Leveraging COSO across the Three Lines of Defense[1]

요약

모든 조직은 달성하고자 하는 목적이 있다. 목적을 달성하고자 하는 과정에서 조직은 이를 위협하는 사건이나 환경과 직면하게 된다. 이러한 잠재적인 사건과 환경들은 조직이 반드시 식별하고, 분석하고, 정의하고, 관리할 리스크를 만들어 낸다. 어떤 리스크들은 조직이 (모두 혹은 일정 부분) 수용할 수 있고, 또 조직이 수용 가능한 수준으로 완전히 혹은 일부 완화될 수 있는 리스크도 있다. 리스크를 완화시키는 많은 방법들 중 효과적인 내부통제를 설계하고 이행하는 것이 가장 핵심적인 방법이다.

COSO 내부통제 통합 프레임워크("COSO 프레임워크")는 조직이 리스크를 효과적으로 관리하는데 필요한 내부통제의 구성 요소(components), 원칙(principals), 요인(factors)를 설명한다. 그러나, COSO 프레임워크에서는 설명된 특정한 임무에 대한 책임을 누가 담당해야 하는가에 대해서는 구체적으로 언급하지 않는다. 리스크와 통제를 관리하는 각각의 그룹이 맡아야 할 역할과 책임은 무엇이며 조직 내 타 그룹과 어떻게 조화를 이룰 것인지가 명확하게 정의되어야 한다. 누락된 리스크와 통제가 존재해서는 안 되고, 불필요하거나 의도하지 않은 중복 업무도 없어야 한다.

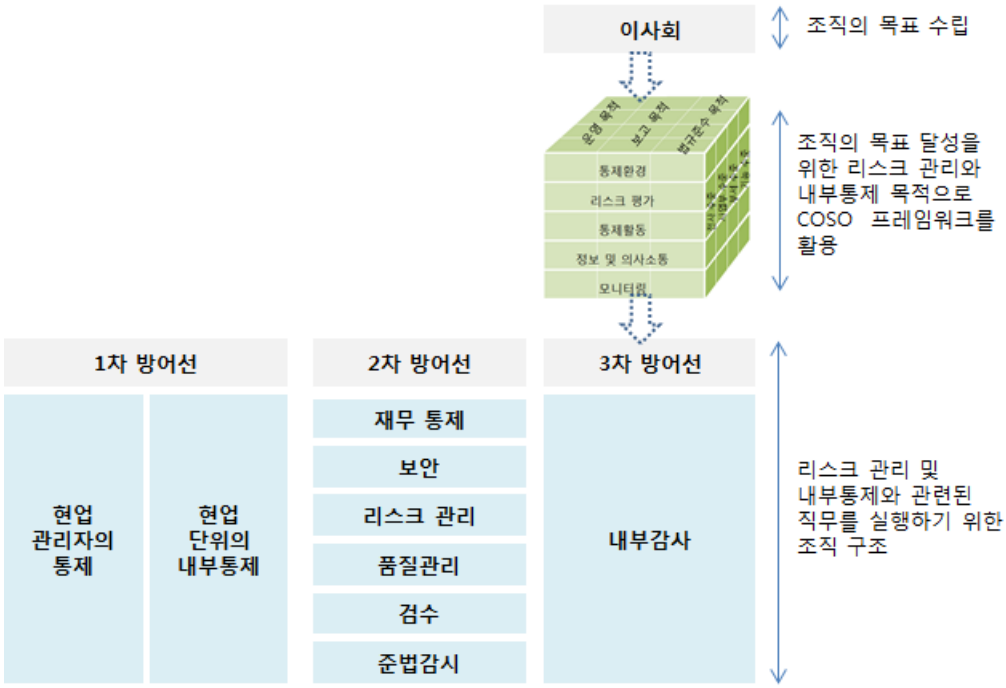
3차 방어선 모형은 리스크 및 통제와 관련된 특정한 직무를, 조직의 크기나 복잡성과 상관없이, 조직 내에서 할당하고 조율할 수 있는 방안을 제시한다. 이사회와 경영진은 이러한 직무들간의 역할과 책임의 중요한 차이를 이해하고, 조직이 목적을 달성할 수 있도록 조직에 가장 적합한 방법으로 배분하여야 한다. 특히, 3차 방어선 모형은, 명확하게 정의되지 않으면 잘못 이해될 수도 있는 확신을 제공하는 업무(assurance)와 모니터링 활동(monitoring)간의 차이와 관련성을 명시하고 있다.

이후의 내용은 독자가 COSO 프레임워크에 대한 기본적인 지식을 보유하고 있다는 것을 전제로기술하였다. COSO 프레임워크에 대해서는 COSO.org에서 더 많은 정보를 확인할 수 있고, 3차 방어선 모형은 뒤의 제1장에 보다 세부적으로 설명한다.

---

[1] 이 자료는 Committee of Sponsoring Organizations (COSO) 와 The Institute of Internal Auditors, Inc ("IIA") 의 공동작업으로 작성되었습니다. 조직 내부에서 내부통제에 대한 역할과 책임을 명확하게 부여하는 방안을 COSO 내부통제 통합 프레임워크(Internal Control – Integrated Framework)과 3차 방어선 모형(Three Lines of Defense Model)을 연계하여 제시함으로써 전반적인 거버넌스 구조를 개선하는 것을 지원하고자 합니다. (July 2015)

[그림 1] 조직의 목표, 내부통제 통합 프레임워크 및 3차 방어선 모형간의 관계



제1장. 3차 방어선 모형

3차 방어선 모형은 역할과 직무를 정의함으로써 리스크 관리와 내부통제를 이해할 수 있도록 한다. 이 모형은 효과적인 리스크 관리와 내부통제를 위해서는 고위 경영진과 이사회의 감독과 지시 하에서, 조직 내의 3가지 분리된 그룹(또는 방어선)이 필요하다는 것을 기본 전제로 한다. 각 그룹(혹은 "방어선")의 책임은 아래와 같다:

1. 리스크 및 통제에 대한 직접적인 책임과 관리 (현업)
2. 경영진을 지원하여 리스크와 통제를 모니터링 (리스크, 통제, 준법감시 기능)
3. 리스크 관리와 내부통제의 효과성에 대해 이사회와 고위 경영진에게 독립적인 확신을 제공 (내부감사)

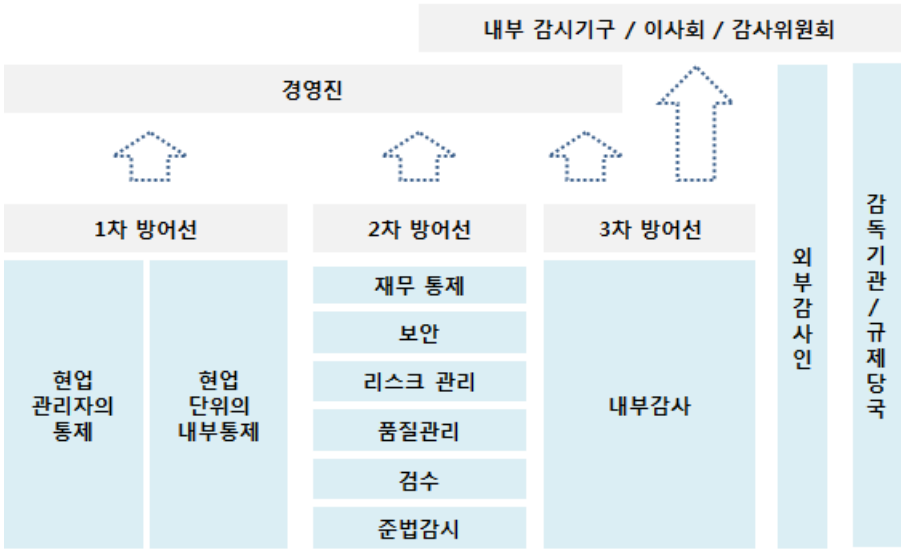
각 방어선은 조직의 거버넌스 체계 하에서 구분된 역할을 담당하며, 각 방어선이 주어진 역할을 효과적으로 이행할 때, 조직 전체의 목표를 달성할 가능성이 높아진다.

조직의 모든 구성원은 내부통제에 일부분 책임을 가진다. 그러나 3차 방어선 모형은 필수적인 직무가 의도한대로 이행될 수 있도록, 세부적인 역할과 책임을 명확하게 정의한다. 조직이 3가지 방어선을 적절하게 구축하고 효과적으로 운용한다면, 누락되거나 불필요하게 중복되는 영역이 없어지며, 리스크 관리와 내부통제가 효과적으로 관리될 가능성이 커진다. 이사회는 조직의 핵심 리스크에 대하여 균형 잡힌 정보와, 경영자가 이러한 리스크에 대해 어떻게 대응하는지에 대한 정보를 보고받을 수 있는 기회가 커진다.

3차 방어선 모형은 COSO 내부통제 프레임워크를 조직 내에 적용할 수 있는 유연한 구조를

제공한다. 각 방어선의 기능은 조직마다 다를 수 있고, 일부 기능은 다른 방어선과 통합되거나 분리될 수도 있다. 예를 들어 2차 방어선의 준법감시 기능이 1차 방어선의 내부통제를 설계하는데 관여하고, 2차 방어선의 다른 조직들은 이러한 통제를 모니터링하는 것에 집중할 수도 있다.

[그림 2] 3차 방어선 모형
효과적인 리스크관리와 내부통제를 위한 3차 방어선 모형, IIA, 2013년 1월



조직이 3차 방어선을 구성하는 방식에 관계없이, 이 모형에는 몇 가지 중요한 원칙이 있다:

1. **1차 방어선**은 조직의 목표 달성을 촉진 또는 저해할 수 있는 리스크를 생성하거나 관리하는 활동을 수행하는 현업의 업무담당자에게 존재하며, 적절한 리스크를 수용하는 것을 포함한다. 1차 방어선은 리스크에 대한 직접적인 책임이 있으며, 리스크에 대응하기 위한 통제를 설계하고 실행한다.
2. **2차 방어선**은 전문성을 바탕으로 1차 방어선을 모니터링함으로써, 경영진이 리스크가 효과적으로 관리되고 있다는 확신을 얻는 것을 지원하는 역할을 한다. 2차 방어선은 1차 방어선과 분리되어 있지만 여전히 경영진의 관리 하에 있으며 일반적으로 일부 관리 기능을 수행한다. 2차 방어선은 기본적으로 리스크 관리에서 많은 역할을 담당하는 관리 및 감독기능이다.
3. 3차 방어선은 1차 및 2차 방어선의 활동이 경영진과 이사회의 기대에 부합되는지에 대한 확신을 제공한다. 3차 방어선은 객관성과 조직 내에서의 독립성을 확보하기 위해 일반적으로 관리기능을 수행하지 않는다. 또한 3차 방어선은 이사회의 주요 보고라인이 된다. 따라서 3차 방어선은 관리기능이 아닌 확신을 제공하는 기능으로서, 이는 2차 방어선과 구분된다.

모든 조직의 목표는 그 목적을 달성하는 것이다. 목적을 추구하는 과정에는 기회를 포착하고, 성장을 추구하며, 리스크를 수용하고 관리하는 것을 포함하는데, 이 모두가 조직의 발전을 위한

활동들이다. 적절한 리스크를 수용하지 못하거나, 수용한 리스크를 적절히 관리하고 통제하지 못하면 조직이 목표를 달성하지 못할 수 있다. 기업가치를 창출하는 활동과 기업가치를 보호하는 활동은 언제나 상충관계에 있다. COSO 프레임워크는 리스크와 통제가 적절한지 그리고 적절하게 관리되고 있는지를 확인할 수 있는 구조를 제시한다. 3차 방어선 모형은 조직 구조에 대한 지침을 제공하여 효과적인 리스크 관리와 내부통제를 위한 역할과 책임을 배분한다.

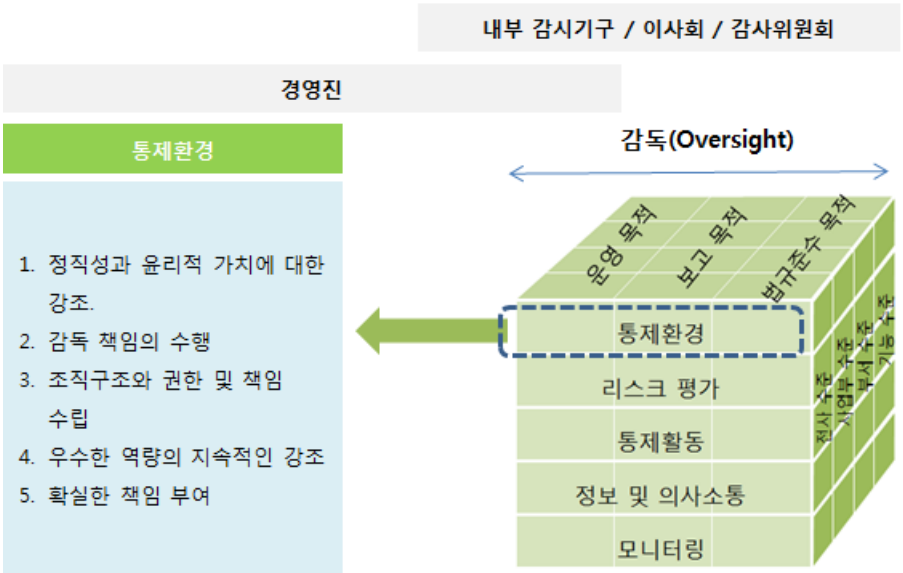
3차 방어선 모형에서 경영진과 이사회의 역할

경영진과 이사회는 3차 방어선 모형에서 핵심적인 역할을 한다. 경영진은 이사회의 감독 하에 내부통제 시스템을 선택하고 개발하며 평가할 책임이 있다. 경영진이나 이사회는 3차 방어선 모형의 일부분으로 고려되지는 않지만, 이들은 조직의 목표를 수립하고, 목표를 달성하기 위한 상위 수준의 전략을 수립하며, 최적의 리스크 관리를 위한 거버넌스 구조를 수립할 책임을 진다. 이들은 또한 리스크 관리와 내부통제에 관련된 역할과 책임을 배분하기에 최적화된 조직구조를 구성할 수 있는 위치에 있다. 경영진은 강력한 지배구조와 리스크 관리 및 내부통제를 전적으로 지원하여야 하며, 1차 방어선 및 2차 방어선의 활동에 대하여 궁극적인 책임을 진다. 3차 방어선 모형의 성공적인 이행을 위해서는 경영진의 참여가 필수적이다.

COSO 프레임워크는 이사회와 경영진의 이러한 책임을 구체화 하는데 도움을 준다. 아래 <그림 3>에서처럼, 경영진과 이사회는 리스크 관리와 내부통제에 대한 조직의 전반적인 분위기를 수립하는 통제환경(Control Environment)을 조성하는데 기본적인 책임이 있으며, COSO 프레임워크에서는 통제환경에 대하여 5가지 내부통제 원칙(Principal)을 제시하고 있다.

3차 방어선 모형은 COSO 프레임워크 하에서 역할과 책임을 배분하는 구조를 제공하며, 효과적으로 이행되기 위해서는 이사회와 경영진의 적극적인 지원이 필수적이다.

[그림 3] 통제환경(Control Environment)에 대한 감독책임



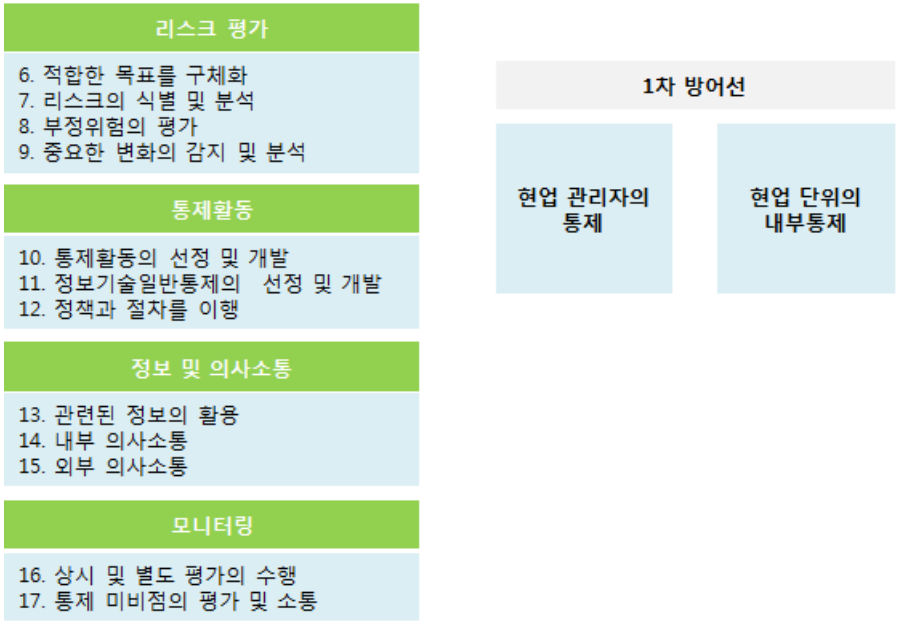
1차 방어선: 현업 차원의 관리

1차 방어선은 리스크 관리와 내부통제를 일상적으로 수행하는 현업의 관리자 수준에서 다루어진다. 현업 관리자는 조직의 내부통제와 리스크 관리 프로세스를 개발하고 실행한다. 이는 주요 리스크를 식별하고 평가하며, 경영진이 의도한대로 업무를 수행하고, 부적절한 프로세스를 보고하고 통제 상의 결함을 처리하며, 통제의 운영에 대해 주요 이해관계자들과 의사소통하는 활동을 포함한다. 현업 관리자들은 맡은 영역에 있어서 이러한 업무들을 수행할 수 있는 역량을 보유하여야 한다.

경영진은 1차 방어선 활동에 대해 전반적인 책임을 가진다. 특정한 고위험 영역에서는 경영진이 1차 방어선의 역할을 직접 수행하는 등 1차 방어선의 관리를 직접 감독하기도 한다.

1차 방어선에 있는 개인들은 COSO 프레임워크 중 리스크 평가(Risk Assessment), 통제활동(Control Activities), 정보 및 의사소통(Information & Communication) 등 4가지 통제 구성요소에 대하여 중요한 책임을 가진다. <그림 4>에 표시된 것처럼, 현업 관리자들은 COSO 프레임워크의 나머지 12개 내부통제 원칙(Principals)에 대해 주된 책임이 있다.

[그림 4] COSO와 1차 방어선



2차 방어선: 내부 모니터링 및 감독 기능

2차 방어선은 1차 방어선에서 실행하고 있는 내부통제와 리스크 관리 과정이 적절하게 설계되고 의도한대로 운영되는지를 확인하기 하기 위해 다양한 리스크 관리와 준법감시 기능을 포함한다. 이는 관리 기능으로써 1차 방어선의 현업 관리와는 분리되지만 여전히 경영진의 통제와 지시 하에 있다. 2차 방어에 있는 기능들은 일반적으로 조직 내에서 운영 중인 내부통제와 리스크를

지속적으로 모니터링하는 책임을 진다. 2차 방어선은 이행전략을 정의하고, 리스크 분야의 전문성을 제공하며, 정책과 절차를 실행하고, 관련된 정보를 수집하여 리스크와 내부통제에 대한 전사적인 시각을 형성할 수 있도록 지원하며, 현업 차원의 관리와 밀접하게 협업한다.

2차 방어선은 조직의 규모나 산업에 따라 매우 다양하게 구성될 수 있다. 대기업, 상장기업, 혹은 복잡하거나 규제가 많은 산업에서의 2차 방어선은 1차 혹은 3차 방어선과 명확하게 분리, 구분될 수 있다. 반대의 경우 일부 2차 방어선 기능은 다른 기능과 통합되거나 존재하지 않을 수도 있다. 예를 들어 일부 조직에서는 법무부서와 준법감시부서를 하나로 통합하거나 보건 및 안전관리부서를 환경 관련 기능과 결합하기도 한다. 어떤 조직에서는 1차 방어선 관리자들이 2차 방어선의 일부 혹은 전체 직무들을 함께 맡는 경우도 있다.

전형적인 2차 방어선의 기능은 특정 영역에 대한 다음과 같은 특별한 전문가 그룹을 포함한다:

- 리스크 관리
- 정보 보안
- 재무적인 통제
- 물리적 보안
- 품질
- 보건 및 안전
- 검수
- 준법감시
- 법규
- 환경
- 공급망
- 기타 산업별, 회사별 필요에 의한 조직

경영진의 감독 하에서 2차 방어선은 특정한 통제를 모니터링하여 설계된 대로 작동하는지를 판단한다. 2차 방어선이 수행하는 모니터링 활동은 일반적으로 COSO 프레임워크에서 제시하는 내부통제의 3가지 목적(운영, 보고, 법규 준수) 모두를 다룬다.

2차 방어선에 내 개인의 책임은 다양하지만 일반적으로 아래사항을 포함한다.

- 리스크 관리를 위한 프로세스와 내부통제를 경영진이 설계하고 개선하는 것을 지원
- 모니터링 대상이 되는 활동과 경영진이 의도한대로 작동되는지를 평가할 수 있는 지표를 정의
- 내부통제 활동의 적절성 및 효과성을 모니터링
- 중요한 이슈나 신규 리스크, 예외사항 등을 보고
- 리스크 관리 프레임워크 제공
- 조직의 리스크 관리와 통제에 영향을 미치는, 이미 알려진 이슈나 신규 이슈들을 식별하고 모니터링
- 리스크 선호도와 리스크 허용 한도의 잠재적인 변화를 파악
- 리스크 관리와 내부통제 프로세스와 관련된 지침과 교육훈련 제공

2차 방어선이 수행하는 모니터링은 조직의 특정한 필요에 맞게 수정되어야 한다. 일반적으로, 이들의 활동은 일상적인 현업 활동과 분리되어 있다. 많은 경우 모니터링 활동은 조직 전반적으로 퍼져 있으나 일부 조직들은 모니터링 활동을 단일 혹은 소수의 영역으로 제한하기도 한다.

각각의 2차 방어선 기능은 1차 방어선을 구성하는 활동과는 어느 정도의 독립적으로 움직이지만, 태생적으로 관리 기능을 한다. 2차 방어선 기능은 조직의 내부통제와 리스크 프로세스를 직접 개발, 실행, 혹은 수정할 수도 있으며, 특정한 관리 활동에 대해서는 의사결정을 할 수도 있다. 2차 방어선 기능이 1차 방어선 활동에 직접적으로 관여하는 한 1차 방어선으로부터 완전히 독립적이지는 못할 것이다.

비록 독립적이지는 않지만, 강력하고 효과적인 2차 방어선 기능은 매우 중요하다. 이들은 적절한 수준의 객관성을 유지하면서 1차 방어선이 수행하는 리스크 관리와 내부통제에 대한 중요하고 유용한 정보를 경영진과 이사회에 제공할 수 있어야 한다. 또한 1차 방어선에서 다루지 않은 전사적인 관점의 리스크와 통제에 대한 정보를 경영진과 이사회에 제공할 수도 있다. 효과적인 방어선이 되기 위해서는 조직 내부에서 충분한 위상이 보장되어야 한다. 2차 방어선의 위상은 권한과 존경을 받을 수 있는 직접 보고라인에서 나온다.

[그림 5] COSO와 2차 방어선

3차 방어선: 내부감사

내부감사조직은 3차 방어선으로 조직에 기여한다. IIA는 내부감사를 "조직에 가치를 창출하고 조직의 운영을 개선하기 위해 고안된 독립적이고 객관적인 인증(assurance) 및 컨설팅 활동으로, 리스크 관리와 내부통제 및 거버넌스 프로세스의 효과성을 평가하고 개선할 수 있는 체계적인 접근방식을 통해 조직의 목표 달성을 지원한다."고 정의한다.

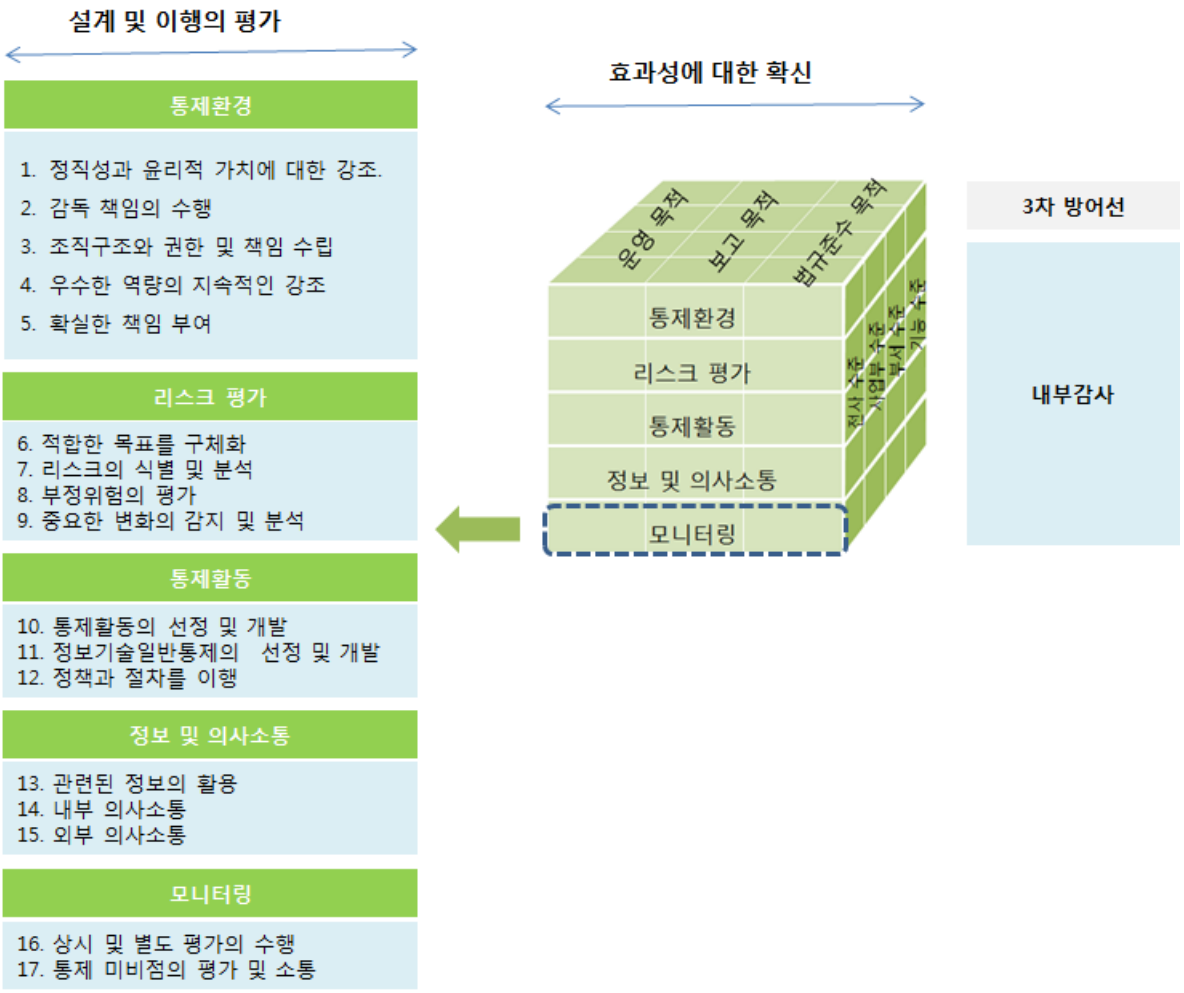
여러 역할들 중에서, 내부감사는 거버넌스, 리스크 관리 및 내부통제의 효율성과 효과성에 관한

확신을 제공한다. 내부감사 업무의 범위는 조직 운영 및 활동에 관한 모든 분야를 포괄한다.

내부감사의 높은 조직적 독립성과 객관성은 1차 및 2차 방어선과 구분되는 특성이다. 내부통제를 설계하거나 이행하는 것은 내부감사의 일상적인 책임이 아니며, 내부감사는 조직의 운영에도 책임을 지지 않는다. 대부분의 조직에서 내부감사 독립성은 내부감사 책임자(CAE; Chief Audit Executive)와 이사회간의 직통 보고 관계를 통해 훨씬 강화된다. 이러한 높은 조직적 독립성 때문에, 내부감사는 거버넌스와 리스크 그리고 내부통제와 관련하여 신뢰할 수 있고 객관적인 확신을 이사회와 경영진에게 제공할 수 있는 최적의 위치에 있다.

독립성과 전문성을 제고할 수 있는 특정한 조건들이 충족되면 내부감사 활동은 조직의 효과적인 거버넌스체계에 활발하게 기여한다. 따라서 전문적인 내부감사 활동을 설립하는 것은 모든 조직에서 우선순위가 되어야 하며, 이는 대규모 조직뿐 아니라 작은 조직에서도 중요하다. 거버넌스와 리스크 관리 프로세스의 효과성을 확인하는데 상대적으로 덜 공식적이거나 상대적으로 활동이 왕성하지 않은 조직구조를 갖추었거나, 효과적인 2차 방어선을 갖추지 못한 소규모 조직도 대기업과 동일하게 복잡한 환경에 직면할 수도 있다. 모든 조직은 독립적이고 유능한 내부감사부서를 설립하고 유지하여야 하고, 내부감사의 직무를 독립적으로 수행할 수 있도록 조직 내에서 충분히 높은 위치에 있는 경영진에 보고하며, IIA의 International Standards for the Professional Practice of Internal Auditing과 같은 글로벌로 인정되는 업무수행기준에 따라 운영되어야 한다.

[그림 6] COSO와 3차 방어선



외부 감사인, 감독기관 기타 외부 기관

외부 기관은 조직 내 3차 방어선의 일부분으로 공식적으로 고려되지는 않지만, 외부감사인이나 규제기관은 조직의 전반적인 거버넌스와 통제구조와 관련하여 중요한 역할을 하기도 한다. 감독기관은 거버넌스와 통제를 강화하기 위한 요구사항을 설정하고 해당 기관들이 이를 준수하는지를 활발하게 검토하고 그 결과를 보고한다. 이와 유사하게 외부 감사인들은 조직의 재무보고에 대한 내부통제와 관련된 리스크에 대해 중요한 발견사항과 평가결과를 제시할 수도 있다.

외부 감사인과 규제기관, 기타 조직 외부의 그룹들을 효과적으로 조율하면, 이사회나 경영진 등 조직의 이해관계자들에게 중요한 시각과 발견사항을 제공하는 추가적인 방어선의 역할을 할 수도 있다. 하지만, 이러한 그룹들의 결과물은 목적이 다르거나 좁은 영역에 집중하는 특성이 있어서 조직의 내부 방어선에서 평가한 것보다 그 범위가 제한적일 수 있다.

예를 들면, 3단계 방어선이 조직이 직면하고 있는 운영, 보고 및 법규준수의 모든 영역을 다루는 반면에 외부기관에 의한 감사는 특정한 영역의 법규준수, 안전, 기타 매우 제한적인 영역에

국한될 수 있다. 리스크를 관리하는 것은 외부 기관이 아닌 조직의 책임이기 때문에, 외부감사인이나 규제기관이 가치 있는 정보를 제공하더라도 이들을 방어선을 대체하는 것으로 고려해서는 안 된다.

II. 3차 방어선의 구조화와 협업

3차 방어선의 구조화

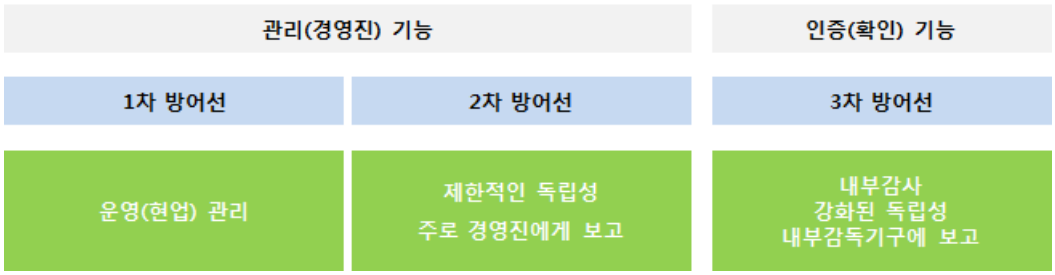
3차 방어선 모형은 의도적으로 유연하게 제작되었다. 각 조직이 속한 산업, 규모, 운영 구조, 리스크 관리에 대한 접근방법 등에 적합한 모형을 적용하여야 한다. 그러나, 전반적인 거버넌스와 통제환경은 3가지 방어선이 명확하게 분리되어 있을 때 가장 강력하게 작동할 수 있다. 조직은 그 규모나 복잡성과 관계없이, 세 가지 방어선이 어떤 형태로건 존재하도록, 3차 방어선 모형과 일치하는 거버넌스 구조를 시행하도록 노력하여야 한다. 이 "방어선"은 분리된 역할과 책임을 통해 구분되고, 조직의 적절한 정책과 절차에 명확하게 정의되어야 하며, 경영진의 일관된 메시지("tone at the top")를 통해 실행되어야 한다.

각 방어선간의 경계를 정확히 어디에 그어야 할 지는 각 조직의 특정한 필요성에 따라 다양할 수 있다. 일부 소규모 혹은 각 방어선 기능을 준비 중에 있는 조직에서는 각 방어선이 명확하게 구분되지 않을 수 있다. 예를 들어 리스크 관리 기능을 처음으로 시작할 때, 일부 조직에서는 이행을 위한 촉매제로 다른 기능을 활용할 수도 있다. 그러나 각 방어선의 기능들이 확실하게 구분되어 있지 않은 상황에서는 이사회는 조직의 잠재적인 영향에 대해 주의 깊게 고려하여야 한다. 방어선이 뚜렷이 구분되지 않은 이러한 상황들은 가능한 단기간에 해소되어야 하며, 방어선 기능들이 성숙함에 따라 적절한 분리가 이루어져야 한다. 짧은 기간이나 일시적인 현상이 아닌 경우, 이사회는 3가지 방어선 중 관리와 인증(확신 제공) 기능이 분리되지 않는 상황이 조직에 어떠한 영향을 미치는 지를 이해하여야 한다.

조직의 다양한 리스크 관리와 통제 기능 사이의 특정한 직무를 배정하거나 조율할 때 3차 방어선 모형 내에서 각각의 그룹의 역할을 염두에 두는 것이 도움이 될 것이다.

조직적인 측면의 독립성과 객관성은 3차 방어선의 핵심적인 특징이기 때문에, 내부감사 기능을 2차 방어선의 어느 역할과 통합하는 경우에는 특별한 주의를 기울여야 한다. 이러한 경우 경영진과 이사회는 내부감사 기능의 조직적인 독립성과 객관성을 훼손하는 방향으로 기능이 통합되거나 협업하는 아니라는 것을 명확하게 하여야 한다. 내부감사인들은 일반적으로 감사하는 업무에 대한 관리 상의 책임을 부담하지 않아야 하며, 내부감사가 2차 방어선의 활동에 참여하는 조직에서는 상충될 수 있는 역할을 서로 다른 개인이나 그룹에 할당하고, 이러한 상황을 단기간에 해소하여야 한다. 내부감사가 2차 방어선 활동에 참여하는 것이 단기간에 해소되지 않는 경우 경영진과 이사회는 내부감사가 독립성이고 객관적인 확신을 제공하는데 제한이 있다는 것을 인식하여야 하고, 특정한 활동에 대한 확신을 제공받기 위해 외부 기관을 활용하는 것을 고려할 수도 있다.

[그림 7] 각 방어선간의 차이



세 가지 방어선 간의 협업

3차 방어선 모형의 각 방어선들은 "효과적인 리스크 관리를 통해 조직의 목표 달성을 지원한다"는 궁극적으로 동일한 목표를 가지고 있다. 각 방어선은 궁극적으로 동일한 이해관계자를 위해 일하며, 동일한 리스크와 통제 이슈들을 다루는 경우도 있다. 경영진과 이사회는 세 가지 방어선이 상호간에 정보를 공유하고 활동을 조율하여야 한다는 요구사항과 함께, 이는 조직 전반에 걸쳐 효과적인 리스크 관리를 가능케 하려는 것이지 특정한 기능을 제거하려는 것이 아니라는 것을 명확하게 전달하여야 한다. 이를 위해 많은 조직들은 이러한 기대사항을 이사회 혹은 경영진 차원의 리스크 규정에 명시하고 있다.

협력과 소통을 조직구조와 혼동하여서는 안 된다. 각 방어선들이 동일한 목적을 가지고 있지만 각자의 고유한 역할과 책임이 있다. 각 방어선은 분리되어 있지만 따로 작업해서는 안 된다. 정보를 공유하고 리스크, 내부통제 및 거버넌스와 관련한 제반 노력들을 조율하여야 한다. 많은 경우 리스크와 통제와 관련하여 서로 공감하는 관점이 있을 수 있다.

중요한 리스크를 누락하지 않으면서 불필요하게 중복된 노력을 투입하지 않기 위해서는 각 방어선간의 협업이 필수적이다. 이러한 협업이 매우 중요하기 때문에 IIA Professional Standard 2050에서는 감사책임자(CAE)가 "조직 내·외부에서 확신이나 컨설팅 서비스를 제공하는 조직과 정보를 공유하고 업무를 조율하여야 한다"고 구체적으로 명시하고 있다.

이러한 협업이 작동하기 위해서는 Chief Risk Officer, Chief Compliance Office, Chief Audit Executive 등 경영진의 중요한 역할이 충분히 검토되고 조직화되어 리스크나 통제를 담당하는 다른 경영진과 협력하고 소통하면서 그들의 고유한 책임을 완수할 수 있도록 하는 것이 매우 중요하다.

1차 방어선은 리스크와 이러한 리스크의 관리방법에 대해 주된 책임을 진다. 2차 방어선은 리스크에 대한 전문성을 제공하고 이행전략의 수립과 정책과 절차의 실행을 지원하는 역할을 맡는다. 이 두 방어선이 리스크와 통제에 대해 담당하는 책임은 서로 다르지만, 이들이 동일한 용어를 사용하면서 협업하고, 조직의 리스크에 대한 각자의 평가결과를 이해하며 공통의 기법과 프로세스를 활용하는 것이 매우 중요하다.

조직의 3차 방어선인 내부감사 기능은 조직 내 중요한 리스크 및 통제활동을 모두 업무범위에 포함하여야 한다. 1차 및 2차 방어선과의 소통을 통해 내부감사는 리스크에 대해 유사한 용어를 사용하고 이 두 방어선이 리스크에 대한 이해하는 바를 이해할 수 있다.

내부감사는 2차 방어선과 적극적으로 협업하여야 한다. 이러한 협업은 조직의 특성이나 각 당사자가 수행하는 고유한 업무, 2차 방어선의 조직적 독립성, 경영진과 이사회의 기대수준 등에 따라 다양한 형태로 이루어질 수 있다. 내부감사 업무의 일정 부분을 2차 방어선이 수행한 업무를 바탕으로 수행하는 경우도 있다. 이러한 경우 내부감사는 해당 업무가 적절히 설계되고 계획되고 감독되고 문서화되고 평가되었는지를 확인하여야 한다. 내부감사가 다른 기능에서 수행한 업무를 활용하거나 의존하는 정도는 상황에 따라 다양할 수 있다. 또한 내부감사는 활용 혹은 의존하고자 하는 업무를 수행한 2차 방어선 기능의 조직적 독립성도 신중하게 고려하여야 한다. 내부감사가 공정하고 객관적인 평가를 수행하기 위해 조직적 독립성을 갖춘 형태로 구성되어 있기 때문에 내부감사가 활용 혹은 의존하고자 계획하는 업무를 수행한 기능 또한 충분히 높은 수준의 독립성과 객관성을 확보하고 있어야 한다. 역량과 효율성만이 전부가 아니다. 1차 및 2차 방어선이 일부 내부감사 업무를 수행할 수 있는 역량을 보유하고 있다고 해서 내부감사로서 필요한 수준의 독립성과 객관성을 가지고 있다는 것을 의미하지는 않는다. 마찬가지로, 내부감사가 1차 및 2차 방어선의 업무를 수행할 역량을 보유하고 있다고 해서, 이러한 업무를 수행하는 내부감사가 내부감사의 조직적 독립성과 객관성을 유지하고 있다는 것을 의미하지는 않는다.

내부감사헌장에서 내부감사가 다른 2차 방어선 기능 혹은 제 3자가 제공한 업무의 성과와 효과성을 평가할 책임이 있다는 것을 명기함으로써, 보다 효율적인 협업을 가능하게 할 수 있다.

조직 내 3차 방어선의 범위를 넘어서서 외부 감사인 같은 외부 단체까지 확대하여 협업을 진행할 수 있다. 외부기관이 수행한 업무, 세부 결과, 독립성과 전문성을 충분히 이해하고 있다면, 내부감사는 거버넌스와 리스크 관리 및 통제에 대한 확신을 제공하는 데 있어 조직 내부 혹은 외부의 다른 기관이 수행한 업무에 의존하거나 활용할 수 있다. 반대로, 외부 기관의 요구사항을 충족하도록 내부감사 업무를 계획하고 실행할 수도 있다. 외부 기관과 협업하는 것은 효율성을 증대시킬 수 있으나 CAE 와 이사회는 이에 따른 비용까지도 고려하여야 한다.

III. 3차 방어선 전반에 COSO를 활용하기

COSO 프레임워크는 내부통제의 5가지 요소(component)와 이 요소와 관련된 기본적인 개념을 설명하는 17가지 원칙(principle)을 정의한다. COSO의 *Internal Control – Integrated Framework* 에서는 17가지 원칙을 내부통제의 5가지 요소로부터 직접 추출하였기 때문에, 각각의 원칙을 적용함으로써 효과적인 내부통제를 달성할 수 있다고 말한다. 경영진은 17가지 원칙과 관련된 필수적인 직무를 배정하고, 이러한 의무가 의도된 대로 수행되는지를 확인할 책임이 있다.

17가지 원칙에 대한 책임을 3차 방어선간에 어떻게 배분할 수 있는지를 부록에서 예시하였다. *Internal Control – Integrated Framework* 은 또한 17가지 원칙과 관련된 다양한 "강조 사항(point of focus)"를 제시하고 있다. 많은 강조 사항들이 세 가지 방어선 내 개개인의 주요 책임을 나타내기 때문에 *Internal Control – Integrated Framework* 와 친숙한 독자는 많은 강조 사항들이 다음 장 전반에서 반영되었다는 것을 알 수 있을 것이다.

부록에서는 조직 내 직무를 세 가지 방어선에 할당하는 방법에 대한 예시를 제공하고자 했다.

모든 조직은 고유의 특성이 있기 때문에 조직들이 역할과 책임을 다르게 정한 것은 합당한 이유가 있을 것이다. 직무가 조직 내에서 어떻게 할당되는지 간에, 누락없이, 중복없이 리스크를 관리하기 위해서는 17가지 원칙과 관련된 특정한 역할과 책임이 명확하게 수립되어 모든 당사자에게 전달되어야 한다.

IV. 결론

모든 조직은 누락되는 통제와 불필요한 노력이 중복되는 것을 최소화하기 위해 거버넌스, 리스크 및 통제와 관련된 책임에 대해 명확히 정의해야 한다. 3차 방어선 모형은 필수적인 역할과 책임을 명확하게 정의함으로써 리스크와 통제에 대한 의사소통을 개선할 수 있는 효과적인 방법을 제공한다. 3차 방어선 모형은 리스크 및 통제와 관련된 책임을 조직 내에서 어떻게 조율할 것인지를 명확하게 하는 데에도 유용할 것이다.

이 모형의 기본 전제는, 효과적인 리스크 관리와 내부통제를 위해서는 경영진과 이사회의 감독과 지시 하에서 아래의 3가지 분리된 그룹(혹은 방어선)이 필요하다는 것이다.

- 리스크 및 통제에 대한 직접적인 책임과 관리 (현업)
- 경영진을 지원하여 리스크와 통제를 모니터링 (리스크, 통제, 준법감시 기능)
- 리스크 관리와 내부통제의 효과성에 대해 이사회와 고위 경영진에게 독립적인 확신을 제공 (내부감사)

3차 방어선 각각은 조직의 거버넌스 프레임워크 내에서 구분되는 역할을 가지며 각 방어선에서 맡은 역할을 효과적으로 수행할 때 중요한 통제가 실패할 가능성은 줄어든다. 이러한 구조를 통해 이사회는 조직의 가장 중요한 리스크에 대해, 그리고 경영진이 이러한 리스크에 어떻게 대응하고 있는지에 대한 공정한 정보를 제공받는 수 있다.

이 모형은 COSO의 *Internal Control – Integrated Framework*와 연계하여 사용함으로써, 각 방어선 내의 개인이 담당하고 있는 리스크와 통제에 대한 책임과, 그들의 책임이 조직의 전반적인 리스크와 통제구조에서 어떤 위치에 있는지를 완전하게 이해하는데 도움을 줄 수 있다.

핵심 사항

1. 경영진과 이사회는 거버넌스, 리스크 관리 및 통제 프로세스가 효율적, 효과적으로 작동하도록 하는 최종적인 책임을 가진다.
2. 리스크 관리는 세 가지 분리되고 명확하게 정의된 방어선이 구축되어 있을 때 가장 튼튼하다. 세 가지 방어선은 규모나 복잡성에 상관없이 모든 조직에서 특정한 형태로 존재하여야 한다.
3. 세 가지 방어선 내 각 그룹의 역할과 책임은 적절한 정책과 절차, 보고 체계를 통해 명확하게 정의되어야 한다.

4. 주요한 리스크를 모두 통제하면서 효율성을 증대시키고 중복된 노력을 회피하기 위해 각 방어선 간에 정보를 공유하고 협업하여야 한다.
5. 각 방어선이 통합되거나 협업할 때 효과성이 훼손되어서는 안 된다. 각 방어선은 조직 내에서 고유한 위상이 있고, 고유한 책임을 부담한다. 방어선간의 기능을 통합하는 경우에는 특별한 주의를 기울여야 한다. 방어선의 통합이 해당 방어선의 고유한 특성을 훼손한다면 2차 혹은 3차 방어선의 효과성에 부정적인 영향을 미칠 수 있다. 역량과 효율성만이 중요한 것이 아니며, 독립성과 객관성 또한 고려해야 할 핵심요소이다.

