세계내부감사인협회 (IIA) 공개 문서

3 선 방어 (Three Lines of Defense)

2019 년 6 월

목차

개요

3 선 방어 (Three Lines of Defense) 모델은 조직의 리스크 관리 및 통제에서 중요한 부분이며, 비판과 지지를 함께 받고 있다. 조직에 대한 신뢰가 공격을 받고 있는 시기이자 상시적인 변화와 격변의 시대를 맞아 세계내부감사인협회 (The IIA)는 3 선 모델의 가치와 유용성을 판단하기 위해 대대적인 리뷰를 실시하고 있다. 본 공개 문서는 리뷰 프로세스의 일부로 세계 각국의 이해당사자들로부터 다양한 의견을 구하고자 고안되었다.

현행 모델의 장점은 간결하고 이해하기 쉬우며, 커뮤니케이션이 용이하다는 것이다. 이사회나 지배 기구 (Governing Body), 고위 경영진 및 운영 관리조직, 리스크 및 준법감시 부서, 내부 감사가 각각 수행하는 역할을 설명하고 있다. 이 모델은 리스크 관리 및 통제 활동의 책임을 배분할 때 혼란, 이해의 차이, 업무의 중복을 피할 수 있도록 도와주며 외부 감사 및 규제당국의 영향도 강조하고 있다.

3 선 방어 (Three Lines of Defense) 모델은 전세계에서 여러 국가 정부와 조직에 의해 널리 채택되었지만, 한편으로는 지나치게 제한적이며 한정적이라는 비판의 소리를 듣고 있다. 비판자들은 이 모델이 기회와 위협을 함께 식별하고 분석하여 대비하는 적극적인 방법 대신, 방어에만 초점을 맞추고 있다고 지적한다. 경직된 구조와 운영의 사일로 (Silo) 현상으로 인해 효율성 및 실효성이 저해될 수 있다. 즉, 현재 조직이 처한 현실을 반영하지 못하고 있는 것이다.

본 문서에서는 3 선 방어 (Three Lines of Defense) 모델을 분석하고, 이 모델을 강화하고 개선할 수 있는 방법을 제안하고자 한다. 그 핵심은 모델의 적용 범위를 가치의 보호로부터 가치의 창출로 확대하는 것이다. 조직을 리스크로부터 보호하기 위해 존재하는 구조와 프로세스는 효과적인 거버넌스 및 조직의 성공에 있어 중요하다. 이해당사자의 니즈와 이익은 조직의 목적을 결정한다. 조직이 이해당사자와 연계되어 있음을 보장하기 위해 거버넌스 메커니즘이 존재한다.

이러한 맥락에서 본 문서는 조직의 성공과 가치 창출에 기여하는 모든 핵심 관계자 (지배 기구 (Governing Body), 경영진, 리스크, 품질, 통제 및 준법감시, 독립적인 내부 감사)에 대해 설명하고 있다. 주로 조직의 내부에 대해 설명하고 있지만 외부 감사, 규제당국 및 기타 관련자들의 역할도 다루었다.

기본 모델의 유연성과 선택의 폭은 넓다. 역할을 어떻게 분배, 분리, 조합할 것인가는 규제당국의 기대와 법적 요건은 물론이고 이해당사자의 바람과 방향을 충분히 고려하는 가운데 각 조직의 지배 기구 (Governing Body)가 내려야 할 결정이다. 또한 사일로 (Silo)화를 피하기 위해 참여자들 간에 긴밀한 조율이 필요하다.

서로 다른 역할 간의 긴밀한 협력과 함께 역할을 자유롭게 분배할 수 있는 재량으로 인해 소위 "흐릿한 경계선 (Blurring of the Lines)"이라 부르는 현상이 발생할 수 있다. 현행 3 선 방어 (Three Lines of Defense) 모델로는 이를 설명할 수 없고 지침을 제공할 수도 없다. 따라서 상충하는 역할을 조합하여 부여하지 않도록 신중하게 고려해야 한다. 특히, 독립성 유지의 중요성을 감안하면 거버넌스, 리스크 관리, 통제장치의 실효성 및 적절성에 대해 신뢰할 수 있는 객관적 보장의 제공 이상으로 내부 감사의 책임이 확대될 경우 각별히 주의해야 한다. 내부 감사가 그 소임을 다할 수 있도록, 보호장치 (Safeguard)가 적용될 수도 있다.

3 선 방어 (Three Lines of Defense) 모델은 지난 20 년 간 지속적으로 그 가치를 입증해 왔다. 본 개정안은 신뢰받는 이 거버넌스 툴을 현대적으로 해석하고 강화하여 그 유용성과 가치를 확대시키고자 한다.

본 문서는 세계내부감사인협회 (The IIA)가 임명하고 Jenitha John 이 의장을 맡고 있는 실무 그룹의 의견과 분석을 반영하였다.

실무 그룹의 서한

"3 선 방어 (Three Lines of Defense)"는 다양한 산업분야에서 거버넌스, 리스크 관리 및 통제를 둘러싼 많은 이슈를 해결하며 봉사해 왔습니다. 20 여년간, 조직의 성공과 지속가능한 가치 창출을 향한 여정에서 조직들은 이 모델을 기반으로 끊임없이 변화하는 운영 환경을 헤쳐왔습니다.

이해당사자들의 기대치 변화와 조직의 복잡성 증가를 인정하여, 세계내부감사인협회 (The IIA)는 전세계의 거버넌스 및 리스크 관리 전문가들과 함께 3 선 방어 (Three Lines of Defense) 모델의 리뷰를 시작하였으며 시시각각 변화하는 오늘날의 환경에서 유관성 (Relevance)을 유지하기 위해 이 모델의 강점, 응용, 실효성에 주목하고 있습니다.

저희 실무 그룹의 목표는 다양한 조직 형태와 급변하는 운영 환경에 적절하게 변용하여 적용할 수 있는 모델을 수립하는 것입니다. 그를 위해서는 모델 전반에 걸쳐 거버넌스, 리스크 관리, 통제 프로세스 간의 역동적인 연계, 조율, 협력이 필수적입니다.

본 리뷰의 목적은 거버넌스 책임자들이 3 선 방어 (Three Lines of Defense) 모델로부터 시사점을 도출하여 조직 내에서 가치의 보존과 제고를 위해 가장 적합한 구조와 자원을 구축하고 배치하도록 돕는 것입니다.

오늘날 3 선 방어 (Three Lines of Defense) 모델의 효과적인 구현 방법에 대해 다양한 견해와 논리가 등장하고 있으며, 저희 실무 그룹은 이해하기 쉬운 토의와 방대한 협의를 통해 3 선 방어 (Three Lines of Defense)를 제안하고자 합니다.

전세계 감사인협회 회원들과 이해당사자들의 집단적인 지혜를 빌리고자 하며, 이 중요한 주제에 대한 세계내부감사인협회 (The IIA)의 입장을 정의하고 모양새를 다듬는 데 도움을 얻을 수 있도록 고견을 청하는 바입니다. 모쪼록 많은 분들의 참여를 부탁드립니다."

Jenitha John, 실무 그룹 의장, 세계내부감사인협회 글로벌 보드 (Global Board) 부의장, FirstRand Ltd, Chief Audit Executive

실무 그룹 멤버:

Mark Carawan, Chief Compliance Officer, Citigroup
Greg Grocholski, Chief Audit Executive, SABIC
Trygve Sørlie, Independent Service Provider, Trygve Sørlie Services EPF
Shannon Urban, Managing Director, EY
Beili Wong, VP, Audit and Risk, CAE, Liquor Control Board of Ontario
Charlie Wright, Chief Risk Officer, Jack Henry and Associates

본 문서에 피력된 견해는 실무 그룹 멤버의 개인적 소견으로, 해당 인물이 속한 조직의 견해를 반영하지 않음.

A. 배경

A.1 3 선 방어 (Three Lines of Defense) 모델 개정의 필요성

3 선 방어 (Three Lines of Defense) 모델은 20 여년 전 처음으로 등장한 이래, 특히 그 기원이 된 금융 부문에서 널리 인정받아 왔다. 세계내부감사인협회 (IIA)는 2013 년 발표한 입장서 "3 선 방어와 효과적인 리스크 관리 및 통제 (The Three Lines of Defense in Effective Risk Management and Control)"에서 이 모델을 공식 채택하였으며, 이후 거버넌스 책임자를 위해 귀중한 툴로써 선전해 왔다. 이 모델의 매력은 리스크 관리 및 통제를 구성하는 다양한 역할과 활동에 대해 직접적으로 간결하게 설명하고 있다는 점이며 (좀 더 광의에서 거버넌스를 고려하지는 못함) 그 가치는 조직이 이러한 역할과 활동에 대한 책임을 분배할 때 혼란, 중복, 이해차이를 겪지 않도록 돕는데 있다.

2013 년 발표된 세계내부감사인협회 (The IIA) 입장서 "3 선 방어와 효과적인 리스크 관리 및 통제 (The Three Lines of Defense in Effective Risk Management and Control)"에 수록된 그림(번역). *제 8 차 유럽 연합 회사법 지침 (EU Company Law Directive) 제 41 조에 관한 유럽내부감사연구연합 (ECIIA)/유럽리스크평가연합 (FERMA) 가이던스 활용*

이 모델이 최초로 수립된 이래 조직의 성격과 조직의 운영 환경, 3 선 각각의 역할과 그 위상, 내부 감사가 조직의 성공에 기여하는 바 등을 포함하여 많은 것이 변하였다. 최근 몇 년간 일련의 스캔들과 위기를 겪으며 조직에 대한 신뢰가 크게 실추되었다. 그 단점을 해소할 수 있다면 3 선 방어 (Three Lines of Defense)는 이해당사자들의 니즈 및 이익에 가장 크게 부합하는 방식으로, 조직에 대한 신뢰를 재건하고 목표를 달성하는데 도움이 될 수 있다.

A.2 3 선 모델의 평가

이 모델은 현대 조직의 복잡성을 해결하는데 한계가 있다는 점 때문에 수년간 비판을 받아왔다. 이 모델을 예시하기 위해 도식화된 그림도 이러한 한계를 강조하는 것으로 보인다. 이 모델을 변용한 몇 가지 대안이 제시되어 왔으나 그 중요성을 인정받아 채택된 것은 아직 없다.

현행 모델은 조직의 니즈에 보다 성공적으로 부응할 수 있도록 개선 및 확대시킬 수 있는 강점을 지니고 있기 때문에, 전면 개정해야 할 필요는 없다.

3 선 방어 (Three Lines of Defense) 모델의 강점	발전 기회
간단 명료. 커뮤니케이션의 용이	이러한 특성을 계속 유지
효과적인 리스크 관리 및 통제의 중요성에 주력	리스크 관리 및 통제를 거버넌스, 조직의 성공, 가치 창출의 일부로 이해
기회와 위협에 대응하는 가운데 조직의 노력 지원	조직의 목표를 향해 전진하는 적극적, 소극적 방법을 모두 장려
리스크 관리 및 통제를 위한 활동과 자원의 배정 시 명료성과 효율성의 기준 제시	전략적 우선순위 및 운영관점의 니즈와 연계하여 조율과 협력의 중요성 강조
리스크 관리 및 통제와 관련하여 각 주요 부서와 외부의 이해당사자가 수행하는 역할을 설명	개별 부서의 역할 및 책임과 거버넌스, 조직의 성공, 가치 창출을 위한 공동 기여에 대해 명료성 제고
핵심 부서를 구성하는 방법 설명	이 모델을 보다 유연하고 기민하게 채택할 수 있는 기회 강조
특히 금융 부문의 조직 및 규제당국이 널리 채택	규모, 부문, 성숙도와 관련하여 조직 간의 차이를 고려하여 유관성을 제시하고 어떤 조직이건 쉽게 채택할 수 있도록 함
리스크 관리 및 통제에서 외부 감사와 규제당국의 역할 인정	모델을 지나치게 복잡하게 만들지 않는 가운데 외부의 기타 이해당사자 및 그들이 거버넌스, 조직의 성공, 가치 창출에 기여하는 바를 고려
“제 3 선 방어 (Third Line of Defense)”로서 내부 감사가 하는 역할을 쉽게 설명	전략적 파트너이자 신뢰받는 자문인으로서 내부 감사의 역할을 수임하기 위해 이러한 설명을 확산
독립성, 객관성, 보장에 대해 유용한 논의의 토대 제공	“흐릿한 경계선 (Blurring of the Lines)”에 대해 설명하고 적절한 보호장치 (Safeguard)를 기술
잘 알려진 단순한 그림으로 표현	모델 그 자체의 변경을 반영하고 발전을 위해 도식 개량

B. 거버넌스: 조직의 성공을 좌우하는 열쇠

B.1 조직의 존재 이유

조직은 취지를 달성하고, 이해당사자들의 구체적인 니즈와 이익에 따라 정의된 바람직한 결과를 산출하고, 다양한 투입을 새로운 결과물로 변형함으로써 가치를 창출하기 위해 설립된다[1, 2]. 이해당사자들은 지배 기구(Governing Body)에게 권한과 자산을 위탁함으로써 대리인으로서 조직에 대한 책임을 갖도록 하며, 결과 뿐 아니라 결과를 달성하는 과정 자체에도 관심을 갖는다[3]. 결국 이해당사자들은 조직이 적절한 결정, 조치, 행위, 결과를 통해 자신들의 목적을 효과적, 효율적, 지속적으로 실현할 것을 기대한다.

조직은 고립 속에 운영될 수 없으며 경제적, 사회적, 정치적, 환경적, 기술적, 물리적 및 기타 많은 요인의 영향을 받는다. 이러한 요인으로 불확실성, 변화, 복잡성, 주관성, 편파성, 이기심, 유한한 자원을 놓고 벌이는 경쟁, 생산능력 및 역량의 제한이 있으며 종종 기회와 위협의 원천이 된다. 조직은 이러한 요인을 조절하는 적절하고 구체적인 수단을 채택함으로써 결정, 조치, 행위, 결과가 이해당사자들의 니즈 및 이익과 연계되도록 하며 그를 통해 전반적인 성과를 최적화한다.

B.2 거버넌스가 조직의 성공 및 가치 창출을 촉진하는 방법

기회와 위협을 다루기 위해 고안된 조치의 예는 다음과 같다.

이해당사자의 관여	자원의 스튜어드십 (Stewardship)	윤리 문화
리더십의 윤리성	리더십의 실효성	방향제시
우선순위의 결정	자원의 위임	목표 설정
책임 분장	특화	업무 분배
불확실성에 대처하는 프로세스	변화에 대처하는 프로세스	성과 측정지표
모니터링과 보고	전문가의 도전	규정의 제정과 검증
독립적인 평가	독립적인 보장	독립적인 조언

[1] 본 문서에서 "조직"은 중앙 정부부처와 지방 자치단체는 물론 규모, 부문, 소유주, 통제의 형태와 무관하게 영세 가족 기업으로부터 다국적 대기업에 이르기까지 형식을 갖추어 구성된 모든 개체를 지칭한다.

[2] 본 문서에서 "이해당사자"는 조직의 활동에 이해가 직결된 모든 당사자를 지칭한다.

[3] 본 문서에서 "지배 기구 (Governing Body)"는 거버넌스 책임을 부여 받은 개인이나 집단을 지칭한다. 단일 및 다층구조의 이사회, 위원회, 유사 기관을 포함하여 구성 방식과 무관하게 조직의 전체 측면을 총괄하여 책임진다. 감사 위원회처럼 지배 기구 (Governing Body) 하에 속한 위원회도 이에 해당된다.

이러한 수단은 효과적인 거버넌스에 기여하며 조직의 성공 및 가치 창출을 가능하게 한다[4]. 이해당사자들의 이익과 연계된 결과를 증진시킬 뿐 아니라 결정, 조치, 행위와의 연계를 유지시킨다.

적절한 거버넌스 수단이 마련되어 있어도, 미래의 일들을 100% 정확하게 예측하거나 성공을 보증하기는 어렵다. 대신, 의사 결정과 조치의 실효성 및 책임성을 극대화하고 윤리적 행위를 권장하고 불확실성을 관리함으로써 성과 전체의 변동가능성을 경감하고 허용가능한 범위 내에서 결과를 달성하게 한다.

앞서 열거된 거버넌스의 수단은 중첩되며 상호 보완적인 4 개의 역할 및 활동 그룹으로 세분된다.

- 리더십과 감시 (Oversight)
- 전략의 실행
- 지원, 가이던스, 통제
- 객관적인 보장과 조언

규제 및 입법 요건 준수를 위해 거버넌스의 구조와 프로세스를 정립할 때, 조직 내에서 이러한 역할 및 활동을 수행할 책임을 적절하게 분장하는 것은 지배 기구 (Governing Body)의 임무 중 하나이다. 조직은 다양하며 시간의 흐름에 따라 변하지만, 거버넌스 역할 및 활동 그룹에서 공통적으로 발견되는 구조적 요소가 존재한다.

- 리더십과 감시 (Oversight)의 책임은 지배 기구 (Governing Body)에게 있다.
- 지배 기구 (Governing Body)는 전략을 실행할 책임을 경영진에게 위임한다.
- 경영진의 책임하에 개별 부서를 설립하여 리스크, 품질, 통제 및 준법감시와 관련하여 지원, 가이던스, 통제를 제공한다.
- 독립적인 내부 감사는 객관적인 보장, 통찰력 (Insight) 및 조언을 제공한다.

이러한 일반적인 토대 위에 거버넌스 역할 및 활동 그룹 중 2 개 이상에 대해 책임을 부여 받은 개인, 팀, 부서가 있을 수도 있다. 본 문서 D.2 의 "흐릿한 경계선 (Blurring of the Lines)"은 이러한 상황을 다루고 있다.

C. 조직의 성공과 가치 창출에 대한 기여

C.1 3 선 모델의 구축

앞에서 기술한 공통의 요소는 3 선 방어 (Three Lines of Defense) 모델의 친숙한 구성요소와 밀접하게 연계되어 있지만 중복과 "흐릿함 (Blurring)"을 허용하고 있다. 이러한 요소들 간에는 3 페이지 (역주! 본 파일에서는 5 페이지)의 익숙한 그림이 제시하는 것보다 훨씬 긴밀한 관계가 존재한다.

[4] 본 문서에서 "거버넌스"는 세계내부감사인협회 (The IIA)의 국제내부감사직무수행기준 (International Professional Practices Framework® (IPPF®)) 용어집에 정의된 "이사회가 조직의 목표 달성을 위한 활동을 보고받고, 지시하고, 관리하고, 모니터링하기 위해 채택한 구조와 프로세스의 조합"과 동일한 의미로 사용되었다.

C.1.1 지배 기구 (Governing Body)

이해당사자들은 지배 기구 (Governing Body)에게 조직의 관리 (Stewardship), 문화, 자산, 활동, 성과, 다른 조직 및 개인과의 관계, 환경에 미치는 영향, 보고 등의 전반적 책임을 위임한다. 그후에는 대개 이해당사자들이 전략적, 운영관련 결정에 직접적인 의견을 제시하기 어려워진다. 이처럼 소유와 거버넌스가 분리되어 있기 때문에 지배 기구 (Governing Body)가 법규 요건 내에서 사회적, 문화적 기대에 부응하는 가운데 조직을 이해당사자들의 니즈 및 이익에 부합하게 경영하고 있음을 보장할 수 있는 수단이 필요하다. 이를 위해 독립적인 감시 및 보고는 물론 주기적인 이해당사자와의 접촉과 청렴성, 투명성, 책임성이 요구된다.

따라서 지배 기구 (Governing Body)의 핵심적 역할은 다음과 같다.

- *솔선수범하여 윤리 문화를 창달하고 유지하며 "최고 경영진의 의지 (Tone at the Top)" 결정*
- *이해당사자들과 접촉하여 결정, 조치, 행위 및 결과가 이들의 이익에 효율적, 효과적, 윤리적, 지속적으로 연계되어 있음을 확신시킴*
- *조직을 위해 윤리적 전략적 리더십을 제공하고 전략적 방향 설정*
- *중대한 프로세스, 책임, 구조의 수립*
- *필요 시 지배 기구 (Governing Body) 산하 위원회 설립*
- *포괄적 성과 목표 수립 및 허용가능한 차이와 오차의 범위 결정*
- *경영진과 내부 감사에 자원 및 권한 위임*
- *리스크, 품질, 통제 및 준법감시 부서가 고안한 내부규정 승인*
- *성과 모니터링*
- *전체 부서가 제출한 보고서 및 보장내용 검토*
- *결정, 조치, 행위 및 결과를 이해당사자들과 관계 당국에 보고*

C.1.2 경영진

지배 기구 (Governing Body)는 보통 경영진에게 전략을 실행할 책임을 위임하고 적절한 자원을 배정한다. 거버넌스와 전략 실행의 분리는 거버넌스 모델의 유형 및 경영진의 거버넌스 참여도에 따라 불분명해질 수 있다.

경영진을 보좌하는 다양한 지원 부서가 존재하는데 이러한 부문은 아웃소싱 되더라도 경영진의 일부로 여겨진다. 예를 들어 재무 및 회계, 인사 (HR), 전산 (IT) 부서는 보통 경영을 지원하는 업무를 수행한다.

경영진에게는 리스크, 품질, 준법감시 및 내부 감사의 지원이 제공된다. 그러나 리스크의 책임주체는 경영진이며 경영진은 통제장치를 설계 및 구축하고, 합의된 성과 변동폭 내에서 전략 실행에 수반되는 불확실성을 관리할 책임이 있다. 이를 100% 정확하게 보장하는 것은 불가능하지만 경영진은 성공의 가능성을 극대화하기 위해 필요한 조치를 취해야 한다.

경영진의 주요 책임은 다음과 같다.

- *조직의 목표 달성*
- *지배 기구 (Governing Body)가 승인한 차이 및 오차 범위 내에서 효율적, 효과적, 윤리적, 지속적 방법으로 이해당사자들의 니즈 및 이익과 연계된 의사결정을 내리고, 조치를 실행하고, 개인의 행동강령을 준수하고, 결과를 도출*
- *결정, 조치, 행위 및 결과에 (긍정적 또는 부정적) 영향을 미칠 수 있는 내외부 요소의 평가*
- *허용가능한 차이 및 오차 범위 내에서 성과를 유지하기 위해 고안된 견제와 균형 제도를 설립하고 운영*
- *현재와 가까운 미래의 운영 환경에 맞게 견제와 균형의 최신성을 유지하고, 실효성이 없거나 결함이 발견될 경우 개비하거나, 더 이상 필요가 없을 경우 완화 또는 제거*
- *결정, 조치, 행위 및 결과가 기대에 못 미칠 때 시정 조치*
- *리스크, 품질, 통제 및 준법감시 부서와 함께 내부규정의 고안 및 수립에 기여. 이러한 규정의 이행 책임*
- *지배 기구 (Governing Body)의 지시사항을 조직 전체에 걸쳐 커뮤니케이션*
- *정책 및 성과 측정지표 설정*
- *모니터링 및 분석 활동*
- *지배 기구 (Governing Body)에 성과 및 예측을 보고하고 보장*

C.1.3 리스크, 품질, 통제 및 준법감시 부서

광의의 경영 지원 부서인 리스크, 품질, 통제, 준법감시 부서는 경영진과 협력하여 실질적 감시 (Oversight), 가이던스, 지원, 반론제기, 통제를 제공하며 특정 분야의 지식과 스킬을 활용할 수 있는 전문성을 갖추고 있다. 이들은 내부규정을 수립하고, 지배 기구 (Governing Body)가 정한 허용가능한 차이 및 오차 범위 내에서 성과를 유지할 수 있도록 설계되었음을 검증한다. 내부규정의 수립, 모니터링, 지속적인 개선에는 내부감사는 물론 경영진도 관여할 수 있다. 측정된 성과의 변동 및 오차는 피할 수 없으며, 이를 파악하여 신중하고 신속하게 대처할 때 가치를 인정받는다. 때로 특정 조치를 승인하는 주체는 리스크, 품질, 통제 또는 준법감시 부서가 될 수 있기 때문에 통제장치로도 기능한다.

이러한 부서의 책임은 일반적으로 경영진의 정책을 지원하고, 역할과 책임을 파악하고, 이행의 목표를 수립하는 것이다. 다음은 구체적인 업무의 예이다.

- *결정, 조치, 행위, 결과에 영향을 미칠 수 있는 알려진 이슈를 분석하고 새롭게 등장하는 이슈를 식별*
- *조직의 성과 변동 및 오차 수용에 발생하는 변화를 파악*

- *전략적 목표와 성과를 연계시키기 위해 경영진이 리스크 프레임워크, 프로세스, 통제장치를 수립하는 것을 돕고, 통제장치가 더 이상 필요하지 않은 시점과 통제장치를 완화하거나 폐지해야 할 시점을 파악*
- *거버넌스, 리스크 관리, 통제 프로세스에 대한 가이던스 및 교육 제공*
- *경영진이 리스크 관리를 효과적으로 실천에 옮기도록 촉진하고 모니터링*
- *경영진에게 새롭게 등장하는 이슈와 규제 환경 변화에 대해 알림*
- *내부 통제의 적절성과 실효성, 보고의 정확성과 완결성, 법규 준수, 미비사항의 신속한 조처 모니터링*

C.1.4 독립적인 내부 감사

내부 감사의 소임은 "리스크 기반의 객관적인 보장, 조언, 통찰력 (Insight)을 제공함으로써 조직의 가치를 증진시키고 보호"하는 것이며, 조직이 그 목적 (예: 가치 창출)을 달성할 수 있도록 직접적으로 기여한다[5].

조직의 일부이면서도 내부 감사는 건전한 거버넌스를 지원하도록 설계된 통제장치, 프로세스, 구조의 적절성과 실효성에 대해 신뢰할 수 있는 객관적 보장을 제공할 수 있다. 지배 기구 (Governing Body)가 효과적으로 감시 (Oversight)를 수행하려면 객관적인 보장이 필요하다. 구조적인 독립성 외에도 내부 감사의 객관성은, 내부 감사인이 객관적인 자세로 엄격하고 체계적인 프로세스를 준수하고 전문가로서의 기준에 부합하는 행동을 할 수 있도록 해준다. 내부 감사의 역할이 성과를 모니터링하고 지배 기구 (Governing Body)에게 보고해야 하는 경영진의 의무를 대체하는 것은 아니지만, 이를 보완하는 필수적인 장치이다. 내부 감사가 업무를 수행하려면 독립성 확보를 위해 지배 기구 (Governing Body)에 직접 보고할 수 있어야 함은 물론 자원, 인원, 기록에 대한 액세스가 필요한데 이를 보장하기 위해서는 지원 및 보고 체계가 있어야 한다.

내부 감사의 업무 계획은 반드시 조직의 전략적 우선순위 및 운영상의 니즈와 명확하게 연계되어야 하며 거버넌스와 그에 내포된 견제와 균형의 적절성 및 실효성에 대해 신뢰할 수 있는 객관적 유권 해석을 제공하는 한편, 발생 가능한 기회와 위협을 파악해야 한다.

[5] 세계내부감사인협회 (The IIA)의 국제내부감사직무수행기준 (International Professional Practices Framework® (IPPF®))

내부 감사의 책임은 다음과 같다.

- *거버넌스, 리스크 관리, 내부 통제의 적절성과 실효성에 대해 보장, 의견, 통찰력 (Insight), 조언 제공*
- *전략적 우선순위 및 운영상의 니즈와 연계된 리스크 기반의 내부 감사와 점검 수행*
- *자산의 보호를 포함하여 운영의 효율성 및 효과성, 보고 프로세스의 신뢰성 및 무결성에 대해 보장, 의견, 통찰력 (Insight), 조언 제공*
- *조직의 준법감시 부서와 해당 부서의 법규, 내부규정, 준칙 및 계약사항 준수상태에 대해 보장과 의견 제공*
- *조직 문화와 행위의 영향력 평가*
- *내부규정 수립에 기여*
- *대두되는 기회 및 위협에 대해 지배 기구 (Governing Body) 및 경영진에 자문 제공*
- *지배 기구 (Governing Body)와 경영진에 보고*

C.1.5 조직의 성공에 기여: 기타 기구

내부 요소 외에도 조직은 가치 창출을 지원하도록 외부 기구 (외부 감사인, 최고감사기구 (Supreme Audit Institution), 규제당국 및 기타)에 의지한다. 그를 통해 이해당사자들은 재무 보고의 정확성과, 경영진의 책임성에 대한 확신을 제고할 수 있다. 외부 기구는 그 역할을 수행함으로써 거버넌스, 리스크 관리, 통제에 한층 더 기여하고, 조직이 그 목적을 향해 발전하고 있으며 조직의 결정, 조치, 행위, 결과가 이해당사자들의 이익 및 니즈와 실질적으로 연계되어 있음을 확인해 준다.

외부 감사/최고감사기구 (SAI)

외부 감사인은 이해당사자들에게 조직의 재무 보고 및 그를 뒷받침하는 제도의 정확성에 대해 추가적으로 독립적 보장을 제공한다. 최고감사기구 (Supreme Audit Institution: SAI)는 공공 부문에서 이 역할을 수행하고 이행 및 준수 (Performance and Compliance) 감사를 실시하며, 추가적으로 점검 (Inspection) 및 사법적 권한을 부여 받기도 한다. 지배 기구 (Governing Body)는 외부 감사나 최고감사기구 (SAI)의 업무를 감시하고 보고를 받을 책임이 있다. 호혜적인 공유와 통합을 위해서는 외부 감사 및 최고감사기구 (SAI)의 기획이 내부 감사의 기획과 조율되는 것이 중요하다. 조직의 초점이 재무적, 비재무적 자본을 모두 반영하는 확대된 형태의 외부 보고로 이동함에 따라, 내외부 감사 모두 추가적인 보장 외에도 이해당사자들을 위한 가치 제고에 한층 더 기여할 수 있게 되었다.

규제당국

규제당국은 재무 보고, 환경 보건 안전, 개인정보, 노동 및 다수의 영역에서 투명성과 책임성을 제고하기 위해 설계된 규정을 적용하고 모니터링한다. 경제 전반에 지니는 파급력 때문에 특히 대형 금융 기관에 주목한다. 일반적으로 규제당국은 조직이 점검 (Inspection), 리뷰, 보고, 과징금의 프로세스를 통해 집행되는 과정을 따를 것으로 기대한다. 많은 국가에서 금융 규제당국은 3 선 방어 (Three Lines of Defense)를 효과적인

거버넌스, 리스크 관리, 통제의 모델로 적극 지지해 왔는데 그 이유는 이러한 활동과 자원을 구축하고 관리하는데 있어 이 모델이 명확하고 간결한 템플릿을 제공하기 때문이다.

책임성, 점검 (Inspection), 감시 (Oversight), 모니터링 및 평가

다자간 금융 기구 (개발 은행)와 같은 일부 공공 부문에서는 (특히 규제기관 부재 시) 책임성, 점검 (Inspection), 감시 (Oversight), 모니터링 및 평가로 다양하게 정의하는 추가적인 역할이 존재할 수 있다. 이 역할을 리스크, 준법감시 또는 내부 감사의 업무에 포함시킬 수도 있고 직접 또는 위원회를 통해 지배 기구 (Governing Body)에 일상적으로 보고하는 특정 부서에 위임할 수도 있다. 보고서는 일반 대중에 공개할 수도 있다. 이러한 업무의 포커스는 대대적인 이니셔티브의 외부적 (특히 환경 및 사회적) 영향은 물론 정책에 맞춰지는 경향이 있다. 모니터링 및 평가의 전문성은 물론 보다 엄격한 독립성에 대한 갈망으로 인해 이러한 활동을 아웃소싱 하거나 전담 부서를 신설하게 된다.

C.2 조율

이 모델을 뒷받침하는 원칙을 성공적으로 적용하려면, 조직의 전략적인 우선순위 및 운영상의 니즈와 연계되지 못한 사일로 (Silo) 사고방식과 활동을 방지할 수 있도록 각 구성요소 간의 고도화된 조율을 추구해야 한다. 기획의 신속성 및 일관성, 실행/모니터링/보고의 효율성과 실효성 제고, 거버넌스의 적절성과 실효성에 대한 명확한 공동의 이해, 보고 및 보장의 피로감 예방, 거버넌스의 전반적 향상이 조율 추구의 장점이다.

거버넌스 프로세스와 구조를 설계하고 수립함에 있어 지배 기구 (Governing Body)는 모든 부서가 역할과 책임을 명확하게 이해하였고, 주기적으로 상호작용하며 커뮤니케이션하고 있음을 확인해야 한다. 지속적인 업무 조율 추구가 중요하다. 자칫하면 연계성이 약화되기 쉽고 조직은 혼란, 이해의 차이, 업무 중복에 노출되어 조직의 성공과 가치 창출을 위한 노력이 전반적으로 무력화될 것이다.

주기적인 커뮤니케이션은 효과적인 조율의 관건이 될 수 있다. 다음과 같은 노력을 통해 더 큰 통합을 도모할 수 있다.

- 개인, 팀, 부서의 목표가 조직의 전략적 우선순위 및 운영상의 니즈와 연계되어 있는지 확인
- 조직내 각 영역의 취지와 역할에 대해 공동의 이해가 도출되었는지 확인
- 거버넌스, 리스크 관리, 통제 측면을 설명하는 공통의 용어 정립
- 전 부서에서 공통의 평가 또는 측정 시스템 사용
- 부서 간 해당 분야 전문가 (Subject Matter Expert)를 포함하는 자원 공유
- 통찰력 (Insight) 확보, 분석, 커뮤니케이션을 촉진하기 위해 데이터와 기술 활용

내부 감사는 조직의 통합을 증진시키는 과정에서 중요한 역할을 수행할 수 있다. 다양한 부서와 내외부 기타 기구가 조직 전체에 대해 수행하는 보장 활동이 일관성 있고, 적절하고, 효율적이고, 신뢰할 수 있고, 연계성이 유지되어 있음을 확인하는 작업이 이에 해당된다. 서로 다른 보장 제공주체가 수행하는 업무는 효과의 극대화를 위해 축적 및 조율되어야 한다. 객관적 보장의 주요 제공자인 내부 감사는 조직을 위해

보장업무의 관리를 향상시킬 수 있으며 지배 기구 (Governing Body)와 조직의 활동 및 역량에 대해 필요한 수준의 보장이 이루어지고 있음을 확인해 줄 수 있다.

D. 확장가능성, 성숙도, 구조선택 및 "흐릿한 경계선 (Blurring the Lines)"

D.1 확장가능성

본 문서에서 새롭게 제안하는 이해방식인 확장가능성은, 3 선 모델을 뒷받침하는 원칙을 한층 유연하고 순응적으로 받아들일 수 있게 해주며 광범위한 조직에 적용시킬 수 있게 해준다.

성숙도가 낮으며 규부터 비교적 자유로운 소규모 조직의 경우 결정, 조치, 행위 및 결과가 이해당사자들의 니즈 및 이익과 연계되도록 유지하기 더 쉽다. 일차적 이해당사자의 수가 더 적을 수 있기 때문에, 이들의 기대치를 추적 및 이해하기도 더 쉽고 성과 변동을 보고하기도 쉽다. 이해당사자와 지배 기구 (Governing Body) 구성원의 경영 활동 및 거버넌스 참여도 더 높을 수 있다. 일반적으로 조직과 운영 환경의 복잡성이 낮으며 타인이 제출하는 보고서에 의존해야 할 필요성도 적고, 지배 기구 (Governing Body)가 직접적으로 감독하기도 더 쉽다.

따라서 작은 조직은 3 선 모델의 거버넌스 역할과 활동을 보다 자유롭게 혼합하여 적용할 수 있다. 또한 경영 여건상 리스크, 품질, 통제 및 준법감시 부서를 개별적으로 설립하기 어려운 대신 운영부서와 통합시키거나 내부 감사에 포함시킬 수도 있다.

반면 조직이 성장함에 따라 복잡성이 증가하여 보다 엄격한 규제 대상이 되고, 같은 업종에 속한 타 조직과의 차별화를 추구하게 되면 3 선 모델의 개정 해석을 활용할 수 있는 범위는 더욱 커진다. 자원이 늘어나면 특화의 기회와 직무의 분리 가능성도 증가한다. 리스크, 품질, 통제 및 준법감시 활동과 내부 감사에 보다 전문적인 전담 인력을 배치할 수 있다.

어떤 경우이건, 3 선 모델의 특정한 형태를 채택하려면 규제당국의 요구사항과 이해당사자들의 기대를 고려하는 가운데 지배 기구 (Governing Body)의 주기적인 리뷰를 통해 결정되어야 한다. 가치 창출과 가치 보호의 우선순위 조정, 거버넌스 역할 및 활동 그룹 간의 분리와 혼합의 정도, 여러 부서에 대한 자원 분배 시 고려사항은 변화하는 니즈와 환경에 따라 다양하게 나타난다.

D.2 "흐릿한 경계선 (Blurring of the Lines)"

3 선 모델에 대한 비판 중 하나는 "흐릿한 경계선 (Blurring of the Lines)"을 제대로 설명하지 못한다는 것이다. 2013 년의 입장서에 수록된 그림에 따르면 3 개 요소는 각각 명확하게 분리되어 있다. 그러나 대부분의 경우 3 개 방어선 간의 분리가 이처럼 뚜렷하지 못하며, 이로 인해 흐릿한 경계선이 거버넌스의 실효성에 미치는 영향에 대한 질문이 제기되어 왔다.

본 문서의 분석은 거버넌스의 실효성에 미칠 수 있는 잠재적 영향이 명확하게 평가되어 있는 한, 내부 감사 부서가 보장 이외의 (Non-assurance) 역할을 수행하여 가치를 증진할 수 있으며 중복되는 상보적 역할과 활동을 수행할 수 있다고 허용한다. 보호장치 (Safeguard)도 반드시 고려되어야 한다. 원칙적으로 지배 기구 (Governing Body)는 아웃소싱 업체나 조직의 개인, 팀 또는 부서에 거버넌스 역할과 활동에 대한 책임을 위임할 수 있다. 상호 관련된 직책을 통합시킴으로써 중복을 최소화하고, 경제성과 효율성을 제고하고, 커뮤니케이션 소요시간을 단축시키고, 경영진과 지배 기구 (Governing Body)가 여러 경로의 보고를 받아야 하는 부담을 축소시키고, 최적화된 결과를 위해 자원을 배치할 수 있다. 동시에, 장기적으로 거버넌스의 전반적 실효성에 영향을 미칠 수도 있는 잠재적으로 *상충하는* 직책의 겸임 여부를 파악하는 것이 중요하다. 지배 기구 (Governing Body)는 조직구조를 둘러싼 여러 옵션의 장단점을 비교함으로써, 반드시 정보에 입각한 결정을 내려야 한다.

내부 감사 부서는 조직 전체에 대해 신뢰할 수 있는 객관적 보장을 제공해야 하기 때문에, 구조적 독립성이 중요함을 감안할 때 "흐릿함"에 대해 각별히 주의해야 한다.[6] 내부 감사 부서는 조직의 니즈에 따라 보장과 보장 이외의 업무를 모두 수행할 수 있다. 다음은 자문 및 기타 보장 이외 업무의 예이다.

- 경영상의 결정에 합의
- 제안
- 현재의 환경과 향후의 조치에 대한 컨설팅
- 변화 이니셔티브에 참여
- 리스크 관련 주제에 대해 교육 실시
- 경영진의 통제 자체 평가 세션 리드
- 경영관련 직책의 수시 수행

내부 감사가 보장 이외의 업무를 수행할 때 최고감사책임자 (Chief Audit Executive (CAE))는 지배 기구 (Governing Body)와 협의하여 이러한 업무가 신뢰할 수 있는 객관적 보장을 제공하는 내부 감사 부서의 업무능력과 상충하는지 여부를 평가해야 하며, 적절한 보호장치 (Safeguard)를 고려해야 한다. 다음은 그 예이다.

- 지배 기구 (Governing Body)에 내부 감사가 수행 요청을 받은 보장 이외 업무나 경영관련 직책에 대해 알리고, 조직 차원에서 신뢰할 수 있는 객관적 보장을 제공하는 내부 감사의 업무능력에 미칠 수 있는 영향에 대해 커뮤니케이션한다.
- 보장 이외의 역할이 명확하게 정의되어 있으며, 가능한 한 시한이 정해져 있는지 확인한다.
- 경영상의 결정과 그에 수반되는 리스크 및 통제장치에 대한 책임을 수락하는 것을 삼간다.

[6] "독립성"과 "객관성"은 관련되어 있지만 서로 다른 개념이다. 본 문서에서는 IPPF 용어집의 정의를 따르고 있는데, 독립성은 "내부 감사 책임을 공평하게 수행하는 내부 감사 활동의 능력을 위협하는 상태로부터의 자유"로 정의되며 최고감사책임자 (CAE)가 지배 기구 (Governing Body)에 보고함으로써 효과적으로 달성된다. 객관성은 "내부 감사인이 자신의 업무 결과에 자긍심을 가지고 품질에 대해 타협하지 않는 가운데 감사를 수행할 수 있게 하는 공정한 태도로 정의되며, 내부 감사인은 감사 사안에 대한 판단 시 다른 이의 의견에 영향을 받아서는 안된다."

- 내부 감사가 최근에 자문이나 경영진의 자격으로 중요하게 관여한 영역을 감사할 때 "냉각 (Cooling off)" 기간을 갖도록 하거나, 아웃소싱 인력을 기용하는 등의 방법을 도입한다.

일부 조직에서는 내부 감사의 직책에 리스크, 품질, 통제, 준법감시 측면을 혼합하기도 한다. 예를 들면 최고감사책임자 (CAE)에게 전사리스크관리 (Enterprise Risk Management) 책임을 부여하거나 리스크 또는 준법감시 부서장이 최고감사책임자 (CAE)에게 보고하는 것이다. 이러한 상황에서는 효과적인 보호장치 (Safeguard)의 중요성이 극대화된다. 최고감사책임자 (CAE)의 보장 이외 직책 수행을 지배 기구 (Governing Body)가 감시하는 것도 효과적인 보호장치 (Safeguard)가 될 수 있다.

참고문헌

IFAC, 2015, *From Bolt-On to Built-In: Managing Risk as an Integral Part of Managing an Organization.*
The IIA, 2013, *The Three Lines of Defense in Effective Risk Management and Control*.
IIA–Netherlands, 2014, *Combining Internal Audit and Second Line of Defense Functions?*
The IIA Research Foundation, 2015, *Combined Assurance: One Language, One Voice, One View.*