, 총무 및 건물 관리 등)를 제2선 역할로 간주한다. 명확성을 위해, 3선 모델은 제1선 역할이 "프론트 오피스" 및 "백 오피스 업무활동을 모두 포함한다고 간주하며 제2선 역할은 리스크 관련 사안에 집중하는 보완적 업무활동으로 간주한다.

원칙 4: 제3선 역할

내부감사는 체계적이며 절제된 프로세스, 전문성, 통찰의 유능한 적용을 통해 거버넌스 및 리스크 관리(내부통제 포함)의 적정성과 효과성에 대해 독립적이며 객관적인 검증과 자문을 제공한다. 발견한 결과를 경영진 및 지배 기구에 보고하여 지속적인 개선을 유도한다. 그 과정에서, 다른 내부 및 외부 제공자의 검증을 고려할 수도 있다.

원칙 5: 제3선의 독립성

내부감사의 객관성, 권위 및 신뢰도를 위해서는 내부감사가 경영진의 책임으로부터 독립성을 유지할 수 있어야 한다. 지배 기구에 대한 책무성, 내부감사 업무를 완수하기 위해 인력, 자원 및 데이터에 대한 제한 없는 액세스, 그리고 감사 서비스를 기획하고 전달하는 과정에서 편향 또는 간섭을 받지 않을 자유를 통해 내부감사의 독립성이 달성된다.

원칙 6: 가치의 창조 및 보호

지배 기구의 역할과 제1선, 제2선 및 제3선 역할은 상호간에, 그리고 이해당사자가 우선시하는 이익과 정렬되어 있을 때 집합적으로 가치의 창조 및 보호에 기여한다. 활동의 정렬은 커뮤니케이션, 협력 및 협업을 통해 달성되며, 리스크에 기반한 의사 결정을 위해 필요한 정보의 신뢰도, 일관성, 투명성을 뒷받침한다.

핵심 역할의 설명

갱신된 모델은 구조가 아니라 역할 및 관계에 대한 것이며 역할을 분장, 조합 또는 분리할 수 있는 방식과 역할 간의 상호연관성을 확인하기 위해 선이 아니라 제1선 역할, 제2선 역할 등으로 표현한다. 구 모델에서, 제1선은 경직된 구조적 특징을 가리켰다. 부서, 팀, 심지어 개인은 혼합된 역할을 수행할 수 있기 때문에 이들이 "제1선" 또는 "제2선"에 있다고 말하기 어려웠다. 신 모델은

또한 "선의 붕괴"나 "흐릿한 경계선"과도 거리가 있다. 역할은 항상 명확해야 한다. 역할은 조직이 결정하는(또는 규제당국이 요구하는) 대로 분장될 수 있다. 제1선 및 제2선 역할은 분리되거나 혼합될 수 있다. 개인, 팀 및 부서는 그러한 혼합된 역할을 담당하거나 보다 전문화될 수 있다.

- **제1선 역할은 클라이언트에게 제품 및/또는 서비스를 제공하는 것에 가장 직접적으로 집중하는 역할로, HR, 서무, IT, 건물 관리와 같은 지원 부서 역할도 포함한다. 제1선 역할을 맡은 이들은 리스크 관리의 책임이 있다.**

- **제2선 역할은 리스크 관리의 특정 측면에 집중하는 이들로 윤리적, 법적, 규제적 요건 준수, 통제, 품질 보증(QA), IT 보안, 지속가능성 및 전사적 리스크 관리(ERM)와 같은 보다 넓은 책임을 포함한다. 제2선 역할은 추가적인 도전, 전문성, 감시 및 철저한 검토를 제공한다.**

이 모델은 경영진의 책임이 어떻게 분장되어 있건, 제1선 및 제2선 역할을 구성한다고 기술한다. 어느 정도의 독립성을 위해 지배 기구에 직접 보고하는 제2선 역할의 고위직(예: 최고리스크책임자(CRO))이 존재할 수도 있다. 그러나, 이는 경영진의 책임 범위 내에 머물러 있다.

경영진 및 경영진의 책임으로부터 독립된 내부감사 고유의 위치는 제3선 역할이다. 이러한 독립성 때문에, 객관적인 검증 및 자문을 제공할 수 있다.

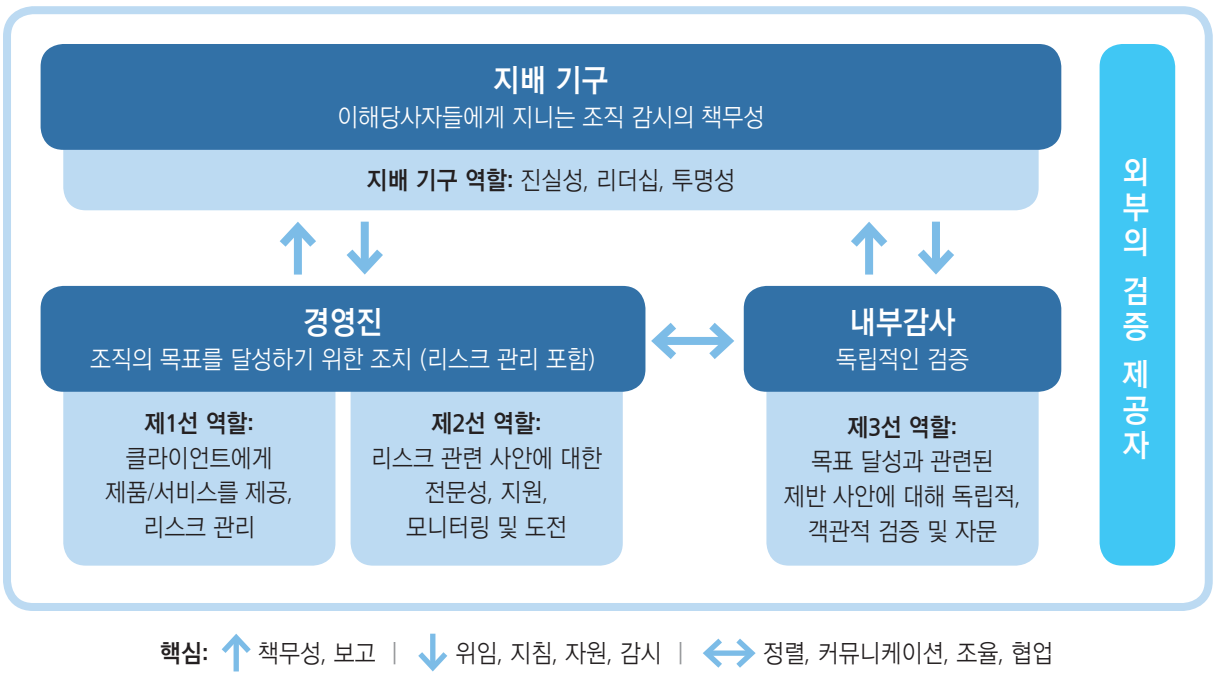
이 모델은 경영진의 책임(즉 제1선 및 제2선 역할)을 수행하면서 동시에 그로부터 독립적일 수 없음을 논리적으로 확인해준다. 내부감사가 이러한 제1선 및 제2선 역할을 수행하고 있다면, 그러한 활동에 대한 독립적인 검증은 다른 이로부터 확보해야 한다.

거버넌스의 근간

새 모델에서 또다른 중대한 변화는 단순히 리스크를 관리하고 통제하는 것과 반대로 리스크 관리의 공격적, 방어적 측면인 가치 창조 및 보호를 모두 포함하여 거버넌스에 기반하고 있다는 것이다.

IIA의 2030 비전은 거버넌스에 필수불가결한 요소로 내부감사를 확립시키는 것이며, 3선 모델은 내부감사를 포함하여 거버넌스의 기본적인 구성요소들이 어떻게 상호 연결되어 있는지 보여준다. 거버넌스에서 내부감사가 맡은 역할의 열쇠는 독립성이지만 독립성이 반드시 단절을 의미하는 것은 아니다. 커뮤니케이션, 협력 및 협업은 필수적이며, 내부감사는 조직의 우선순위에 적절히 대응해야 하고 경영진과 충분히 협력해야 한다.

IIA의 3선 모델



새로운 모식도

언뜻 보아, 업데이트된 모식도는 구 모델을 현대화한 버전으로 보인다. 하지만 자세히 보면 중대한 차이를 발견할 수 있는데, 이 중요한 변화가 거버넌스의 기본원칙을 설명하는데 중심이 된다.

새 모식도는 거버넌스에 3대 요소가 필요하다고 보다 뚜렷하게 정의한다. 그것은: 이해당사자들에게 지배 기구가 지니는 감시 책무성, 조직의 목표를 달성하기 위해 경영진이 취하는 조치(리스크 관리 포함), 독립적인 내부감사 부서가 통찰, 확신, 지속적인 개선 독려를 통해 제공하는 검증 및 자문이다.

새 모식도의 변화로, 지배 기구 역할의 중요성에 대한 인식 제고와 전세계 공공 및 민간 부문의 수용을 위해 이사회 대신 지배 기구라는 용어를 채택한 것이 포함된다. 새 모식도는 경영진과 지배 기구 간에 필요한 만큼 많은 보고선(예: CEO, CRO)을 허용한다. 방어라는 단어를 제외시킴으로써 모식도는 방어가 이 모델이나 일반적인 리스크 관리의 유일한, 또는 일차적인 포커스가 아님을 명확하게 한다.

아마도 가장 중요한 것은 지배 기구 역할과 경영진 및 내부감사 사이에, 그리고 경영진과 내부감사 사이에 양방향으로 화살표가 그려져 있다는 점이다. 이는 세 역할의 관계를 보다 잘 대변하며, 반드시 존재해야 하는 협력을 보여준다. CAE는 내부감사인에게 지배 기구와 함께 프로젝트에 참여하도록 지시할 수 있고, 이사회는 내부감사에게 부정행위에 대한 조사를 이끌도록 요청할 수 있으며 이는 건전한 거버넌스 구조의 부분이다.

3선 모델의 적용

3선 모델은 다양한 구조를 가진 조직에서 적용될 수 있다. 모식도나 모델을 그 자체로 구조도나 조직도로 사용하지 않도록 고안되었음을 이해해야 한다. 이 모델은 제1선 및 제2선 역할이 혼합되거나 분리될 수 있으며, 지배 기구에 많은 보고선(예: CEO, CRO, CCO)이 있을 수 있고 이러한 부서에 필요한 수준의 독립성을 허락했음을 보여주도록 설계되었다.

필요시 여러 개인이 이사회에 직접 보고하도록 구조화할 수 있기 때문에, 준수나 리스크 관리 등을 위해 필요한 일정 수준의 독립성이 확보된다. 제2선 역할 담당자들이 자문, 모니터링, 평가, 보고 및 검증을 제공하는 한, 그 독립성은 내부감사와 똑같지 않을 수 있지만 이들은 실질적으로 제3선 역할을 수행하는 것이다. 또한 리스크 관리에 대해 결정할 때 – 설계 및 구현, 한도 결정, 규정 마련, 목표 수립 등 – 이들은 분명 경영진의 조치와 책임의 일부로 개입하게 된다. 어떤 경우이건 리스크 관리는 경영진의 책임으로 남아있다.

내부감사는 질적으로 다르다. 내부감사는 또 다른 제2선 컨설팅 부서가 아니다. 내부감사는 경영진의 책임 및 결정과 간섭으로부터 독립적이며 지배 기구에게 직접 책임이 있다.

그러나 조직은 목적, 자원, 규제 문화 등에 따라 원하는 구조를 선택할 수 있다. 제1선 및 제2선 역할은, 어떻게 분장이 되었건 경영진의 책임이다. 내부감사는 경영진의 책임으로부터 독립적이다. 제2선 및 제3선 역할은 결합될 수 있을까? 지배 기구의 재량으로 그렇게 할 수는 있지만 역할은 양립할 수 없다. 무언가를 책임지면서 동시에 독립적인 의견을 제공할 수 있는 사람은 없다. 내부감사인이 이 역할을 수행하게 된다면, 독립적인 소견을 제공할 누군가를 찾아야 할 것이다.

기타 고려사항

3선 모델은 여러 역할의 중요성과 각 역할이 어떻게 결합 또는 분리될 수 있는지를 인지하기 때문에 조정이 가능하다. 여러 부문은 자신의 조직에 어울리는 최상의 거버넌스 구조에 따라, 역할을 분장하거나 상호관계를 수립할 수 있다. 그러나 이러한 뉘앙스 차이에도 불구하고, 성공적인 거버넌스의 구조 면에서 내부감사는 근본적으로 동일하다.

다음은 3선 모델과 여러 산업 및 이슈에서 내부감사 부서 수립 시 어려움에 처할 수 있지만 독립적, 객관적인 검증을 제공함으로써 거버넌스를 고취시키기 위해 어떻게 협력할 수 있는지 보여주는 예이다.

전사적 리스크 관리(ERM): ERM은 구조화되고 일관성 있는 리스크 관리 접근법으로, 조직의 목표에 영향을 미칠 수 있는 기회와 위협을 파악 및 평가하고, 그에 대한 대응을 결정하고, 보고함으로써 전사적으로 도움이 된다. ERM은 잘 구현되면 조직 전체에 걸쳐 통합되어 내재된다. 기본적으로, 이것은 건실한 거버넌스 구조가 조직이 내리는 모든 결정의 핵심에 있을 때 3선 모델이 어떻게 기능할 수 있고, 기능해야 하는지 보여주는 공식화된 적용이다. 조직은 리스크 관리를 위해 존재하지 않는다. 리스크 관리는 거버넌스의 일부이다. ERM이 효과적이려면, 그리고 불필요한 중복, 혼란 또는 격차를 피하려면 명료성과 핵심 주체 간의 커뮤니케이션이 필요하다.

금융 서비스: 2008년 금융 위기 이래, 대형 금융 기관과 보험 회사의 내부 통제 구조 및 리스크 관리 부서와 관련된 규제당국의 기대는 더욱 구체화되었다. 그러나 비즈니스, 리스크 관리/컴플라이언스 부서, 내부감사 간에 잘 정의된 분리는 중소 금융 서비스 기업에서는 실용적이지 않거나 규제 요건이 아니다. 3선 모델은 베스트

프랙티스 측면에서 기준을 수립하지만 조직이 고유의 니즈에 따라 각 선의 업무를 보다 유연하게 분리할 수 있는 여지가 있다. 이들은 독립성을 유지하는 가운데 조직을 위해 실용적인 방식으로 기능할 수 있다. 3선 모델은 국내의 중소 기관이나 보험 회사로부터 다국적 대형 기관이나 보험 회사에 이르기까지 모든 금융 서비스 기업에서 사용을 고려해 볼 수 있다.

공공 부문: 정부의 내부감사는 관할권에 따라 다양하다. 예를 들어, 미국에서 내부감사는 지방 자치단체, 주 정부 및 연방 정부마다 다르다. 내부감사는 종종 부서에 내재하며, 부서장에게 보고한다. 내부감사는 유엔(UN) 및 기타 다국간 금융 기관과 같은 조직에서 세분화될 수 있는데, 이들의 업무는 검사(Inspection), 교정(Remediation), 조사(Investigation), 평가(Evaluation) 또는 감시(Oversight) 서비스라 불린다. 내부감사가 검증 제공 이상의 일을 하는 공공 부문에서는 신중함이나 확신의 결여 또는 독립성에 대한 우려가 일반적이다. 진정하게 독립적인 감사위원회가 없는 경우가 많고, 거버넌스는 정치적 사이클을 따른다. 내부감사조직의 목적은 재무적 성과의 최적화보다는 공공 서비스 제공에 집중된다. 직함이 다를 수 있고 감사인이 CAE에게 보고하지 않을 수도 있지만, 공공 부문에서 3선 모델을 적용하면 합의로 귀결된다. 지배 기구는 발견사항을 비교하고 그 결과가 동일한 내부 프로세스의 일부임을 알게 된다.

지속가능성: 공공선을 진작시키거나 사회악을 예방하기 위한 투자는 팬데믹 위기 동안 그 어느 때보다 널리 알려졌다. 이는 지배 기구와 경영진이 매 단계에서 재무 리스크 뿐만 아니라 환경적, 사회적 및 거버넌스 이슈도 고려해야 함을 의미한다. 3선 모델은 장기적인 사고에 대해 올바른 검증을 제공하는데 있어 필수적이다. 내부감사는 조직 내에서 비재무 정보에 대해 검증을 제공하고 장기적 관점에 대해 통찰을 제공할 수 있는 완벽한 위치에 있으며, 3선 모델을 이용한 최상의 구조를 갖추고 있다. 예를 들어 제너럴 모터스(General Motors)는 글로벌 차원에서 거버넌스의 일관성을 달성하기 위해 2020년 7월 3선 모델이 발표되자마자 이 모델을 구현하였다.

중소 기업(SME): SME에서는 전통적으로 특화의 기회가 적고 자원 및 인력이 한정되어 있기 때문에, 종종 제1선 역할과 제2선 역할 간의 조합이 이루어진다. 직무와 직함은 섞여 있다(예: 임원 역할을 하는 이사진). 또한 인하우스 내부감사 부서가 없을 수도 있다. SME는 3선 모델에 제시된 대로 거버넌스의 3대 역할을 갖추지 못할 경우 조직이 감당하게 되는 리스크를 이해해야 한다. 일부 역할은 통합될 수 있다. 그러나 제1선 역할과 제2선 역할의 결합은 여전히 경영진이다. 제3선 역할이 없는 조직에는 거버넌스가 결여되어 있으며, 자신의 성과가 좋게 보이는 것만 이사회에 보고하려는 경영진의 사익 추구 경향에 대해 견제와 균형도 없을 것이다. 제3선 역할은 외부의 서비스 제공자에게 아웃소싱할 수 있는데, "효과적인 내부감사 부서를 유지할 책임은 조직에 있다"(IIA 기준 2070).

부정/투명성: 3선 모델의 구체적인 적용은 이 모델이 적용지침으로 기능하는 가운데 부정, 투명성 및 부패에 있어서 조직에 도움이 된다. 광의로 경영진의 역할을 생각할 때, 부정행위와 관련하여 내부감사의 역할에 집중하면 3선 모델은 강화된다. 경영진이 부정에 관여했는데 내부감사 부서가 없을 경우, 지배 기구는 부정행위자가 확인한 정보에 의존하게 된다.

국제공인부정조사사협회(Association of Certified Fraud Examiners(ACFE))의 2020 글로벌 직무 부정행위 및 직권남용에 대한 보고서에서 내부감사는 내부고발자들이 보고하는 3대 조직의 하나로 밝혀졌다. ACFE의 Report

to the Nations에서도 내부감사는 보고된 부정부패 사건의 15%를 적발하여, 40%인 일반 제보에 이어 두번째로 높았다. 뿐만 아니라, 이 보고서는 부정행위를 방지하는 통제장치로서 내부감사의 존재가 부정행위로 발생한 평균 손실액을 반감시켰다고 밝혔다(74%). 흥미롭게도 이 연구에서 조사한 가장 일반적인 통제장치는 외부감사였고(피해 조직의 83%는 외부감사인에게 재무제표 감사를 의뢰), 내부감사는 적발된 부정의 4%만을 차지했다.

맺음말

새로운 3선 모델에 거는 큰 기대 중 하나는 이 모델이 모든 조직을 포함할 수 있는 적용가능성을 확대하고자 적절한 유연함과 확장가능성을 입증함은 물론, 내부감사의 역할을 명확히 밝히고 내부감사에 보다 큰 확신을 제공하는데 도움이 될 것이라는 점이다. 이 모델은 내부감사 부서 내에서뿐만 아니라, 내부감사의 가치에 대해 지배 기구 및 경영진 내에서도 보다 큰 확신을 제공해줄 것이다.

3선 모델은 자문 서비스 제공에 대한 혼란을 불식시킨다. 자문은 "선의 붕괴" 또는 "흐릿한 경계선"에 해당하거나, 독립성을 위험에 빠뜨리지 않는다. 내부감사는 그 독립성 때문에 가치 있고, 신뢰할 수 있고, 권위 있고, 객관적인 자문 및 통찰을 제공할 수 있는 이상적인 위치에 있다. 효과적인 검증은 훌륭한 통찰을 바탕으로 했을 때 가능하다. 내부감사가 통찰을 제공할 수 없다면 내부감사의 가치를 제한하는 것이다.

이것은 흔히 잘못 이해하는 내부감사와 외부감사의 독립성 비교에도 해당된다. 내부감사는 충분히 독립적이다. 그 독립성은 감사위원회의 감시를 통해 확보된다. 감사위원회는 외부감사의 경우와 마찬가지로, 내부감사의 임면과 보수를 감시한다. 내부감사가 지닌 큰 장점은 조직과 그 성공에 대해 잘 알 수 있는 위치에 있다는 점이다.

전통적인 "선"을 세분화할 수 있거나, 크게 중첩되는 영역이 있기 때문에 3선 모델의 구조는 조직에 따라 다르다. 구조는 영원히 변하지 않는 것이 아니라 변화하는 우선순위와 환경의 맥락에서 계속 리뷰해야 한다. 그렇기 때문에 3선 모델은 그 자체로 여정이다.