pwc 삼일회계법인

Discovery of K-SOX Excellence

내부통제 미래전략 보고서

Volume 7.0

삼일PwC Risk Assurance Group

June 2026

Table of contents

들어가는 말

최근 기업 환경은 빠르게 변화하고 있다. 상법 개정으로 이사회의 책임이 한층 강화되고, 내부통제에 대한 규제가 확대되고 있는 가운데, AI 확산과 사이버 보안 위협까지 동시에 다가오고 있다. 이제 기업들은 기존 규제를 준수하는 것을 넘어, 새로운 리스크까지 선제적으로 관리해야 하는 시점에 놓여 있다.

이러한 변화 속에서 내부통제는 더 이상 '규제 대응 수단'에 머무르지 않고, 기업의 리스크를 선제적으로 식별하고 관리하는 '경영 인프라'로 자리매김하고 있다. 특히, 전사 리스크 관리체계의 중요성이 확대되며 재무보고 중심의 내부회계관리제도를 넘어 운영 및 컴플라이언스 영역까지 통합하는 접근이 요구되고 있다. 더불어 사이버 보안, 데이터 관리, AI 거버넌스 등 새로운 리스크 영역이 등장함에 따라 내부통제의 범위와 역할 또한 지속적으로 확대되고 있다.

본 보고서는 이러한 환경 변화에 대응하여 국내 기업의 내부회계관리제도 운영 현황과 주요 이슈를 분석하고, 사이버 보안, 전사 리스크 관리, AI 거버넌스 등 핵심 영역별 시사점을 제시하고자 한다. 이번 보고서가 기업들이 미래 환경에 대응할 수 있는 내부통제 및 거버넌스 전략을 구체적으로 수립하는 데 실질적인 도움이 되길 기대한다.

01

내부회계관리제도 트렌드

- 내부회계관리제도 트렌드 서베이 개요
- 내부회계관리제도 운영 현황
- 2조 원 이상 회사의 연결내부회계관리제도 현황
- 부정 위험 대응 현황
- 신규 규제 환경 인식 현황
- 2025년 자금통제 공시 분석 및 시사점

내부회계관리제도 트렌드 서베이 개요

서베이 목적

- 국내 기업의 내부회계관리제도 주요 운영 현황 분석

서베이 내용

- 내부회계관리제도 운영의 세부 항목별 실태 조사

서베이 항목

- 운영 / 연결 / 부정 / 신규 규제

전체응답자 수

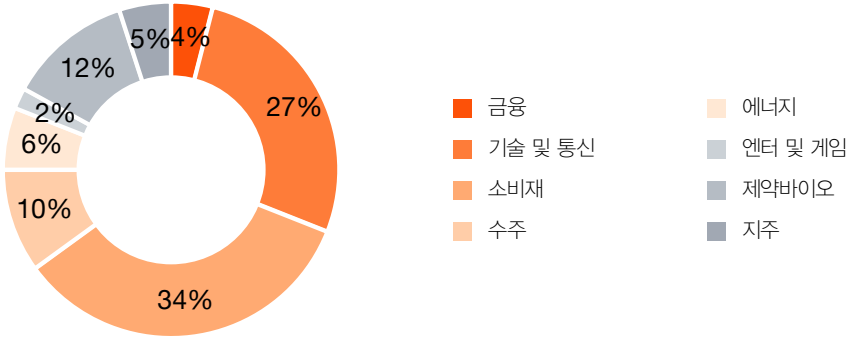
- 464개사

분석 대상 회사 산업별 및 총자산 규모별 현황 (단위: 개수)

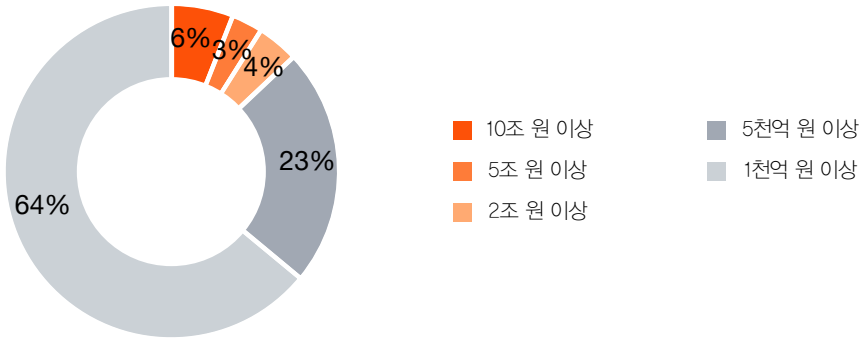
구분	10조 원 이상	5조 원 이상	2조 원 이상	5천억 원 이상	1천억 원 이상	총 합계
기술 및 통신	4	2	2	24	100	132
금융	10	1	–	1	6	18
소비재	8	5	10	43	107	173
수주	4	2	2	10	29	47
에너지	3	2	3	9	12	29
엔터 및 게임	–	–	1	4	7	12
제약바이오	–	–	1	11	45	57
지주	2	1	3	9	11	26
총 합계	**31**	**13**	**22**	**111**	**317**	**494**

분석 대상 회사 산업별 및 총자산 규모별 현황 (단위: 개수)

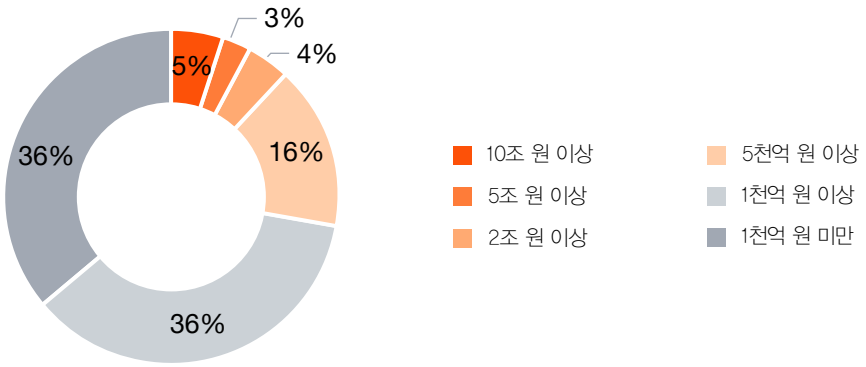
산업별 비율



총자산 규모별 비율



매출액 규모별 비율



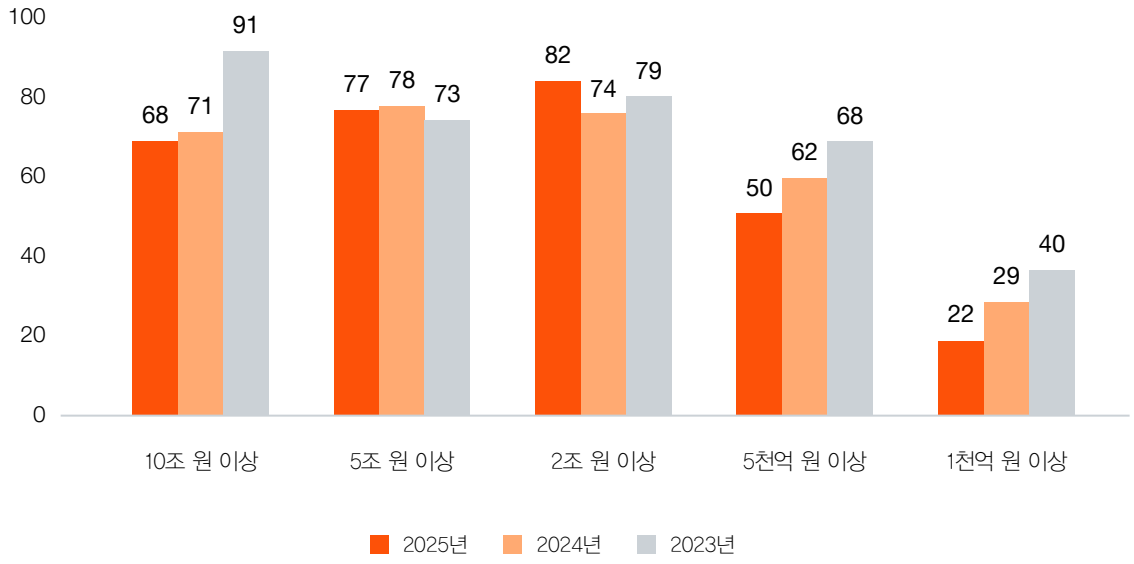
분석 대상 회사의 산업별 비율은 소비재 산업이 약 34%로 가장 높고, 기술 및 통신(27%), 제약바이오(12%) 순이다. 총자산 규모별로는 1천억 원 이상 회사가 약 64%로 가장 큰 비중을 차지하며, 5천억 원 이상 회사가 약 23%, 2조 원 이상 회사(10조/5조/2조 합산)가 약 13%를 차지한다. 매출액 규모별 분포도 총자산 규모와 유사한 분포를 보이며, 매출액 1천억 원 미만 회사도 일부 포함되어 있어 매출액과 자산규모간 직접적인 상관관계가 회사별로 상이한 결과를 나타낸다.

이러한 구성은 한국상장사협의회 및 코스닥협회 회원사 중 내부회계관리제도 적용 대상이 되는 다양한 규모 및 산업의 기업이 폭넓게 참여하였음을 보여 주며, 분석 결과의 대표성 및 시사점이 국내 상장사 전반에 적용될 수 있는 수준임을 의미한다.

내부회계관리제도 운영 현황

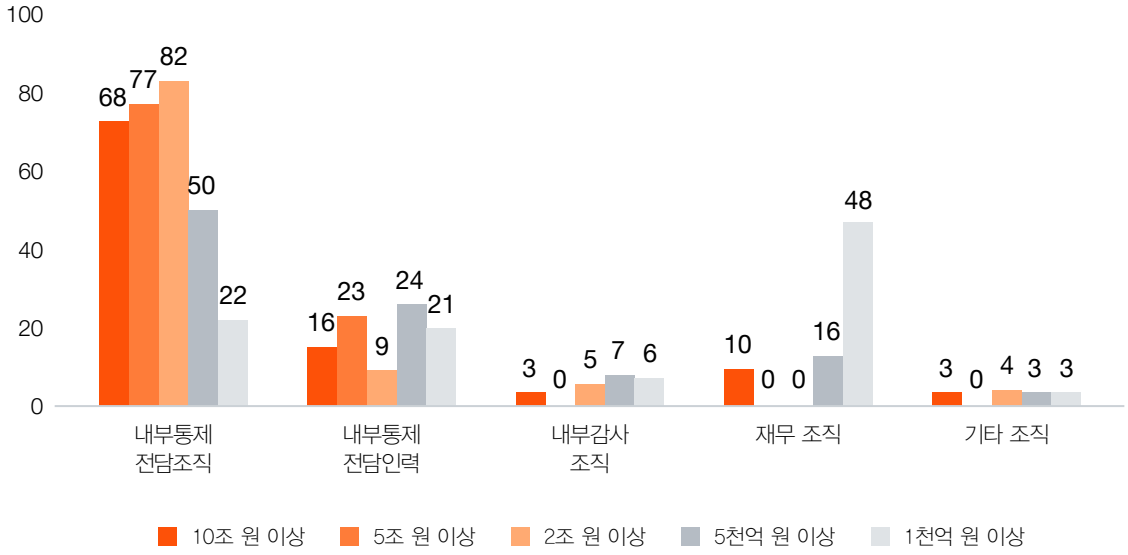
1. 내부회계관리제도 전담조직

도표 1. **자산규모별 내부회계관리제도 전담조직** (단위: %)



조사대상회사 수	10조 원 이상	5조 원 이상	2조 원 이상	5천억 원 이상	1천억 원 이상	합계
2025년	31	13	22	111	317	494
2024년	28	18	34	115	191	386
2023년	23	11	29	78	154	295

도표 2. **자산규모별 회사 내부회계관리제도 전담조직** (단위: %)



2025년의 경우 과거 조사 대비 2조 원 ~ 10조 원 규모에서는 10조 원 이상 법인에서 23년 이후 전담조직의 감소가 20%가량 발생하였으나 24년부터는 안정적이며, 전반적으로 약 70% 이상의 회사가 전담조직을 운영하고 있다. 한편 1천억 원의 경우 전담조직 비율이 22% 수준이며, 전기대비 조사대상회사가 60% 정도 증가한 점을 고려하더라도 뚜렷하게 감소하고 있는 상황이다.

자산규모별 운영 주도 조직을 분석한 결과, 2조 원 ~10 조 원 이상 회사는 최소 84% 이상이 내부통제 전담인력 또는 전담조직을 통해 내부회계관리제도를 운영하고 있어 안정적인 패턴을 유지하고 있다. 반면 5천억 원 이상 및 1천억 원 이상 회사 그룹은 내부통제 전담인력 또는 전담조직의 비율이 각각 74% 및 약 43% 수준에 그치고 있어 자산규모에 따른 운영 주도 조직의 격차가 명확히 드러난다.

2029년부터 연결내부회계관리제도 감사가 확대 적용되는 5천억 원 이상 2조 원 미만 회사의 경우 그룹 현황과 내부통제 전담조직 및 전담인력 등의 상황 등을 고려하여 내부통제 전담조직의 확충 등을 사전적으로 고려할 필요가 있다.

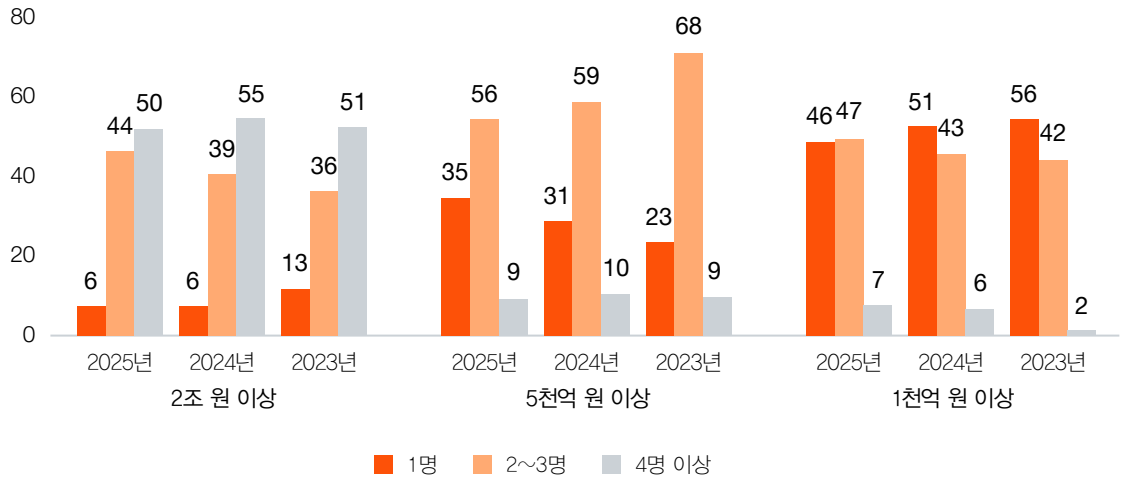
2. 내부회계관리제도 전담인력 규모 및 충분성

내부회계관리제도 전담인력의 적정 규모는 회사의 인력 현황, 외부 자문 활용여부 및 운영 방식 등 다양한 요소가 고려될 수 있다.

2조 이상 회사의 경우, 대부분 2~6명 정도의 인력으로 내부회계관리제도 담당 인력이 운영되고, 5천억 이상 및 1천억 이상 회사는 대부분 1~3명의 인력으로 운영되고 있는 것으로 확인됐다.

참고로 동 인력은 사업보고서에 공시되는 내부회계관리제도 관련 인력과는 달리, 내부회계관리제도 담당 팀이나 지정 인력의 규모를 확인한 결과이다.

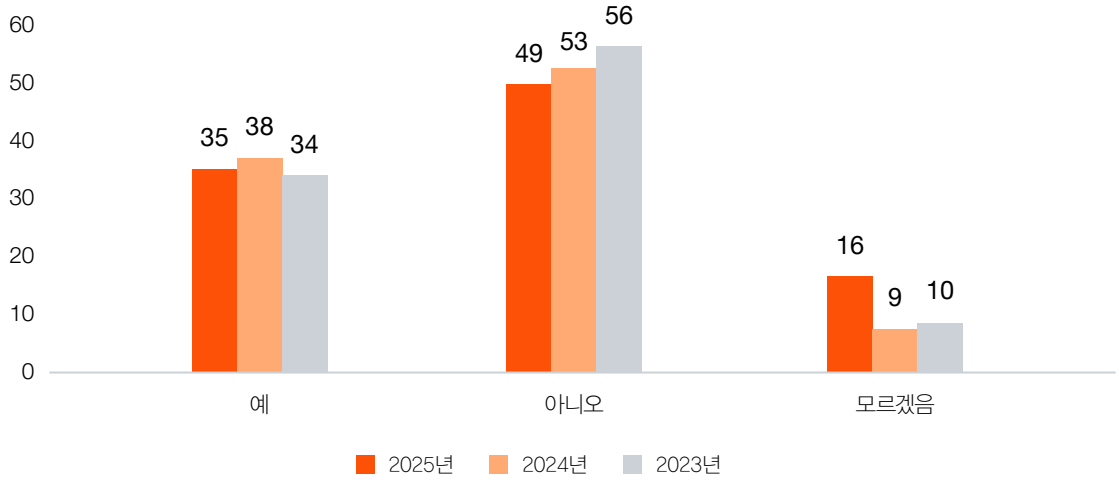
도표 3. **자산규모별 내부회계관리제도 전담인력 규모 현황** (단위: %)



자산규모별 전담인력 규모를 분석한 결과, 2조 원 이상 회사는 4명 이상이 약 50%로 비교적 풍부한 인력 구성을 유지하고 있으며, 5천억 원 이상 회사는 2~3명이 약 56%, 1천억 원 이상 회사는 1명이 약 46%로 회사 규모가 작을수록 담당 인력의 수가 부족하다는 점을 의미한다.

최근 3개년 비교 또한 자산규모별 차이를 뚜렷하게 보여준다. 2조 이상의 경우 1명인 경우가 13% → 6%로 감소하였지만, 5천억 이상의 경우 23% → 35%로 증가, 1천억 이상의 경우는 56% → 46%로 감소하였지만 과거 50% 이상이 1명이었다는 점에서 자산규모 별 인원 수는 정확히 반비례하고 있다.

도표 4. **자산규모별 내부회계관리제도 전담인력의 충분성** (단위: %)

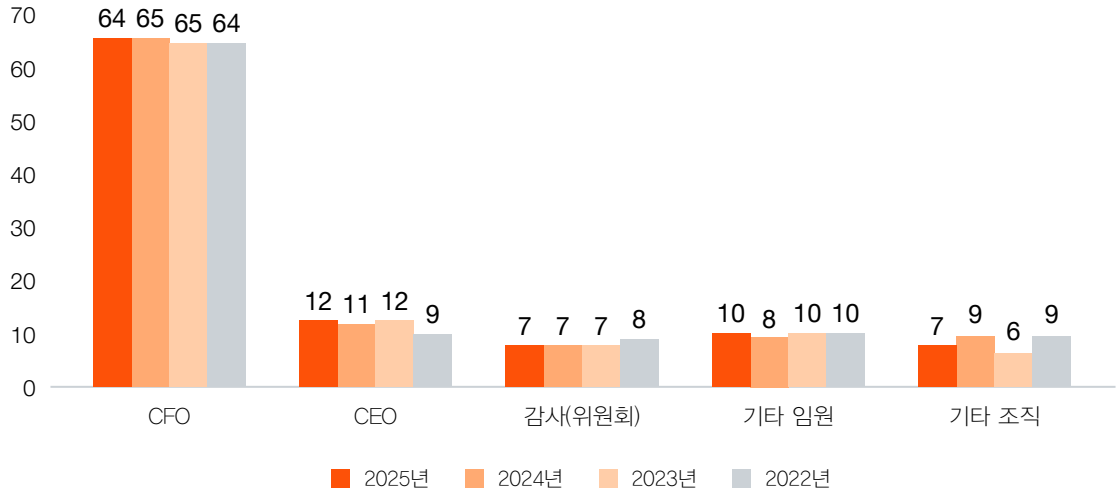


내부회계관리제도 전담인력 수의 충분성에 대하여 응답 회사의 약 49%가 '불충분하다'고 응답하였다. 이는 전년(53%)에 비해 소폭 감소하였으나, 여전히 절반에 가까운 비율이 인력 부족을 인식하고 있어 구조적 문제가 해소되지 않고 있음을 보여 준다.

특히 별도 자산총액 5천억 원 이상 2조 원 미만 회사의 경우 2029년부터 연결내부회계관리제도 감사 대상이 될 예정이어서 내부통제 전담조직을 포함한 전담인력의 수의 충분성에 대해 사전적으로 고려가 필요하다. 특히 최근 급격히 기술이 진보하고 있는 AI의 활용계획도 전담인력 부족 현상을 보완할 수 있는 좋은 대안으로 여겨진다. AI를 활용하는 것이 반드시 AI 인프라를 구축 해야함을 의미하지는 않는다. AI를 일시적 또는 정기적으로 활용한 외주 서비스의 이용도 고려할 수 있기 때문이다. 또한 최근 내부회계관리제도 법제화, 자금통제 공시 강화 등 신규 규제 환경 하에서 전담인력의 업무 부담은 더욱 가중되고 있어 인력 충원과 함께 시스템 활용, 외부자문사 활용, 업무 효율화 등 다각적인 접근이 필요한 시점이다.

3. 내부회계관리제도 담당 조직 편제

도표 5. **연도별 내부회계관리제도 담당 조직 편제** (단위: %)

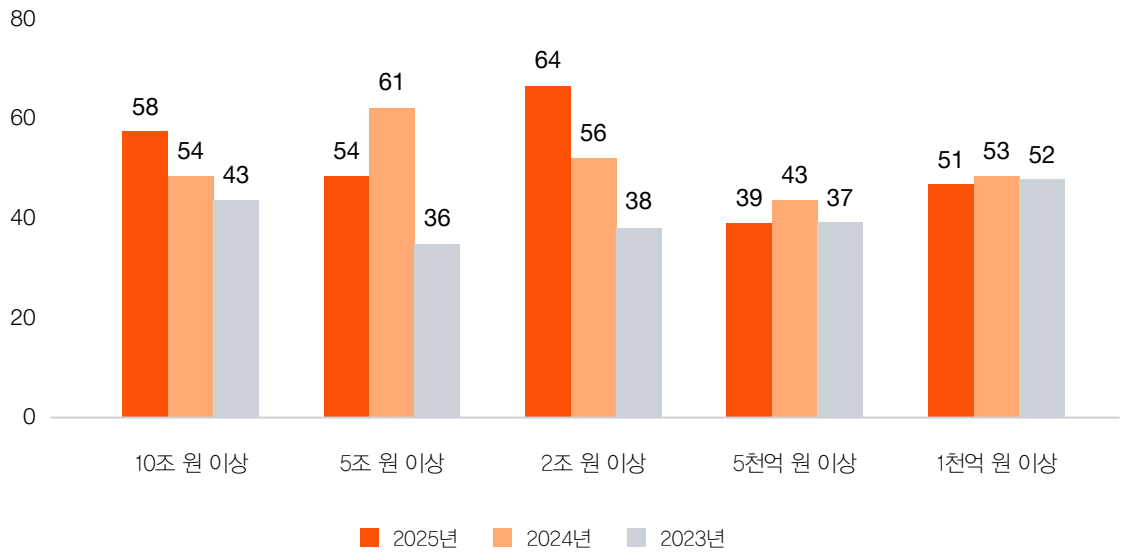


연도별 내부회계관리제도 담당 조직 편제는 최근 4개년 동안 CFO 비율이 약 64~65% 수준으로 일관되게 가장 높은 비중을 차지하고 있으며, 유의한 변화는 보이지 않는다.

CEO 비율은 약 9~12% 수준에서 등락을 보이고 있으며, 감사(위원회) 비율은 약 7~8%로 안정적이다. 향후 내부회계관리제도 평가에 대한 객관성에 대한 요구 및 상법 개정 등으로 감사위원회의 역할과 책임이 증가하고 있는 상황에서 감사(위원회) 또는 독립적 평가 조직의 비중이 점진적으로 증가할 가능성이 있다.

4. 내부회계관리제도 운영평가 수행 시 외부자문사 활용 현황

도표 6. **연도별 외부자문사 활용 현황** (단위: %)



구분	2025년	2024년	2023년	2022년	2021년	2020년	2019년
활용함	50	51	52	66	43	58	75

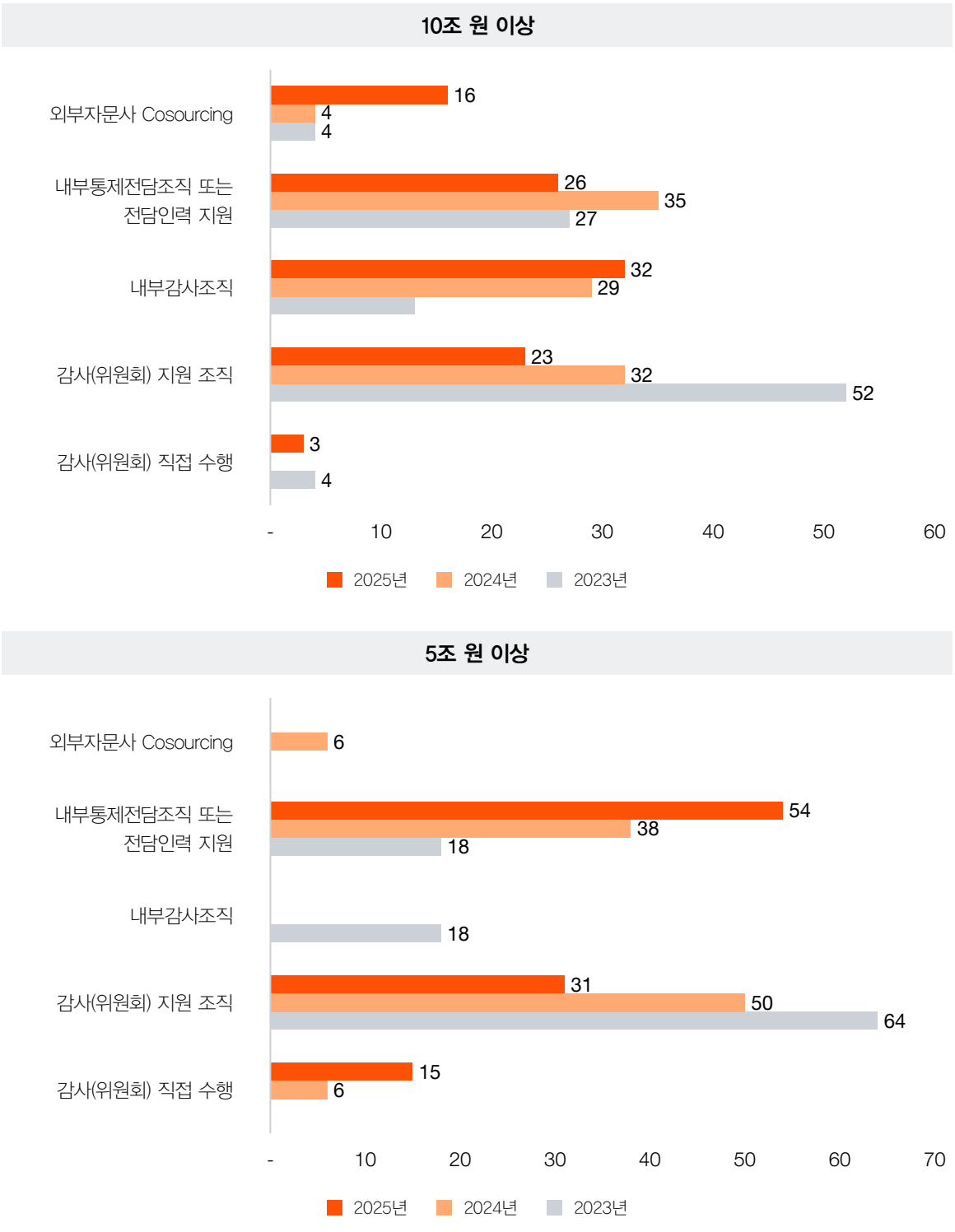
내부회계관리제도 운영평가 시 외부자문사를 활용한 회사 비율은 2025년 약 50% 수준으로 2024년(51%)과 유사한 수준을 유지하고 있다. 내부회계관리제도 감사가 처음 도입된 2019년 75%에서 점차 감소하다가 1천억 원 이상 상장회사에 감사가 적용된 2022년에 66%로 다시 증가한 이후 50%대에서 안정화되는 추세를 3년째 유지하고 있다.

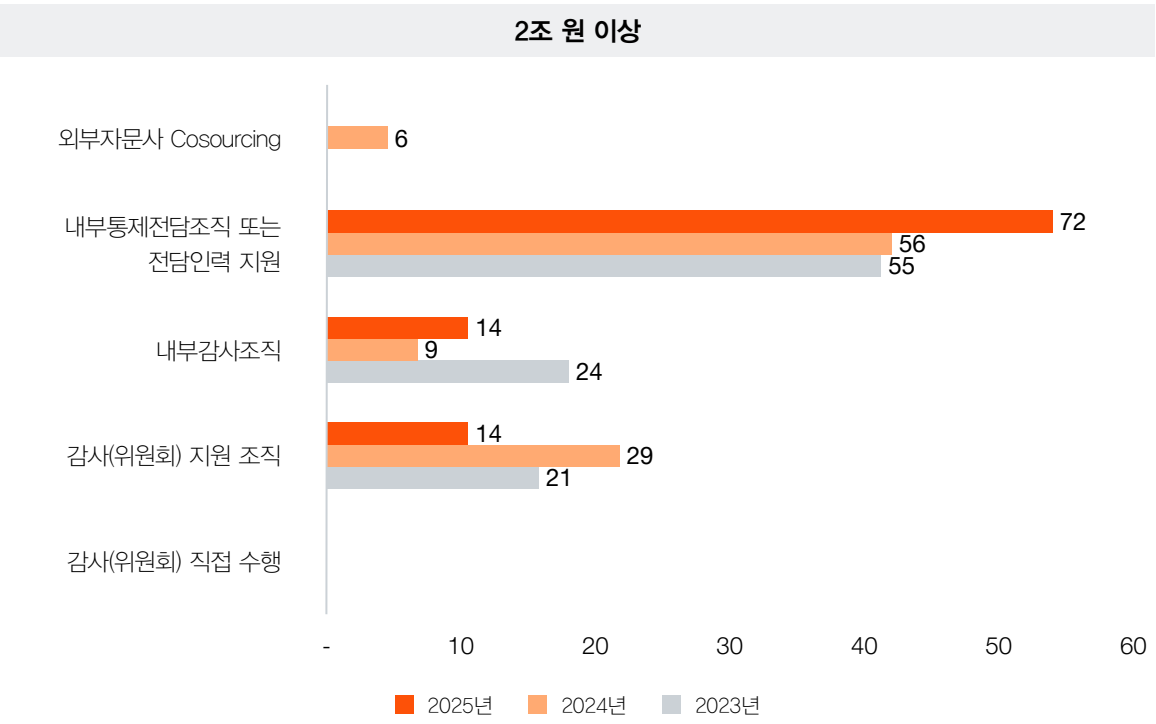
최근 3개년 각 자산규모 별로 검토 시 10조 원 이상, 2조 원이상 구간의 회사는 꾸준히 상승하고 있으며, 5천억 원 이상, 1천 원 이상 회사는 3년 동안 유사한 수치를 보이고 있다. 상대적으로 규모가 작을수록 활용비율이 낮은바, 이는 각 사의 재무현황 등의 요소가 작용하고 있다고 여겨진다.

내부회계관리제도 업무의 복잡성 증가, 회사 내부 자체 인력 부족 및 적시성 있는 외부감사인 대응 등의 사유로 외부자문사에 대한 수요가 일정 수준으로 유지되고 있음을 보여 준다. 특히, 최근 내부회계관리제도 법제화와 자금통제 공시 적용 등 강화된 규제 환경 하에서 전문적이고 독립적인 운영 및 평가 업무 수행을 위해 외부자문사 활용은 일정 수준으로 유지되거나 일부 영역에서 확대될 것으로 보인다.

5. 감사위원회 평가 수행 지원 조직

도표 7. **2조 원 이상 상장 회사의 감사위원회 평가 수행 지원 조직** (단위: %)





10조 원 이상 회사들의 경우 감사위원회 지원조직의 비율이 꾸준히 하락하고 이를 내부감사조직과 외부 자문사로 대체되고 있는 움직임이 뚜렷하다. 이는 최근 내부회계관리제도 법제화 및 상법 개정 등으로 감사위원회의 역할과 책임이 증가하고 있는 상황에서, 감사위원회가 평가 지원 조직의 전문성과 객관성을 적극 고려하고 있는 결과로 보여진다.

5조 원 이상의 회사에서도 감사위원회 지원조직의 비율이 꾸준히 감소하고 내부통제전담조직 또는 전담인력이 이를 흡수하고 있다. 2조 원의 경우 내부통제전담조직 또는 전담인력 지원이 23년부터 55% 이상이며, 당기에는 72%로 증가하였다.

5조 원 이상 회사와 2조 원 이상 회사의 경우 내부통제전담조직 또는 전담인력 비중이 증가세를 보이는데 이는 감사위원회의 독립적인 평가를 위한 실질적인 운영에 있어 많은 애로사항이 존재할 것이다. 10조 원 이상의 회사와 마찬가지로 동일한 환경하에 놓인 만큼 점진적인 변화가 있을 것으로 예상된다.

6. 내부회계관리제도 운영상 애로 사항

표 1. **내부회계관리제도 연도별 운영상 애로 사항**

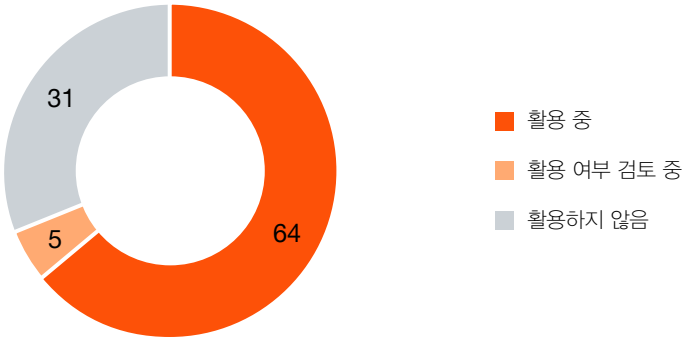
구분	2025년	2024년	2023년	2022년
경영진 지원 부족	1순위	3순위	1순위	3순위
재무보고 중요성 인식 부족	2순위	2순위	2순위	4순위
통제수행부서(현업)의 내부회계관리제도 책임과 역할 인식 부족	3순위	1순위	4순위	1순위
내부회계관리제도 전문인력 부족	4순위	4순위	3순위	2순위
내부회계관리제도 시스템(패키지) 미 활용	5순위	–	–	–

내부회계관리제도 운영상 애로 사항 분석 결과 2025년 1순위는 '경영진 지원 부족'이 차지하였다. 해당내역은 23년 1순위, 24년 3순위를 기록하였으며 매년 상위권에 위치하고 있다. 이는 내부회계관리제도 감사 도입이 7년이 경과한 시점에도 경영진의 의지(Tone at the Top)가 여전히 핵심애로사항으로 남아 있음을 보여준다. 2순위는 '재무보고 중요성 인식 부족'으로 이 또한 4년째 상위권을 차지하고 있으며 세부적인 회계정책 정립 및 실무 교육 기회 제공 등을 포함한 재무팀의 역량강화와 함께 재무보고 중요성에 대한 인식 제고 노력이 지속적으로 필요함을 보여준다.

3순위는 '현업의 내부회계관리제도 책임과 역할 인식 부족'이, 4순위는 '내부회계관리제도 전문인력부족'이 상위 애로 사항임이 확인된다. 특히 5순위 '내부회계관리제도 시스템 미활용은 당기 처음 상위권에 포함된 항목으로, AI 시대에 걸맞게 업무를 효율화하고 효과적으로 운영하고자 하는 회사 내부의 Needs가 점차 커지고 있음을 확인할 수 있다.

7. 내부회계관리제도(ICFR) 운영 및 평가 시 시스템(패키지) 활용 여부

도표 8. **내부회계관리제도(ICFR) 운영 및 평가 시 시스템(패키지) 활용 여부** (단위: %)



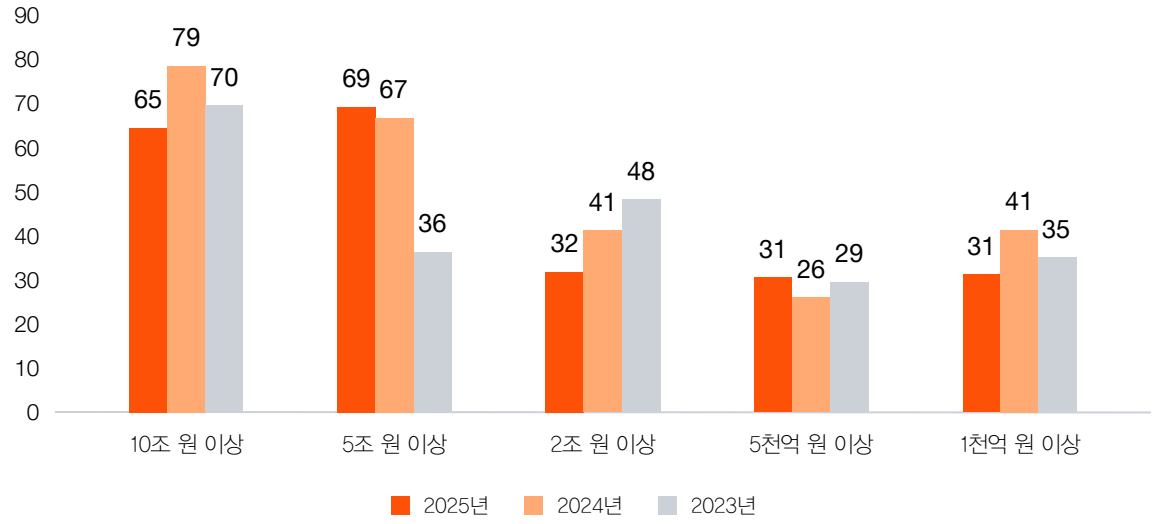
구분	2025년	2024년
활용 중	64	56
활용하지 않음	31	37
활용여부 검토 중	5	8

설문 결과, 내부회계관리제도(ICFR) 운영 및 평가에 시스템(패키지)을 활용하고 있는 회사 비율은 2025년 및 2024년 각각 약 64% 및 56%로 전기대비 8% 증가하였다. 회사들이 내부회계관리제도 업무의 효율성 제고, 외부감사인에 대한 적시성 있는 대응과 경영진의 적시성 있는 모니터링 등을 위해 내부회계관리제도 시스템(패키지)을 지속적으로 활용하고 있다는 것을 보여준다.

최근 10조 원 이상의 회사에서 AI를 활용한 내부회계관리제도 솔루션 구축을 적극적으로 검토하는 움직임이 있다. 25년 처음 시장에 AI 솔루션이 공개된 이후 점차적으로 대기업부터 전면적이 도입에 나서는 것으로 여겨진다. 향후 AI 기능을 포함한 Digital Tool 활용 요구가 더욱 높아지는 환경에서 시스템(패키지) 활용은 업무 효율화 및 적시성 있는 모니터링을 위해 적극적으로 고려되어야 할 사항이다.

8. In-scope IT 시스템 현황

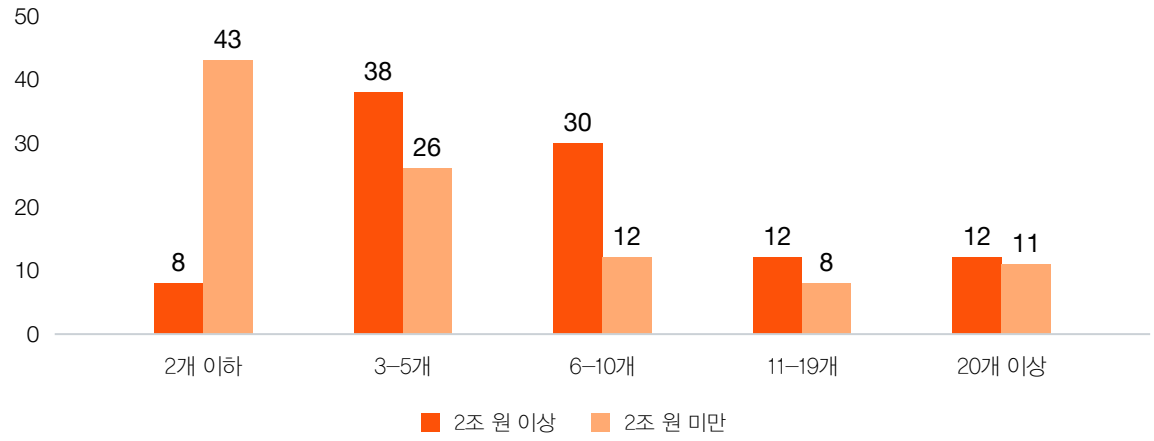
도표 9. **회사 규모별 In-scope IT 시스템 10개 초과 비율** (단위: %)



올해 분석 대상 회사의 In-scope IT 시스템 개수가 10개 이상인 경우를 조사하였다. 5조 원 이상 회사는 전기대비 유의적인 변동이 없는 반면, 10조 원 이상, 2조 원 이상, 1천억 원 이상 구간의 회사에서는 모두 9%~14% 수준의 유의적인 감소가 확인되었다.

자산 규모와 In-scope IT 시스템의 개수는 비례하는 것으로 파악되었으며, 특히 5조 원 이상, 10조 원 이상 구간의 대규모 기업의 경우 방대한 데이터 규모, 복잡성 및 다수의 사업부 등으로 인해 10개 이상의 In-scope시스템 비율이 각각 69%, 65% 이상을 보였다. 다수의 In-scope 시스템이 내부회계관리제도의 신뢰성을 대변하지는 않는다. ITGC In-scope과 자동통제의 평가 비용과 수기통제로 운영 시 발생하는 평가 비용의 효익비교, 그리고 평가의 신뢰성을 고려하여 신중하게 접근하는 것이 중요하다.

도표 10. **회사 규모별 In-Scope IT 시스템 개수 현황** (단위: %)

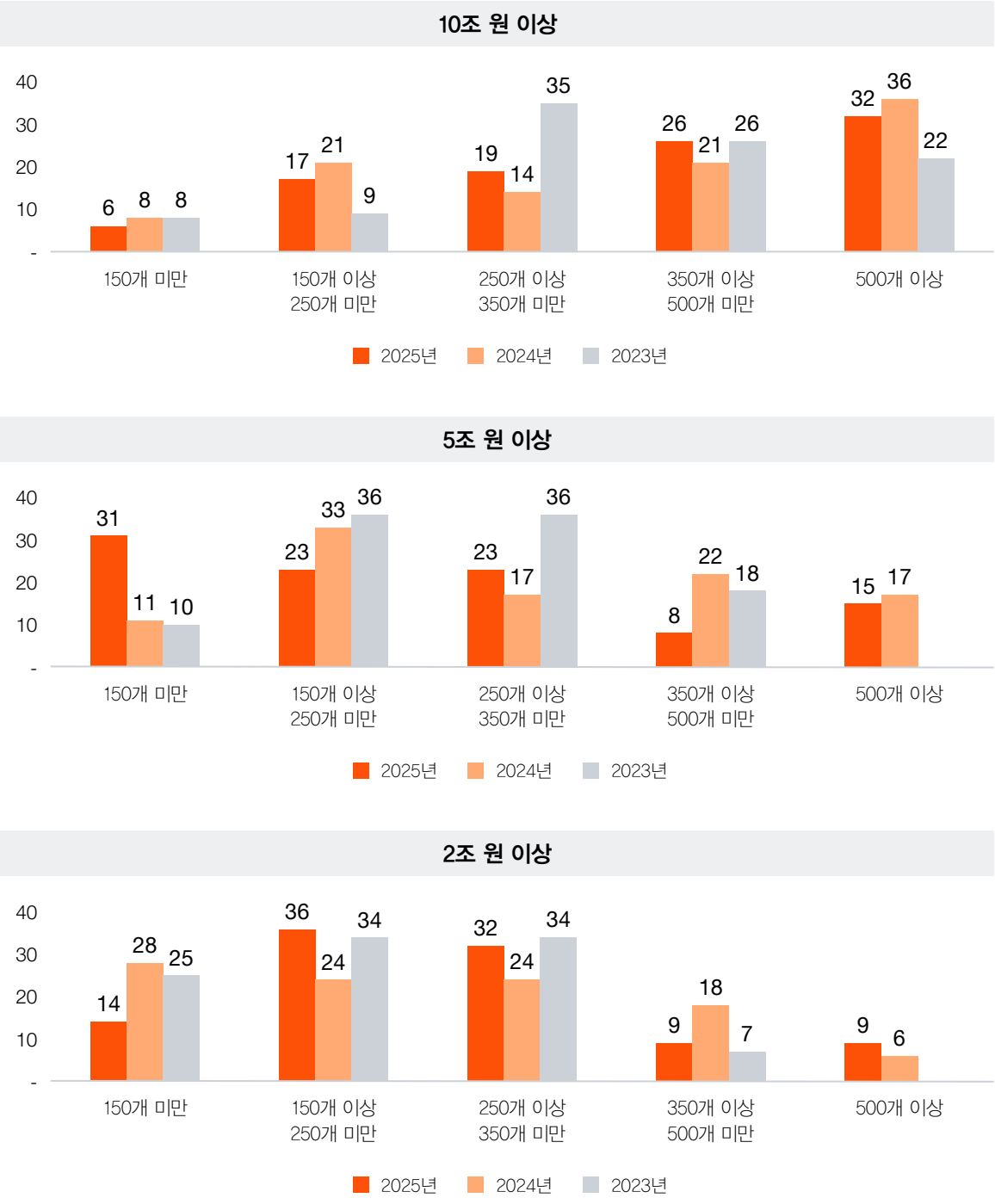


자산규모별 In-Scope IT 시스템 개수를 보면 2조 원 이상 회사의 경우 6개 이상의 시스템을 운영하는 비율이 약 54%로 2조 원 미만 회사(약 31%) 대비 현저히 높게 나타난다. 이는 회사의 규모가 클수록 사업의 복잡성, 다수의 ERP 운영, 데이터 분석 인프라 등에 의해 통제 대상 IT 시스템 수가 자연스럽게 증가하기 때문이다.

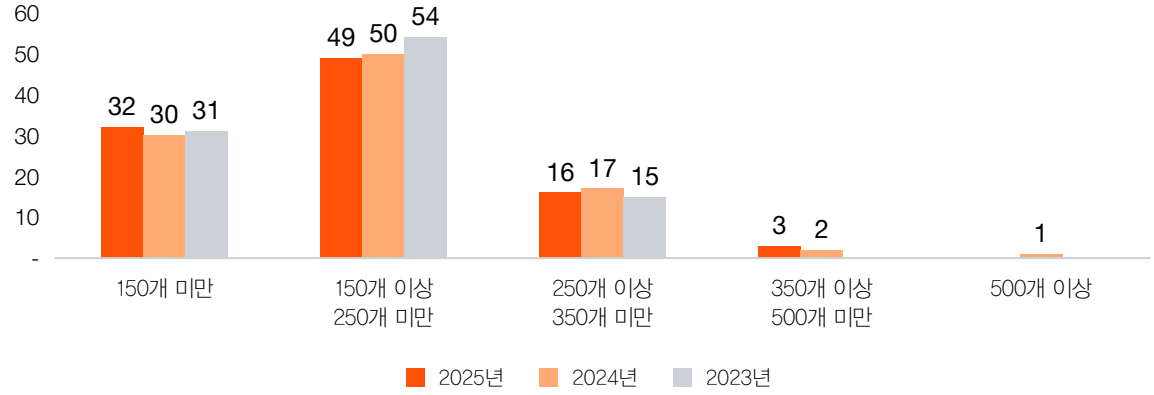
전년과 비교할 때 자산규모별 분포는 큰 변화가 없으며, 2조 원 미만 회사 그룹에서 2개 이하 보유 비율이 여전히 높아 시스템 통합·최적화 흐름이 지속되고 있는 것으로 보인다. 향후 AI 도입, 클라우드 전환 등 IT 환경 변화에 따라 In-Scope IT 시스템에 대한 변화관리 및 사이버 보안 통제활동의 점검 필요성이 더욱 커질 것으로 예상된다.

9. 거래수준 핵심통제활동 현황

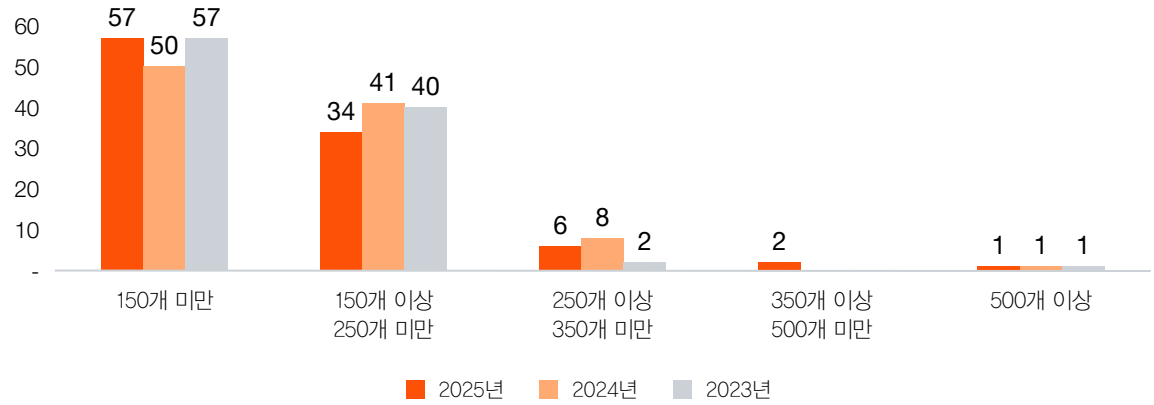
도표 11. **자산규모별 거래수준 핵심통제활동 현황** (단위: %)



5천억 원 이상



1천억 원 이상



회사 규모에 따라 거래수준 핵심통제활동의 개수는 뚜렷한 특징을 보이고 있다.

- 10조 원 이상 규모의 경우 250개 이후 구간에서 점진적인 증가가 파악된다.
- 5조 원 이상의 경우 150개 구간이 크게 증가하였다. 새로운 회사의 유입도 있을 수 있으나, 전반적으로 통제수의 축소의 움직임이 있다고 이해된다.
- 2조 원 이상의 경우 150개 이상 ~ 350개 미만 구간의 비율이 전기대비 증가하였으나, 23년과 비교시 유의적인 차이가 없다. 해당 2개 구간내에서 상대적으로 안정적인 추이를 보인다고 판단된다.
- 5천억 이상, 1천억 이상의 경우 250개 미만 2개 구간의 합이 모두 80%를 넘는다. 2조 원 이상 3개구간의 경우 각 사의 현황에 맞게 통제가 구축된다고 판단되는 반면, 5천억 이상, 1천억 이상 구간의 경우 전반적으로 적은 수의 통제를 운영하려는 유인이 강하게 작용하였다고 여겨진다.

한편 2조 원 이상의 회사 50%가 250개 미만의 통제활동을 운영 중이며, 10조 원 이상 회사도 6%가 150개 미만의 통제활동을 관리하고 있다. 회사의 실질적인 현황 및 복잡성 등을 고려하여 효율화 관점에서 통제활동의 최적화를 점검해 볼 필요가 있다.

10. 거래수준 자동통제활동 현황

도표 12. **거래수준 핵심통제의 자동통제가 30% 이상인 회사 비율** (단위: %)

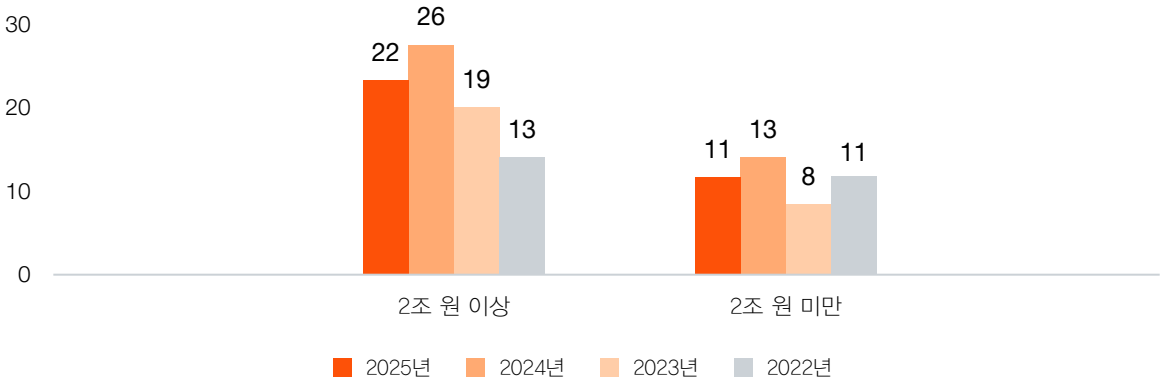
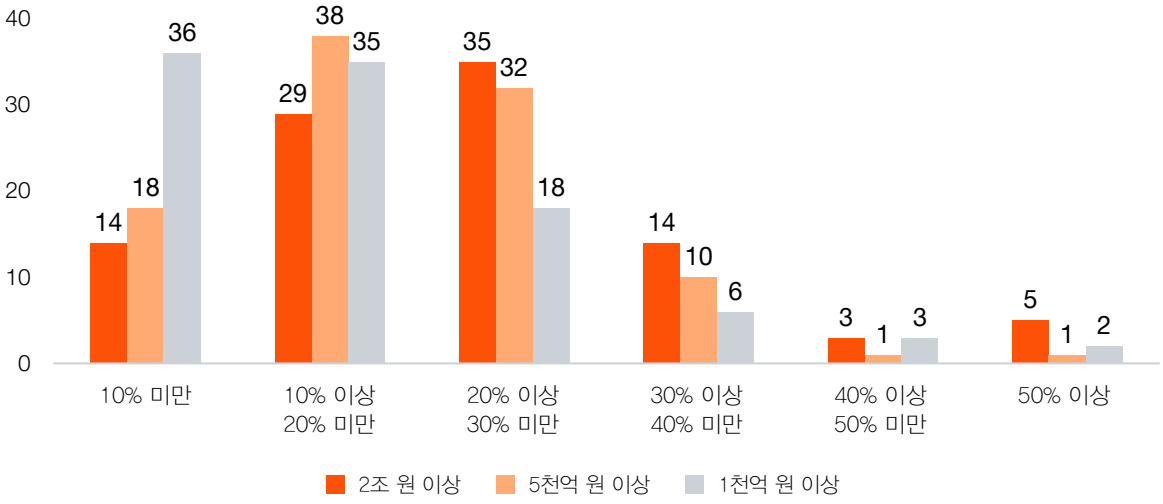


도표 13. **자산규모별 거래수준 핵심통제활동 중 자동통제 비율** (단위: %)



자산규모별 자동통제 비율 분포를 분석한 결과, 자동통제 10% 미만 비중이 1천억 원 이상 5천억 원 미만 회사에서 가장 높게 나타나는 반면, 2조 원 이상 회사는 20% 이상 구간의 비중이 가장 높게 나타난다.

이는 대규모 회사일수록 IT 시스템 기반의 자동화 투자가 지속적으로 이루어지고 있음을 보여 주며, 향후 AI 기반 통제활동 도입이 확산되면 자동통제 비율의 추가 상승이 예상된다. 최근 AI 및 Digital을 활용해서 자동통제를 포함한 내부통제 전반의 업무 효율화 및 고도화를 추진하는 회사들이 증가함에 따라 향후 점진적인 자동통제 비율의 확대가 예상된다.

11. MRC 항목 현황

도표 14. **연도별 MRC 핵심통제활동 개수** (단위: %)

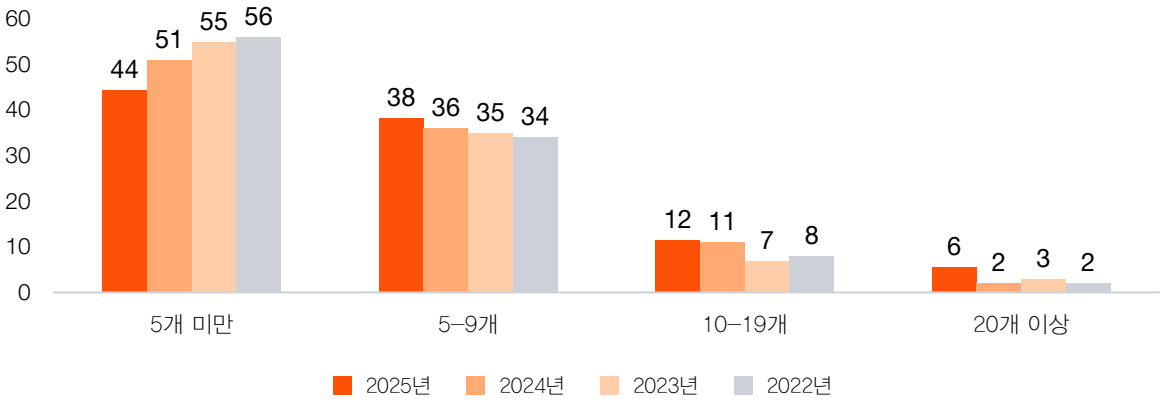
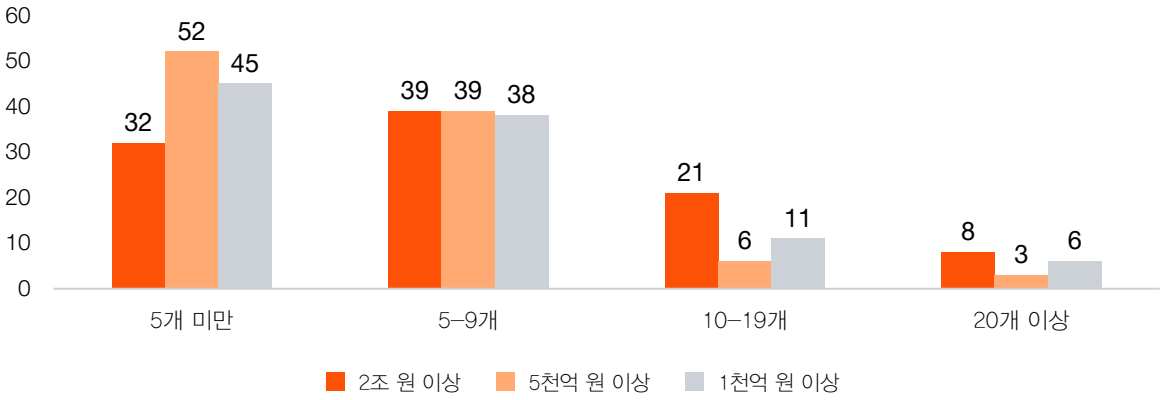


도표 15. **규모별 MRC 핵심통제활동 개수** (단위: %)



MRC(Management Review Control, 경영진 리뷰 통제)는 리스크 및 프로세스의 복잡성에 의존한다. 2조 원 이상의 경우 10개 이상으로 운영하는 비율이 약 30% 이며, 2조 미만의 경우는 동일 구간에서 20% 미만의 비율을 보여 주고 있다. 전체적으로 꾸준히 소폭이지만 MRC 통제 비율은 올라가고 있는 것으로 보여진다.

통제활동 수행 과정이 복잡하고 중요한 판단과 추정을 요구하는 통제활동을 의미하므로 실무적으로 회사의 재무 리스크 등을 고려하여 반드시 필요한 항목인지 여부에 대한 고민은 필요하다. MRC가 많고 적음으로 위험이 증가 혹은 경감되는 것은 아니며, 각각의 위험에 직접적으로 대응하는 통제를 고려하여 MRC를 최적화 할지를 고려할 필요가 있다. 특히 회사의 규모가 작은 경우 실질적으로 MRC를 운영할 수 있는 여건이 갖추어져 있는지 객관적인 판단이 요구된다.

12. IPE 항목 현황

도표 16. **규모별 IPE 대상 항목 개수** (단위: %)

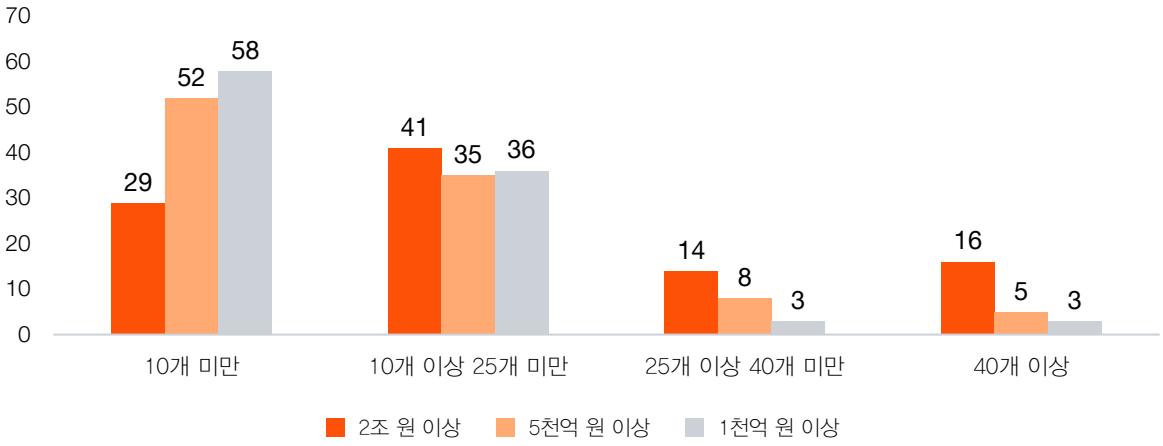
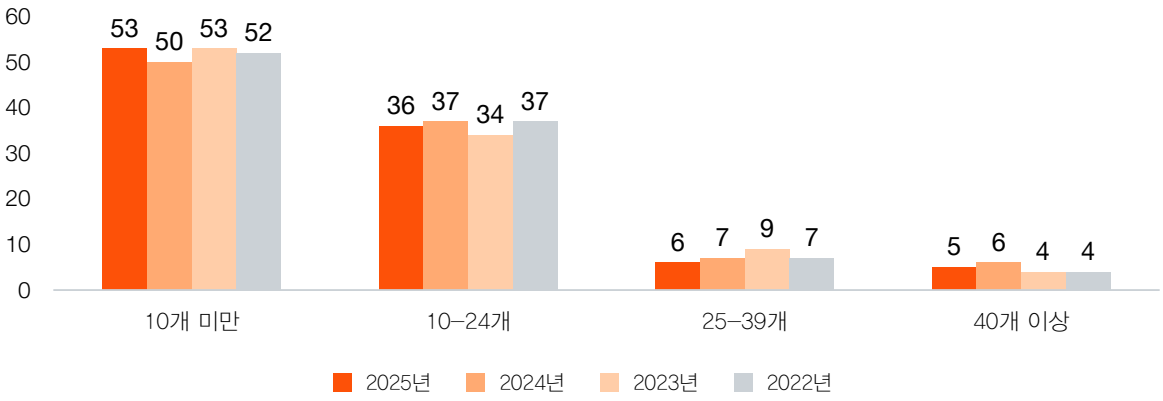


도표 17. **연도별 IPE 대상 항목 개수** (단위: %)



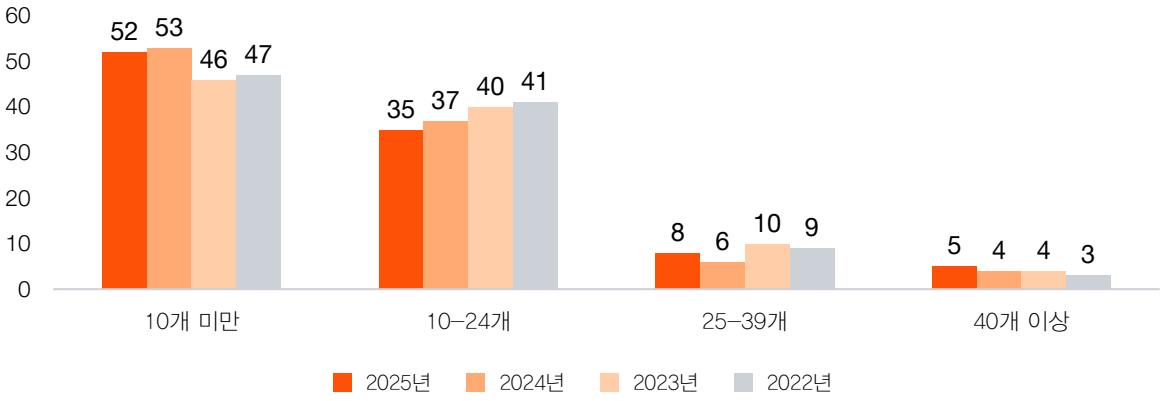
IPE(Information Produced by the Entity) 대상 항목 개수는 10개 미만으로 분류된 회사가 2조 원 이상 회사 보다 2조 원 미만 회사에서 월등히 많은 것으로 확인되었다. 이는 회사의 규모가 클수록 기업의 규모 및 시스템 체계 및 복잡도에 따라, 상대적으로 많은 IPE 개수를 관리하는 것으로 해석된다.

연도별 IPE 대상 항목 변동을 보면 최근 4개년 동안 안정적인 분포를 유지하고 있다. 유의적인 변화는 확인되지 않는데, 이는 회사의 시스템 변경이나 사업부 추가 등의 변화 사항이 중요하지 않는 경우 일반적으로 전기 대비 IPE 내역을 크게 수정하지 않는 경향이 있음을 보여 준다.

통제활동 수행 시 IPE에 대한 의존도를 명확히 판단하여 평가여부를 식별해야 하며. 별도의 관리 및 신뢰성 확인이 필요한 중요한 재무정보가 무엇인지에 대한 점검이 매년 필요하다. 또한, 형식적이거나 비효율적인 IPE 관리가 아닌 실질적인 IPE 관리가 필요하다.

13. EUC 항목 현황

도표 18. **연도별 EUC 대상 파일 개수** (단위: %)

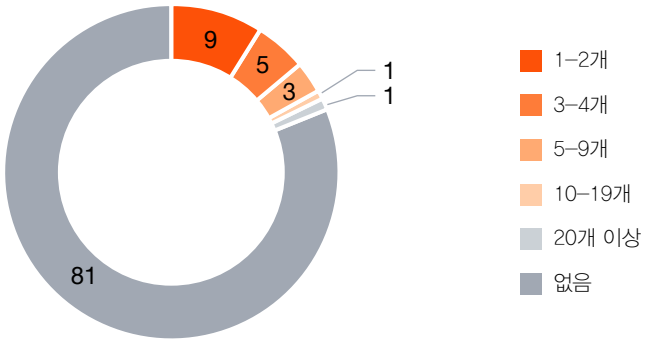


연도별 EUC(End User Computing) 대상 파일 보유 개수는 최근 3개년 동안 10개 미만이 약 46% 에서 ~ 52%로 꾸준히 상승하고 있다. 회사들이 EUC 대상 파일을 최적화하거나 통합한 결과로 해석된다.

EUC는 재무제표 작성 과정에서 외부 증빙에 근거한 것이 아닌, 회사가 자체적으로 계산한 재무제표에 반영될 결산 결과의 유일한 증거이므로 철저한 관리가 필요하다. 다만 그 경우에도 복잡도와 중요도의 개념은 존재한다. 단지 엑셀파일 등을 통해 계산했다는 사실이 EUC임을 입증하지 않는다. 내부회계관리제도 도입 초기에는 EUC의 무분별한 지정이 존재하였으나, EUC의 내용 및 범위가 점점 구체화 및 체계화됨에 따라 실질적인 관리 수준이 향상되고 있다.

14. 유의적 미비점 및 중요한 취약점 현황

도표 19. **개선 여부와 관계없이 발견된 유의한 미비점 및 중요한 취약점 개수** (단위: %)



구분	2025년	2024년
1–2개	9	5
3–4개	5	4
5–개	3	2
10개–19개	1	–
20개 이상	1	–
없음	81	89

내부회계관리제도 평가기준일 현재 개선 여부와 관계없이 발견된 유의한 미비점 및 중요한 취약점의 개수를 분석한 결과, 2025년에는 약 81%의 회사가 당기 중 발생한 미비점 및 취약점이 없다고 답하였으며, 약 9%의 회사가 1개 혹은 2개의 미비점/취약점을 발견했다고 답변했다. 이는 전년(89% 없음)과 비교하여 약 8%p 감소한 수치로, 미비점/취약점 발생 빈도가 높아지는 추세를 보인다.

다른 분석 결과에서도 나타나듯 아직 내부회계관리제도의 안정적인 정착을 위해서는 많은 과제들이 선결되어야 할 것으로 여겨진다. 또한 미비점을 식별하고 있는 추이가 점진적으로 지속적으로 높아지고 있다는 점은 각 기업들의 내부회계관리제도에 대한 관심을 좀 더 기울여야 하는 이유가 되고 있다.

표 2. **연도별 발생한 미비점 원인 유형 분석 결과**

구분	2025년	2024년	2023년	2022년
감사인이 발견한 중요한 재무제표 수정 사항	1순위	1순위	3순위	3순위
자금내부통제 이슈	2순위	5순위	3순위	2순위
업무분장 이슈	3순위	3순위	3순위	2순위
정보기술통제(ITGCs) 이슈	4순위	2순위	1순위	1순위
내부감사기능의 부재 또는 불충분한 기능	5순위	9순위	6순위	7순위
비경상적 거래에 대한 통제활동 이슈	6순위	5순위	5순위	5순위
추정관련 통제활동 이슈	6순위	7순위	2순위	4순위
경영진 및 종업원의 윤리적 이슈	8순위	10순위	10순위	10순위
주석공시 관련 통제활동 이슈	9순위	12순위	8순위	9순위
회계인력의 적격성 이슈	10순위	10순위	10순위	10순위
재무제표 재작성	11순위	4순위	8순위	5순위
범위 제한 또는 기타 제한	11순위	7순위	6순위	10순위
감사(위원회)의 불충분한 기능	11순위	12순위	12순위	8순위

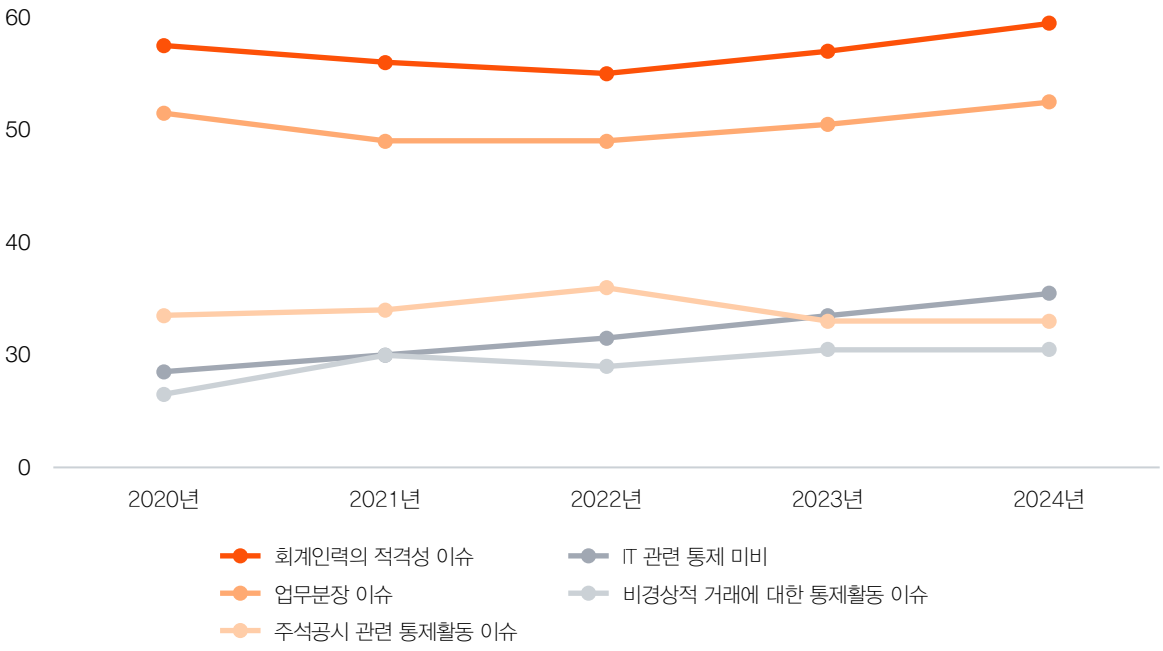
내부회계관리제도 평가기준일 현재 개선 여부와 관계없이 발견된 미비점의 원인 유형 분석 결과, 2025년 1순위는 '감사인이 발견한 중요한 재무제표 수정 사항'으로 2024년과 동일하게 1위를 유지하였다. 2순위는 '자금내부통제 이슈'로 2024년 5순위에서 큰 폭으로 상승한 점이 주목할 만한 변화이다. 이는 최근 횡령 등 부정위험 관련 자금통제 공시 의무화 이후 관련 이슈가 더욱 부각된 결과로 해석된다.

3순위는 '업무분장 이슈', 4순위는 '정보기술통제(ITGCs) 이슈'로 ITGC 이슈는 2022~2023년 1순위였으나 2024년 2순위, 2025년 4순위로 점진적으로 하향 안정화되고 있다. 한편 '내부감사기능의 부재 또는 불충분한 기능'이 2025년 5순위로 전년(9순위) 대비 상승한 점은 거버넌스 및 부정위험 대응 차원에서 내부감사 기능의 실효성이 다시 중요하게 부각되고 있음을 시사한다. 자금관련 통제 강화 및 거버넌스 기능 보완이 향후 핵심 과제이다.

표 3. **미비점 발생 해외 사례(미국)**

구분	순위
회계인력의 적격성 이슈	1순위
업무분장 이슈	2순위
IT 관련 통제 미비	3순위
주석공시 관련 통제활동 이슈	4순위
비경상적 거래에 대한 통제활동 이슈	5순위

도표 20. **연도별 미비점 원인 유형 순위(미국)** (단위: %)



Source: IDEAGEN, SOX 404 disclosures: A twenty-year review, 2025, p10

미국 내부통제 이슈 분석 결과, ICFR 평가에서 식별되는 주요 취약 요인은 특정 영역에 집중되는 구조적 특성을 보인다. 특히 회계 인력 부족과 업무 분장 미흡은 최근 5년간 지속적으로 가장 높은 비중을 차지하며 내부통제 취약성의 핵심 요인으로 작용하고 있다. 회계 인력 이슈는 지속적인 증가세를 보이며 가장 높은 수준을 유지하고 있으며, 업무 분장 또한 안정적으로 상위권을 유지함에 따라 인력 및 조직 구조 기반 통제의 한계가 반복적으로 발생하고 있는 것으로 나타났다.

한편, 정보기술(IT) 통제 이슈는 상대적으로 낮은 수준에서 시작하였으나 최근 빠르게 증가하며 주요 리스크 영역으로 부상하고 있다. 이는 기업의 디지털 환경 확대 및 시스템 의존도 증가에 따른 자연스러운 현상으로, 기존 인력 중심 통제 취약성과 결합될 경우 내부통제 전반의 유효성을 저해하는 복합적인 위험 요인으로 작용할 수 있다. 반면 공시 통제 및 비경상 거래 관련 이슈는 일정 수준에서 반복적으로 발생하고 있으나 뚜렷한 개선 추세는 나타나지 않고 있다.

종합적으로 볼 때, 미국과 국내의 내부통제 미비점 원인 구조는 뚜렷한 차이를 보인다. 미국의 경우 회계인력의 적격성, 업무분장 미흡, IT 통제 미비 등 특정 핵심 원인이 전기간에 걸쳐 높은 수준을 지속적으로 유지하는 특징을 보이며, 이는 내부통제 미비점이 비교적 일관된 원인 구조 하에서 발생하고 있음을 시사한다. 반면, 국내의 경우 특정 원인이 지속적으로 지배적인 양상을 보이기보다는 재무제표 수정 사항, 자금통제, ITGC, 업무분장 등 다양한 원인이 연도별로 순위 변동을 보이며 나타나고 있다.

이러한 차이는 미국이 인력 역량 및 통제 수행 체계와 같은 실행 기반 요인에 미비점이 집중되는 반면, 국내는 특정 영역에 국한되지 않고 재무보고, 자금, IT, 통제 환경 등 전반적인 내부통제 체계 내에서 복합적으로 미비점이 발생하고 있음을 시사한다. 따라서 국내의 경우 특정 원인에 대한 단편적인 개선보다는, 주요 통제 영역 전반에 걸친 균형적인 점검과 체계적인 통제 고도화가 필요하며, 특히 재무보고 정확성 및 IT 기반 통제에 대한 지속적인 관리 강화가 요구된다.

15. 미비점 발생 프로세스 분석

표 4. **연도별 미비점 발생 프로세스별 구분**

구분	2025년	2024년	2023년	2022년
전사수준통제	1순위	3순위	6순위	3순위
재무보고	2순위	1순위	1순위	5순위
전산일반(ITGC)	3순위	4순위	2순위	2순위
자금	4순위	5순위	2순위	4순위
영업	5순위	2순위	4순위	1순위
영업비용(생산,구매)	6순위	2순위	4순위	1순위
고정자산	7순위	6순위	7순위	7순위
투자	8순위	–	–	–
인사	9순위	–	–	–

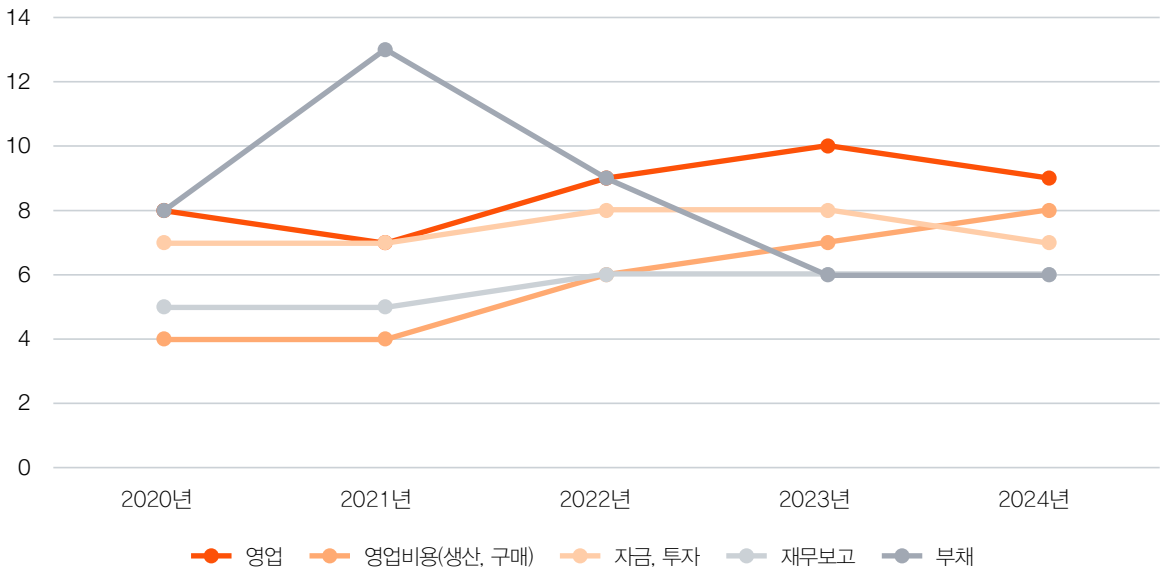
미비점 발생 프로세스 분석 결과, 2025년 1순위는 '전사수준통제(Entity–Level Control)' 프로세스로 확인되었다. 타 프로세스에서 미비점이 발생한 경우 전사수준통제활동 모니터링 관점의 미비점을 언급하는 경우 지속적으로 늘어나고 있으며 최근 횡령 등 부정위험과 관련한 자금통제 공시에서 전사수준통제의 중요성이 높아지고 있음을 보여준다.

그 외 4개년 추이를 살펴보면 전사수준통제이외에 재무보고 및 전산일반 프로세스가 꾸준히 상위권에 위치하고 있으며, 이는 기업 규모나 업종과 관계없이 해당 영역의 설계·운영 취약점이 보편적으로 나타남을 시사한다. 그리고, 자금통제 공시 의무화 이후 자금 프로세스에 대한 중요성이 높아지면서 향후 해당 프로세스의 상위권으로의 순위 변동이 예상되므로 기업들은 자금 흐름 전반에 대한 내부통제 체계를 지속적으로 강화할 필요가 있다.

표 5. **미비점 발생 프로세스 해외 사례(미국)**

구분	순위
영업	1순위
영업비용(생산,구매)	2순위
자금, 투자	3순위
재무보고	4순위
부채	5순위

도표 21. **연도별 미비점 발생 프로세스 순위(미국)** (단위: %)



Source: IDEAGEN, SOX 404 disclosures: A twenty-year review, 2025, p13

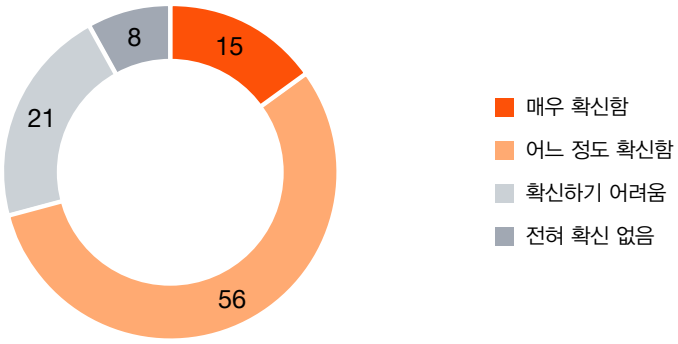
미국 사례를 중심으로 내부통제 미비점 발생 영역을 살펴보면, 영업 관련 이슈가 여전히 가장 주요한 영역으로 식별되며 전반적으로 높은 비중을 유지하고 있다. 특히 2022년 이후 다시 증가하여 2023년에는 가장 높은 수준을 기록한 이후에도 2024년까지 유의미한 수준을 유지하고 있어, 영업 활동 전반 및 관련 수익 창출 프로세스에 대한 통제의 중요성이 지속적으로 강조되고 있는 것으로 나타났다. 영업비용(생산·구매) 역시 완만한 증가 추세를 보이며 점진적으로 중요성이 확대되고 있으며, 재무보고 영역 또한 최근으로 갈수록 비중이 증가하는 경향을 보여 재무정보 산출 및 검증 프로세스 전반에 대한 통제 강화 필요성을 시사한다. 반면, 부채 관련 이슈는 2021년을 정점으로 감소 추세를 보이며 상대적인 중요도는 낮아지는 모습을 나타낸다.

한편, 국내 데이터의 경우 연도별 주요 이슈의 순위 변동이 비교적 큰 특징을 보인다. 2025년 기준으로는 전사수준 통제가 1순위로 상승하며 가장 중요한 이슈로 나타났고, 재무보고 및 IT 일반통제(ITGC) 또한 상위권을 유지하고 있어, 통제 환경 및 IT 기반 통제에 대한 중요성이 상대적으로 강조되고 있는 것으로 해석된다. 또한 자금, 영업, 영업비용 등 운영 프로세스 관련 이슈는 연도별로 순위 변동이 크며 특정 영역에 집중되기보다는 다양한 영역에서 분산적으로 발생하는 특징을 보이고 있다.

종합적으로 볼 때, 미국의 경우 영업과 영업비용 등 운영 프로세스 중심의 미비점이 지속적으로 주요 이슈로 나타나는 반면, 국내는 전사수준 통제, 재무보고, ITGC 등 보다 상위 구조적 통제 영역의 중요성이 상대적으로 높게 나타나는 차이를 보인다. 이는 국내 기업의 경우 개별 거래 수준의 통제뿐만 아니라 통제 환경 및 전사적 관리 체계의 효과성에 대한 이슈가 보다 중요하게 부각되고 있음을 시사하며, 향후 내부회계관리제도의 고도화를 위해서는 전사수준 통제와 IT 기반 통제에 대한 체계적인 정비와 함께 주요 운영 프로세스에 대한 지속적인 모니터링이 병행될 필요가 있다.

16. 내부회계관리제도의 실효성

도표 22. **내부회계관리제도의 실질적인 재무 리스크 통제 수행에 대한 확신 여부** (단위: %)



구분	2025년	2024년
어느 정도 확신함 운영되고 있으나, 실질적인 리스크 통제 효과는 다소 미흡함	56	54
확신하기 어려움 형식적인 프로세스는 있지만, 실질적인 리스크 통제가 부족함	21	24
매우 확신함 내부회계관리제도가 실질적인 리스크 통제에 기여하고 있음	15	17
전혀 확신 없음 내부회계관리제도의 실효성이 매우 낮다고 판단됨	8	5

내부회계관리제도의 실질적인 재무 리스크 통제 수행에 대한 확신 여부 응답에서 2025년 '매우 확신함'(15%)과 '어느 정도 확신함'(56%)의 합계가 약 71%로 전년(약 71%)과 동일한 수준을 유지하고 있다. 이는 내부회계관리제도의 효익에 대해 다소 의구심이 있었던 상황에서 감사 도입 이후 회사들이 제도에 대한 상당한 효용을 체감하는 흐름이 지속되고 있음을 보여준다. 즉, 내부회계관리제도가 재무제표 신뢰성 제고라는 본연의 목적에 대해 매우 긍정적인 영향을 미치고 있음을 고려할 수 있다.

향후 내부회계관리제도의 실효성을 보다 더 확보하기 위해서는 실질적인 리스크 관리 및 고도화 방안 도입이 필요하며, 특히 AI를 포함한 디지털 기술을 활용한 실시간 모니터링, 데이터 분석 기반 위험평가 등을 통해 형식적 운영을 넘어 업무 효율화를 포함하여 실질적인 효용을 달성하는 체계 구축이 요구된다.

표 6. **내부회계관리제도 실효성 제고를 위한 핵심 과제**

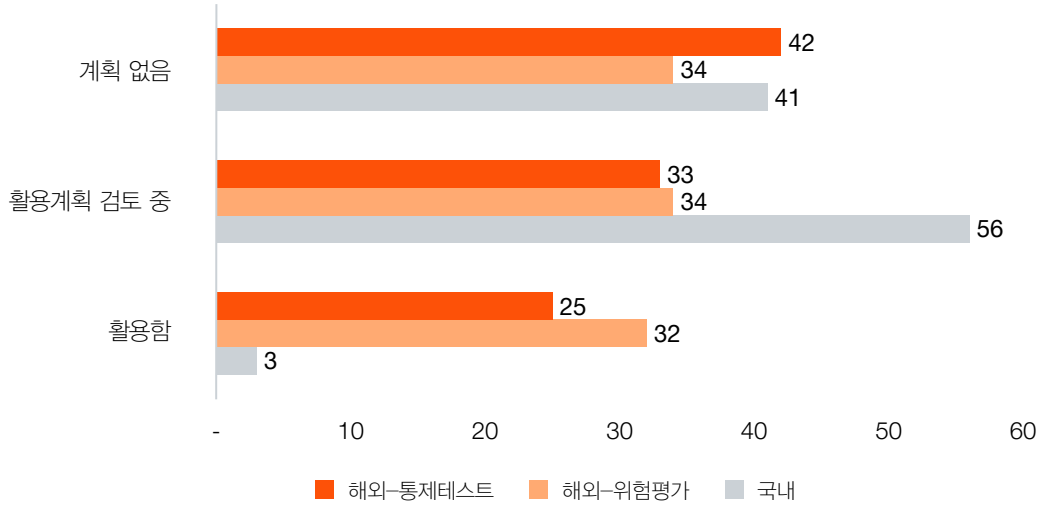
구분	2025년	2024년
현업의 내부통제 중요성 및 이해도 증대	1순위	1순위
경영진의 적극적인 관심 및 지원	2순위	1순위
내부회계관리제도 전담인력의 증가	3순위	4순위
실질적 위험평가	4순위	5순위
임직원에 대한 지속적인 교육	5순위	3순위
Digital 및 AI 등을 활용한 업무 효율화	6순위	7순위
데이터 분석을 활용한 내부회계관리제도 효율화	7순위	6순위
내부회계관리제도 시스템(패키지) 활용	8순위	9순위
외부 자문사 활용	9순위	8순위

내부회계관리제도 실효성 제고를 위한 핵심 과제 분석 결과, 2025년 1순위는 '현업의 내부통제 중요성 및 이해도 증대'로 확인되었다. 이는 2024년에도 경영진의 관심 및 지원과 공동 1순위를 차지했던 항목으로, 내부회계관리제도의 실질적 작동을 위해서는 재무부서 뿐만 아니라 업무 현장의 통제 주체인 현업 부서의 인식 전환이 가장 중요한 선결 과제임을 보여준다. 2025년 2순위는 '경영진의 적극적인 관심 및 지원'으로, 경영진 리더십이 내부통제 문화 확립의 핵심 동인임을 재확인시켜 준다.

내부회계관리제도의 내재화 및 실효성 제고를 위해서는 현업 직원 및 경영진에 대한 역할과 책임을 강조하는 내부회계관리제도 교육 프로그램의 지속적이고 정기적인 수행이 병행되어야 한다. 그리고, '현업의 이해도 증대'와 '경영진의 관심 및 지원'은 상호 보완적인 과제로, 두 가지가 동시에 강화될 때 내부통제 문화가 조직 전반에 뿌리내릴 수 있다. 이는 단순한 절차적 준수를 넘어 내부회계관리제도를 진정한 리스크 관리 수단으로 정착시키는 핵심 조건이기도 하다.

17. 내부회계관리제도 AI 활용 여부

도표 23. **내부회계관리제도 AI 도입 현황** (단위: %)

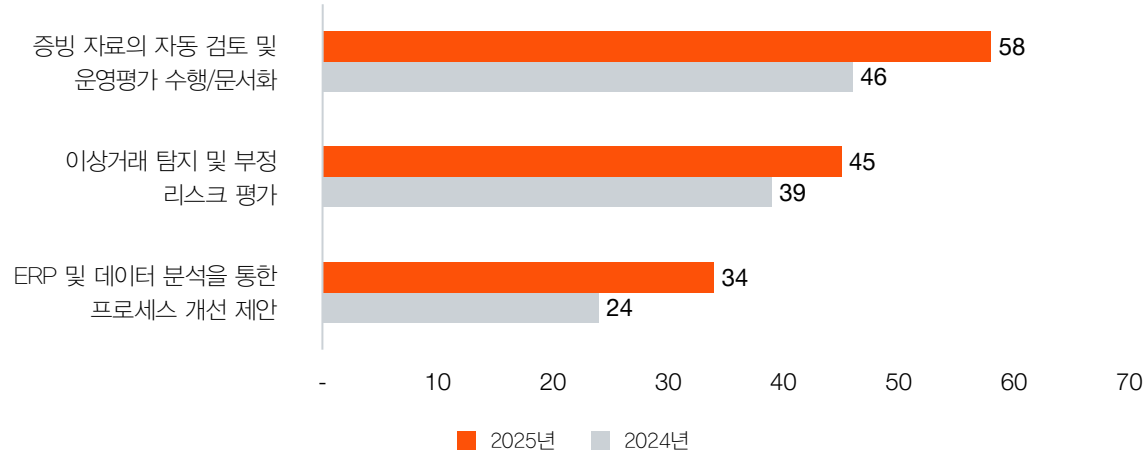


해외 Data Source: PwC, 'Use of AI for compliance' PwC, 'Global Compliance Survey 2025' p.29

PwC Global Compliance Survey 2025에 따르면 해외 기업들의 약 32%가 AI를 위험평가 그리고 25%가 통제테스트에 적용 하고 있는 것으로 확인되었다. 또한 활용계획을 검토 중인 곳 또 33%~34%에 달하였다.

반면 국내의 경우 내부회계관리제도와 관련하여 전체의 약 3%만이 AI를 활용하는 것으로 나타났으며 계획 없는 경우는 41%에 달하였다. 다만, 작년의 경우 "활용 중"이 1%였던 점과 "활용계획 검토 중"이 작년 대비 약 24%가 늘어난 약 56%인 점은 향후 AI를 활용한 내부회계관리제도의 고도화 가능성이 높아지고 있음을 보여 준다. 매월, 매일 성능이 업그레이드 되고 있어 AI 혁명이라는 용어 또한 심심치 않게 들을 수 있는 현 시대상을 고려하면, 다가오는 변화가 아닌 현재 활용 가능한 Tool인 AI에 대한 적극적인 활용을 고려 해야 하는 시점으로 판단된다.

도표 24. **내부회계관리제도 AI 도입 희망 기능** (단위: %) (복수응답)



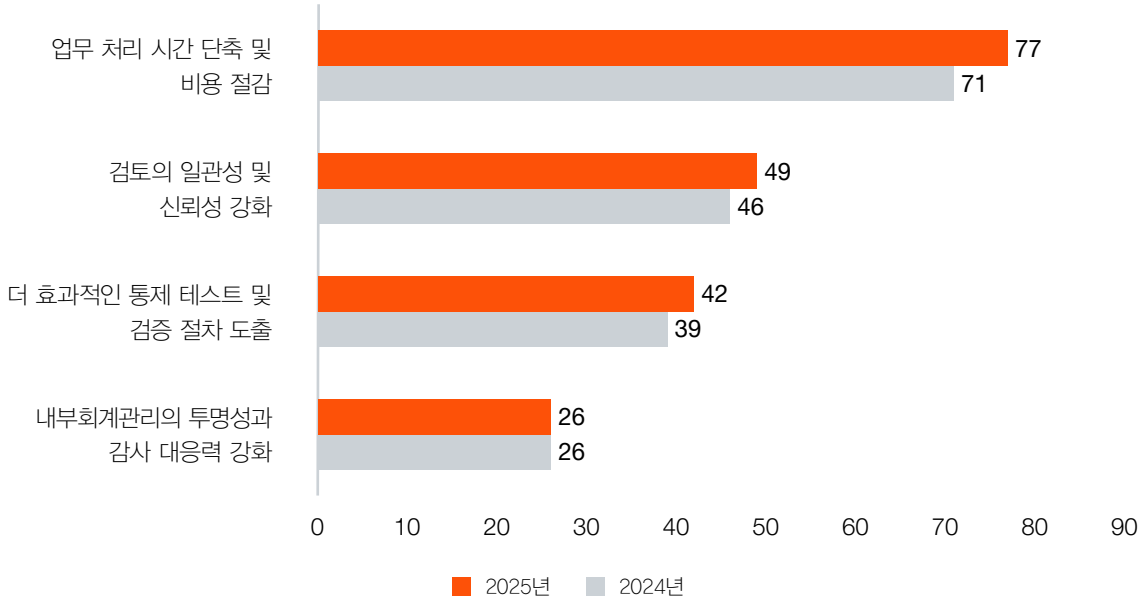
기업들이 내부회계관리제도에 도입을 희망하는 AI 기능 중 가장 높은 응답률을 보인 항목은 2025년 '증빙 자료의 자동 검토 및 운영평가 수행·문서화'로 약 58%로 전년(약 46%) 대비 약 12%p 상승하였다.

작년의 경우 단순히 가능할지도 모르다는 시기의 조사이며, 현재는 이미 활용가능한 기능이라는 점에 대한 시장 컨센선스가 형성된 시점이므로, 당연한 결과로 보여진다.

또한 '이상거래 탐지 및 부정 리스크 평가'는 약 45%로 전년 (약 39%) 대비 약 6%p 상승, 'ERP 및 데이터 분석을 통한 프로세스 개선 제안'은 약 34%로 전년(약 24%) 대비 약 10%p 상승하였다. 모두 다 기존에는 가능하면 좋은 것들이었으나 이제는 실제로 가능한 시기가 도래하였다. 과거에는 막대한 인력을 운영해야한 유지가능하던 개념들이 AI 혁명이 일어나 충분히 도달가능한 목표가 된점이 반영된 결과로 보인다.

이처럼 전반적으로 모든 AI 기능에 대한 도입 희망 비율이 큰 폭으로 상승한 점은 AI에 대한 기업의 인식이 빠르게 변화하고 있음을 보여 준다. 반대로 'AI 도입을 고려하지 않음' 응답이 약 41%로 전년(약 67%) 대비 큰 폭으로 감소한 점도 동일한 흐름을 확인시켜 준다.

도표 25. **내부회계관리제도 AI 기대 효과** (단위: %)



AI 도입 시 기대되는 효익으로는 2025년에도 '업무 처리 시간 단축 및 비용 절감'이 가장 높은 응답을 기록하였으며, '검토의 일관성 및 신뢰성 강화', '더 효과적인 통제 테스트 및 검증 절차 도출'이 그 뒤를 잇고 있다. 전년과 동일한 우선순위 구조를 유지하면서도 전반적으로 응답률이 상승하는 흐름을 보이고 있다.

이는 운영평가 테스트 및 문서화 과정에서의 휴먼 에러 방지와 업무 효율화를 통한 비용 절감을 동시에 추구하고자 하는 기업의 실질적 요구를 반영한다. 내부회계관리 업무의 복잡성과 반복성이 높아지는 환경 속에서 AI가 제공하는 자동화와 분석 기능이 기업의 실질적 요구와 맞닿아 있다. 중장기적으로 AI를 포함한 디지털 기술을 제도 운영에 접목하고, 시스템 기반의 효율적인 내부통제 체계를 병행하여 구축해 나가는 전략이 필요할 것이다.

18. 내부통제 업무에 AI 도입 시 가장 큰 장애 요인

표 7. **AI 내부통제 업무 도입 시 가장 큰 장애 요인**

장애 요인	국내 순위	해외 순위*
도입 및 유지 비용 부담	1순위	4순위
AI의 정확성 및 신뢰성에 대한 우려	2순위	1순위
기존 시스템과의 통합 문제	3순위	2순위
내부 직원의 AI 사용에 대한 기술적 이해 부족	4순위	2순위
규제 및 법적 요구사항과의 충돌 가능성	5순위	2순위

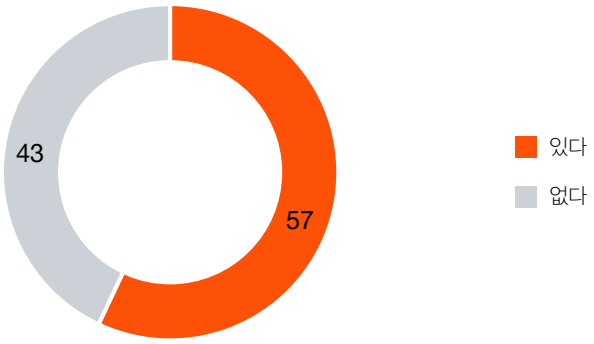
* PwC, 'Level of concern around the use of AI for compliance activities', PwC's Global Compliance Survey 2025, P.32

내부통제 업무에 AI 도입 시 주요 장애 요인을 분석한 결과, 2025년 국내 1위는 여전히 '도입 및 유지 비용 부담'으로 전년과 동일하다. 2위는 'AI의 정확성 및 신뢰성에 대한 우려', 3위는 '기존 시스템과의 통합 문제'로 이는 국내에서 AI의 효익보다는 투자 금액과 시스템 호환성에 더 많이 집중하는 경향이 있음을 보여 준다.

해외(PwC Global Survey 기준)에서는 AI의 정확성·신뢰성, 규제·법적 요구사항과의 충돌 가능성, 내부 직원의 기술적 이해 부족이 상위에 위치하는 점과 대비된다. 국내는 주로 초기 투자 부담에 집중, 해외는 운영 안정성과 제도 정합성 리스크에 무게를 두는 상반된 도입 판단 프레임이 존재한다. 특히 국내의 경우 2026년 1월 AI 기본법 시행 등 신규 규제 환경에 대한 사전적 대응이 더욱 중요해지고 있어, 국내 기업들도 비용 부담 중심의 단기적 시각을 넘어 운영 안정성, 신뢰성, 법적 정합성 등 중장기 관점의 도입 전략 수립이 필요한 시점이다.

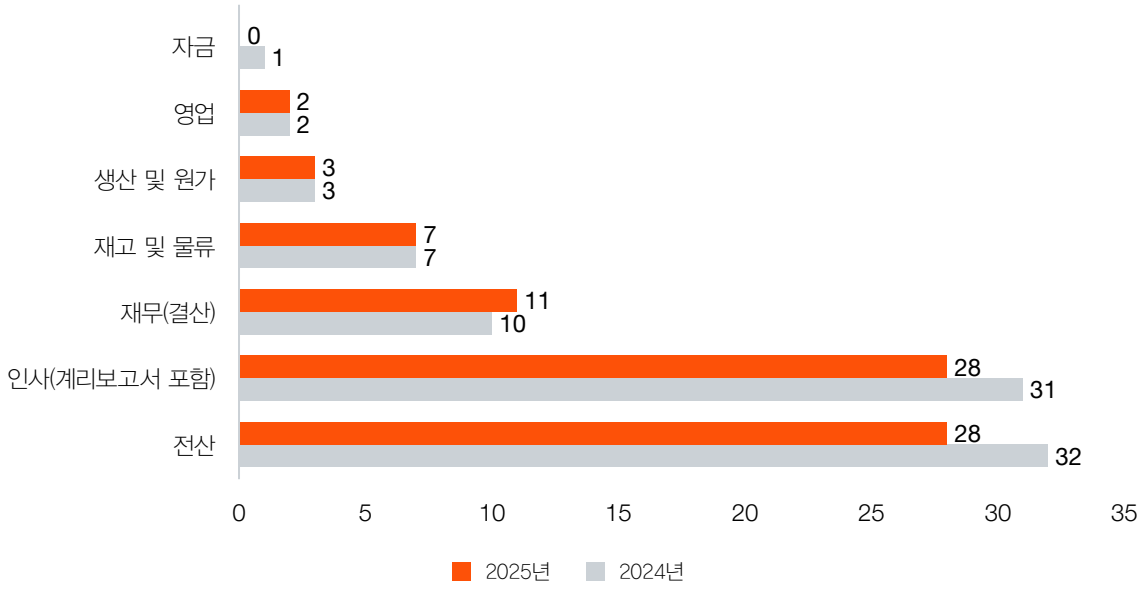
19. 회사 업무 중 외부 아웃소싱 여부 및 업무 영역

도표 26. **회사 업무 중 외부 아웃소싱 여부** (단위: %)



전체 응답 기업의 일부 업무를 외부에 아웃소싱 하고 있는 비율이 2025년에도 과반을 유지하고 있다. 이는 기업들이 표준화된 업무와 전문 인력이 요구되는 영역에서 외부 서비스 활용을 통해 업무 효율성을 확보하고자 하는 흐름이 지속되고 있음을 보여 준다. 전년 대비 아웃소싱 비율의 큰 변동은 없다.

도표 27. **회사 업무 중 외부 아웃소싱 영역** (단위: %)



아웃소싱이 가장 많이 이루어지는 업무는 2025년에도 전산과 인사(계리보고서 포함) 영역으로 나타났다. 이는 두 영역 모두 업무의 표준화 수준이 높고 기업 내부 운영과의 분리가 비교적 용이하여 외부 전문 인력 활용에 효과적인 특성을 갖고 있기 때문이다.

전산 업무는 전문적인 IT 인프라 운영 역량과 인력 확보의 어려움으로 인해 외부 위탁 업체가 활용되며, 인사 업무는 급여 계산, 근태 관리, 계리보고서, 연말정산, 4대 보험 신고 등 반복적이고 기준이 명확한 업무 중심으로 이루어진다. 주목할 만한 부분은 재무(결산)의 경우도 일정 비율로 외부에 아웃소싱을 하고 있다는 응답이다. 아웃소싱의 영역도 내부통제 관점에서는 동일한 관리 대상이 되므로 기업 내부 부서의 내부통제와 동질의 수준의 내부통제 설계 및 운영을 통해 내부통제의 실효성을 높일 필요가 있다. 따라서 계약시점에 아웃소싱 업체가 회사의 통제 수준과 유사한 수준으로 내부 통제가 작동하고 있는지 확인하여 업체를 선정하도록 내부 프로세스를 운영해야 한다.

20. 외부 서비스 조직(아웃소싱 업체) SOC 인증보고서 요구 실태 및 영역

도표 28. **아웃소싱업체 SOC 인증보고서 요구 실태** (단위: %)

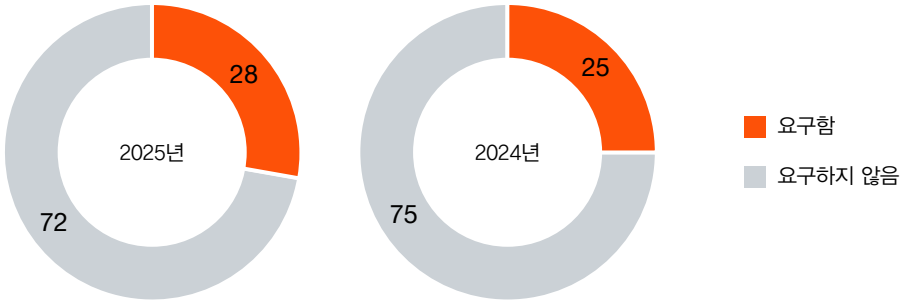
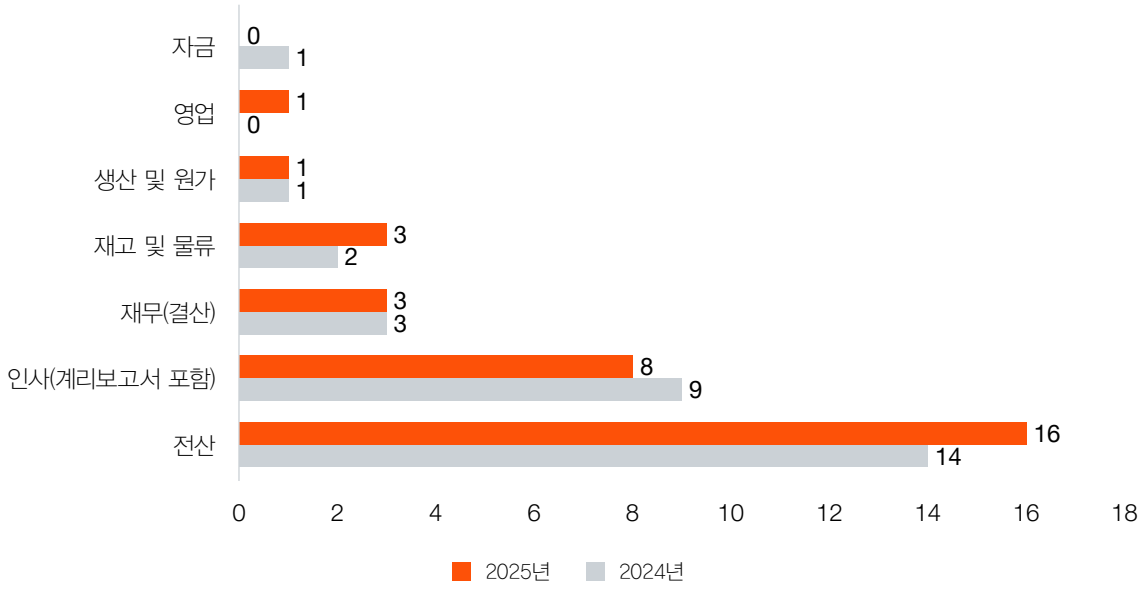


도표 29. **아웃소싱업체 SOC 인증보고서 요구 영역** (단위: %)



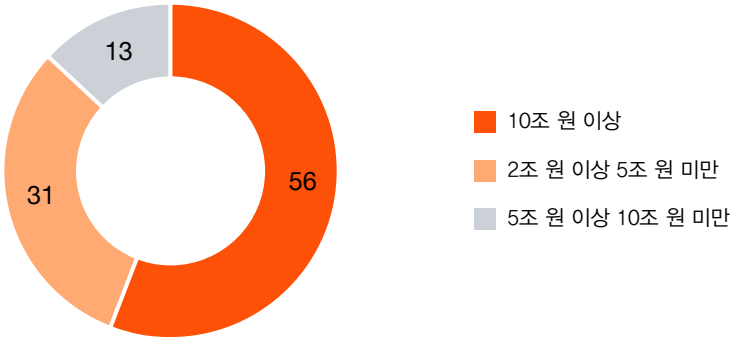
아웃소싱된 영역이 전산, 인사 등 회사의 재무제표와 관련된 중요한 프로세스인 만큼, 위탁 업무를 수행하는 외부서비스제공자의 통제 설계 및 운영 효과성 평가가 또한 중요하다. 그럼에도 불구하고, 2025년에도 외부 서비스를 이용하는 기업 중 실제로 SOC(System and Organization Controls) 혹은 ISAE3402(International Standard on Assurance Engagements, Assurance Reports on Controls at a Service Organization) 리포트를 요구한 비율은 여전히 일부에 그치고 있어, 미국의 경우와 비교할 때 상대적으로 외부서비스제공자의 통제 검증이 아직 보편화 되지 않은 것으로 나타난다.

SOC 인증보고서를 요구하는 업무 영역은 2025년에도 전년과 유사하게 전산 영역이 가장 높고, 인사(계리보고서 포함) 영역이 그 뒤를 잇고 있다. 다만 인사는 아웃소싱 수행 비율에 비해 SOC 요청 비율이 현저히 낮다. 일반적인 인식으로 전산영역에 대해서는 직접적인 테스트가 현실적으로 어려운 점이 존재하여 SOC를 요구하는 경향이 높고, 인사의 경우 상대적으로 중요도가 낮은 바 SOC 요청비율이 낮은 것으로 추정된다.

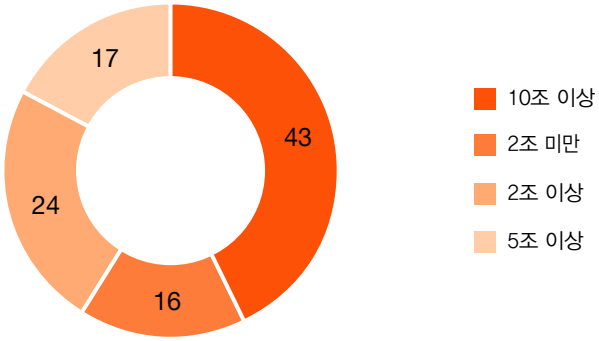
2조 원 이상 회사의 연결내부회계관리제도 현황

도표 1. **2조 원 이상 회사의 총자산/종속기업/매출액 규모별 비율** (단위: %)

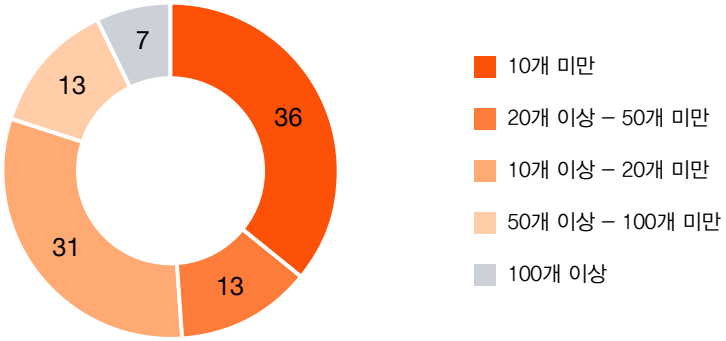
연결자산



연결 매출액

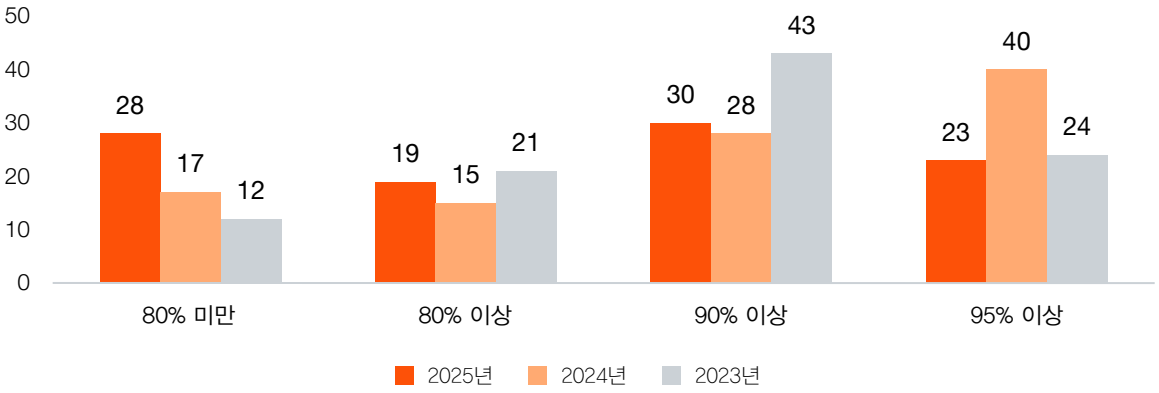


종속회사수



1. 연결내부회계관리제도 구축 범위

도표 2. **연결내부회계관리제도 구축 범위** (단위: %)

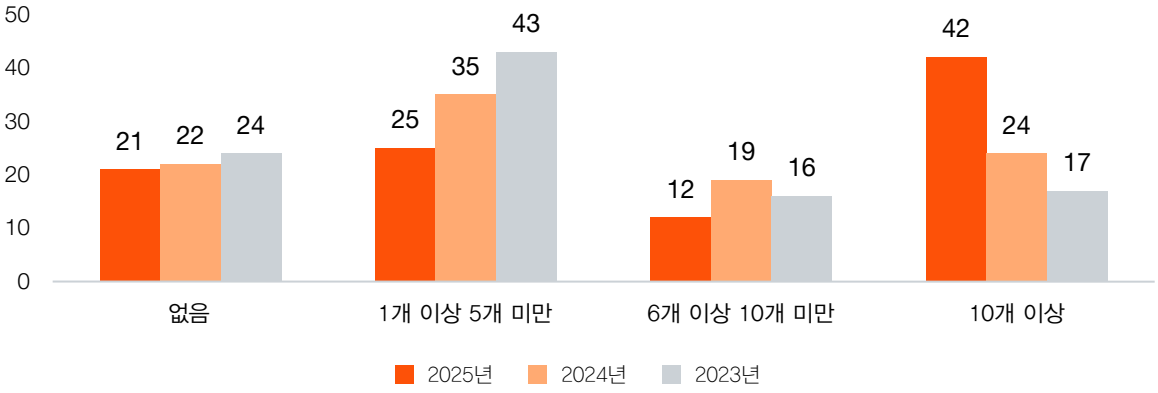


연결내부회계관리제도 운영과 관련하여 매년 연결재무제표의 총자산 및 매출 등의 변동, 종속기업의 재무성과의 변동 등으로 인한 In-scope 대상 종속기업의 선정관련 변화관리는 매우 중요한 항목이다.

연결내부회계관리제도 운영 범위와 관련하여 Coverage 분포를 분석한 결과, 2025년 90% 이상 및 95% 이상 Coverage를 적용하는 기업은 약 53%로 과거 2개년 대비 15% 정도 감소한 것으로 파악되었다. Coverage를 80% 미만으로 적용하는 회사 역시 2025년 28%로 지속적으로 23년 이후 지속적으로 증가하는 추세이다(12% → 28%). 또한 이러한 흐름은 종속회사 숫자와 무관하게 나타나고 있음을 확인하였다. 따라서 전체적으로 Coverage가 감소하고 있으며 이는 연결내부회계관리제도 대상범위에 대한 금융감독원의 가이드라인이 각 회사에 안정적으로 반영되고 있음을 보여주는 사례라고 판단된다.

향후 2029년 별도자산 5천억 원 이상 회사로 연결 감사가 확대될 예정인데, 해당 회사들은 기존 별도자산 2조 이상 회사들의 연결내부회계관리제도 대상 범위 선정에 대한 Data를 참고하여 연결내부회계관리제도 구축 시 연결그룹 상황 및 금융감독원의 관련 가이드라인 등을 고려해서 실질적인 구축이 필요하다.

도표 3. **GWC 설계의 수** (단위: %)

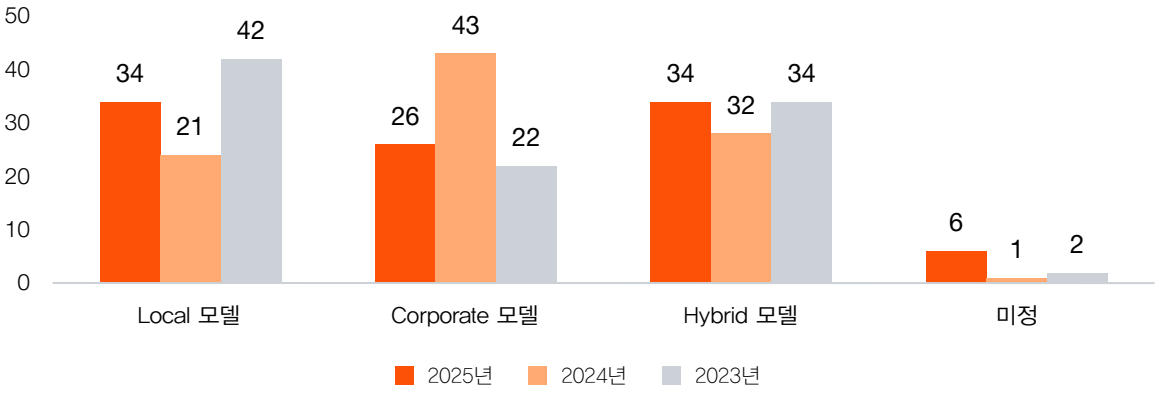


거래수준통제를 직접 수립하지 않고 그룹수준 레벨로 통제(Group Wide Control, GWC)를 설계한 개수를 분석한 결과, 2025년에는 '10개 이상'이 42%로 가장 많은 비중을 차지하며, 전년(24%)과 전전년(17%)와 비교하여 지속적으로 크게 증가하였다. '1개 이상 5개 미만'이 25%, '없음'이 21%, '6개 이상 10개 미만'이 12%로 나타났다. 이는 연결내부회계관리제도가 3년간 운영됨에 따라 그룹수준 통제 설계 범위가 확대되고 있음을 보여 준다.

이러한 그룹수준 레벨 통제의 설계 및 운영은 내부통제를 통한 그룹 리스크 관리 측면에서 매우 실효적인 방안이고 In-scope 포함 여부를 떠나 전체 종속기업들에 적용하는 것이 일반적이고 보다 더 효과적일 수 있다. 또한, 최근 그룹차원에서 종속기업에 대한 실질적인 관리 및 모니터링에 대한 노력과 관심의 증대되고 있는 점을 고려할 때 점차적으로 그룹레벨수준통제가 증가할 것으로 예상되고 연결내부회계관리제도를 효율적으로 운영할 수 있는 대안인 동시에 전사적인 리스크 관리 측면에서도 매우 유용한 수단이 될 수 있다.

2. 연결내부회계관리제도 조직 운영 방식

도표 4. **연결내부회계관리제도 운영 조직 구성 방법** (단위: %)

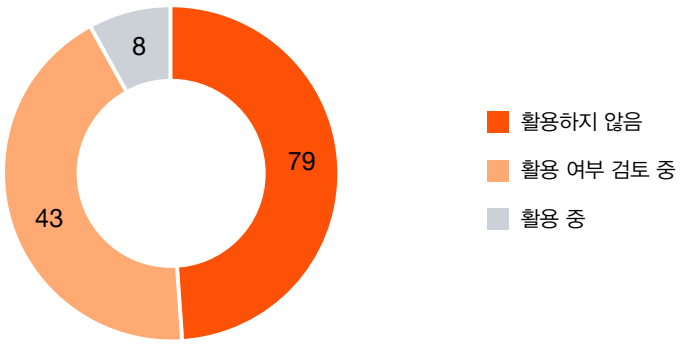


연결내부회계관리제도 운영 조직 구성 방법의 경우, 2025년에는 Hybrid 모델(본사+Local 병행) 약 34%, Corporate 모델(HQ 총괄) 약 26%, Local 모델(종속기업별 전담) 약 34%로 세 가지 구조가 공존하고 있다. 연결내부회계관리제도 감사가 처음 적용된 2023년(약 56%)에 비교해서 Hybrid 모델(본사+Local 병행)과 Corporate 모델(HQ 총괄)이 2024년 및 2025년이 각각 약 43%에서 26%로 감소한 점은 연결내부회계관리제도의 궁극적인 책임은 본사에 있으나, 3년차를 맞아 점차 안정적으로 구조로 운영되고 있어 그룹 내부통제의 효율적 관리감독을 위해 Local중심의 구조로 전환되는 경향을 반영한다.

향후 2029년 별도자산 5천억 원 이상 회사로 연결 감사가 확대될 예정인데, 해당 회사들은 기존 별도자산 2조 이상 회사들의 연결내부회계관리제도 조직 운영 방식의 사례 및 교훈을 참고하여 연결내부회계관리제도 구축 시 종속기업를 포함한 연결그룹 상황 등을 고려해서 연결그룹에 최적화된 조직 운영 방식 등에 대해 사전적인 고려가 필요하다.

3. 연결내부회계관리제도(ICFR) 시스템(패키지) 활용 현황

도표 5. **연결내부회계관리제도ICFR 시스템(패키지) 활용 현황** (단위: %)

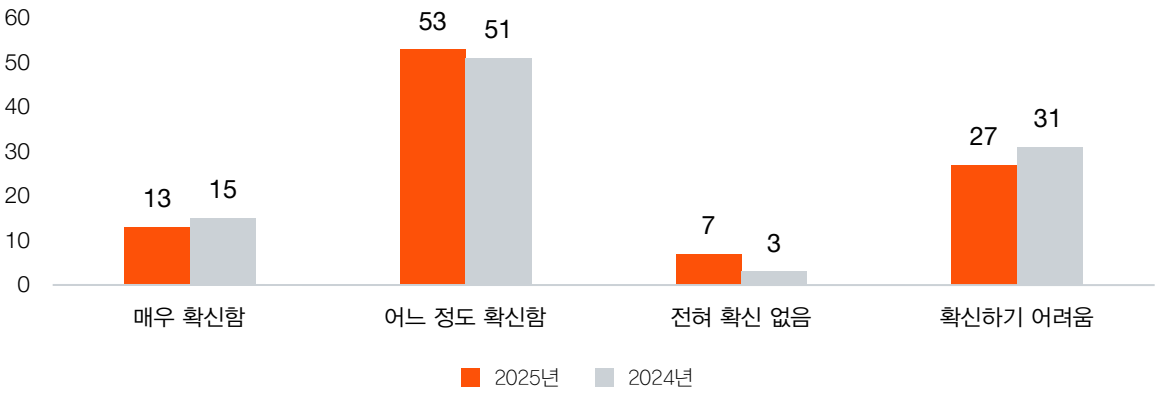


설문 결과 연결내부회계관리제도 평가 시 시스템(패키지)을 활용하는 회사 비율은 2025년의 경우 약 43%로 전기(약 47%)와 유사하게 약 40% 이상으로 나타난다. 또한 별도 부문 패키지 활용률에 비해 다소 낮은 수준을 유지하고 있다. 특히 연결 부문의 경우 다수의 국내외 종속기업가 포함될수록 평가 업무의 효율성과 적시성 증대, 평가 업무의 표준화, 그룹 경영진의 모니터링 효과성 등에서 시스템 활용의 가치가 더욱 크다.

AI를 적용한 다양한 시스템이 출시되고 있으며, 업무의 효율화 등을 고려할 때 향후 연결내부회계관리제도 평가 시에도 시스템을 활용하는 비율이 점진적으로 증가할 것으로 예상된다.

4. 연결내부회계관리제도 재무 리스크 통제 확신 여부

도표 6. **연결내부회계관리제도 재무 리스크 통제 확신 여부** (단위: %)



연결내부회계관리제도의 실질적인 연결 그룹 재무 리스크 통제 수행에 대한 확신 여부 응답에서 2025년에도 '매우 확신함'과 '어느 정도 확신함'의 합계가 전기와 유사하게 60%를 넘는 수준을 유지하고 있다. 연결내부회계관리제도의 효익에 대해 지속적으로 높은 비율의 긍정적인 응답이 있다는 것은 연결내부회계관리제도 감사가 도입된 이후로 연결그룹차원의 실질적인 재무리스크 관리에 효익이 있음을 보여주고 있다. 다만 '매우 확신함'의 비율은 여전히 제한적이며, '확신하기 어렵다'는 응답도 27%에 달해 연결내부회계관리제도의 실효성을 보다 더 체감할 수 있도록 하는 노력과 지속적인 고도화와 개선이 필요하다.

최근에는 이러한 연결내부회계관리제도의 효익을 바탕으로 재무보고 목적의 내부회계관리제도를 넘어서 운영목적 및 법규준수목적을 포함한 그룹 전사 리스크 관리체계로 확대하고자 하는 회사도 점차적으로 증가하고 있다.

5. 연결내부회계관리제도 실효성 제고 핵심 과제

표 1. **연결내부회계관리제도 실효성 제고를 위한 핵심 과제**

구분	2025년	2024년
종속기업 현업의 내부통제 중요성 및 이해도 증대	1순위	1순위
그룹 경영진의 적극적인 관심 및 지원	2순위	1순위
그룹 및 종속기업 내부회계관리제도 전담인력의 증가	3순위	3순위
실질적 위험평가	4순위	7순위
종속기업 임직원에 대한 지속적인 교육	5순위	4순위
종속기업의 내부통제 자체 역량 증대	5순위	4순위
데이터 분석을 활용한 내부회계관리제도 효율화	7순위	8순위
Digital 및 AI 등을 활용한 업무 효율화	8순위	8순위
모회사의 종속기업 내부통제 운영 등에 대한 참여 및 모니터링 강화	8순위	6순위
연결 내부회계관리제도 시스템(패키지) 활용	10순위	10순위

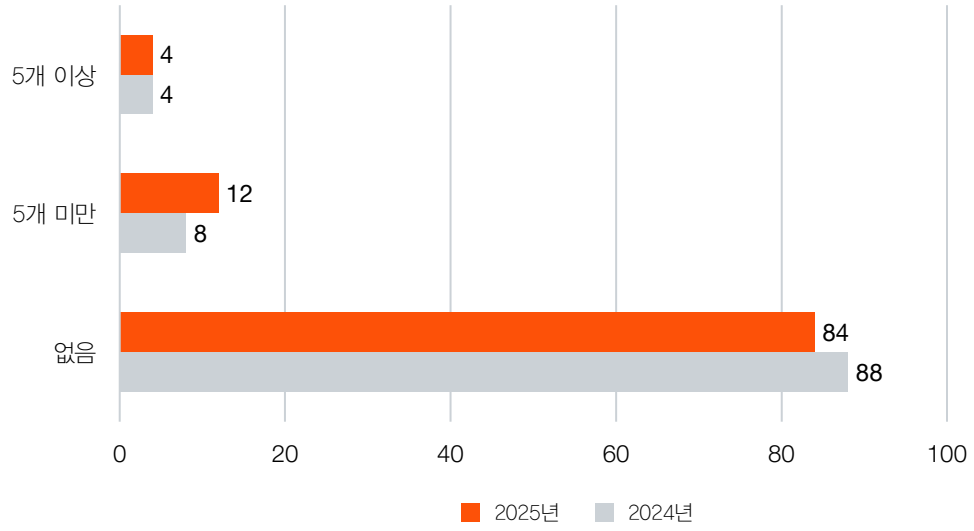
연결내부회계관리제도의 실효성을 높이기 위해 가장 시급한 과제로는 2025년에도 '종속기업 현업의 내부통제 중요성 및 이해도 증대'와 '그룹 경영진의 적극적인 관심과 지원'이 전기와 유사하게 상위권으로 꼽혔다. 이는 별도 자산총액 2조 이상 회사에 대한 연결내부회계관리제도 감사가 도입된 지 3년 차이지만 아직은 충분한 내재화가 이루어지지 않은 상황이 지속되고 있음을 보여 준다.

'실질적 위험평가'가 2025년에 4위(전기 7위)로 순위가 올라간 점은 해당 제도가 3년간 운영되면서 연결그룹관점에서의 실질적 위험평가를 통한 실효적인 연결내부회계관리제도의 운영의 필요성이 강조되고 있음을 보여준다. 그리고, '그룹 및 종속기업 내부회계 전담인력의 증가', '종속기업 임직원에 대한 지속적인 교육', '종속기업의 내부통제 자체 역량 증대' 등 종속기업 차원의 역량 강화 항목들이 상위에 위치한 점은 연결내부회계관리제도의 핵심이 종속기업의 통제 운영 역량에 달려 있음을 재확인하는 결과이다. 또한 데이터 분석 및 Digital/AI 활용 항목도 최근 업무 효율화에 대한 수요가 확대되고 있는 점을 볼 때 연결내부회계관리제도 실효성 제고를 위해 향후 지속적인 관심과 투자가 필요한 항목으로 판단된다.

향후 2029년 별도자산 5천억 원 이상 회사로 연결 감사가 확대될 예정인데, 해당 회사들은 기존 별도자산 2조 이상 회사들의 연결내부회계관리제도 실효성 제고를 위한 핵심과제를 고려하여 실효적인 연결내부회계관리제도 구축이 필요하다.

6. 미비점 및 취약점 개수

도표 7. **미비점 및 취약점 총 개수** (단위: %)



연결내부회계관리제도 평가기준일 현재 In-scope 종속기업과 관련하여 개선여부와 관계없이 발견된 유의한 미비점 및 중요한 취약점의 개수는 2025년에도 대다수의 연결회사가 '없음'으로 응답(2024년 88% 및 2025년 84%)하고 있으며, 일부 회사만이 미비점/취약점을 발견했다고 답변했다. 전년과 유사한 패턴을 유지하고 있다.

다만 제한적이나 5개 미만의 미비점을 언급한 회사의 개수가 늘어났음을 확인할 수 있어 점차, 미비점 식별 및 개선을 위한 노력이 증가하고 있음을 알 수 있다. 내부회계관리제도는 지속적인 미비사항 식별과 치유의 선순환을 통해 위험 경감이 그 목적에 있다고 할 수 있을 것이다. 시행 초기에는 형식적 요건을 충족하기 위한 부분에 대해 집중이 되었다면 향후에는 통제 미비점 발생을 단순히 '없음'으로 관리하기 보다는, 보다 객관적이고 실질적인 평가를 통해 통제 미비점의 파악과 철저한 원인 분석을 통해 실질적인 개선과 실효적인 리스크 관리로 연결이 되어야 의미가 있다.

7. 미비점 사유

표 2. **미비점 사유 (연도별 순위)**

구분	2025년	2024년	2023년	2022년
정보기술통제(ITGCs) 이슈	1순위	3순위	1순위	1순위
감사인이 발견한 중요한 재무제표 수정 사항	2순위	1순위	3순위	3순위
비경상적 거래에 대한 통제활동 이슈	3순위	2순위	5순위	5순위
업무분장 이슈	3순위	–	–	–
재무제표 재작성	3순위	3순위	–	5순위
경영진 및 종업원의 윤리적 이슈	3순위	–	–	–
자금내부통제 이슈	7순위	–	3순위	2순위
주석공시 관련 통제활동 이슈	7순위	3순위	–	–
내부감사기능의 부재 또는 불충분한 기능	7순위	–	6순위	7순위
회계인력의 적격성 이슈	7순위	–	–	–
범위 제한 또는 기타 제한	–	2순위	6순위	–
추정관련 통제활동 이슈	–	3순위	2순위	4순위
감사(위원회)의 불충분한 기능	–	–	–	–

연결내부회계관리제도 미비점 사유 분석 결과, 2025년에는 정보기술통제(ITGCs) 이슈가 1순위를 기록하였다. 이는 2024년 3순위에서 상승한 것으로 IT 환경의 복잡성 증가와 사이버 보안 리스크 확대에 따라 종속기업의 ITGC의 설계·운영상 미비점이 연결 범위 전반에서 주요 과제로 부상하고 있음을 시사한다.

2순위는 감사인이 발견한 중요한 재무제표 수정 사항이며, 비경상적 거래에 대한 통제활동 이슈·업무분장 이슈·재무제표 재작성·경영진 및 종업원의 윤리적 이슈가 공동 3순위를 기록하였다. 연결내부회계관리제도 관점에서 종속기업의 경우도 여전히 감사의 수정사항 및 재무제표 재작성에 기인한 미비점 식별이 중요한 평가 방식으로 유지되고 있음을 보여준다. 특히, 2025년부터 적용된 자금통제 공시 의무화로 인해 종속기업을 포함한 연결그룹차원의 자금통제 이슈에 대해 그룹차원의 지속적인 모니터링과 점검이 필요한 상황이다.

한편 전기 조사시에는 없었던 경영진 및 종업원의 윤리적인 이슈, 주석공시, 내부감사기능의 부재, 회계인력의 적격이슈가 순위권에 들어와 다양한 관점에서 미비점을 바라보려는 노력도 증가하고 있음을 알 수 있다.

8. 미비점 발생 영역

표 3. **미비점 영역 (연도별 순위)**

구분	2025년	2024년	2023년
전산일반	1순위	4순위	2순위
재무보고	2순위	2순위	1순위
자금	2순위	–	2순위
투자	2순위	3순위	–
전사수준통제	5순위	3순위	6순위
고정자산	5순위	4순위	–
영업,영업비용(생산,구매)	7순위	1순위	4순위

연결내부회계관리제도 미비점 발생 영역 분석 결과, 2025년 1순위는 '전산일반' 영역으로 나타났다. 이는 앞서 살펴본 미비점 사유에서 ITGCs 이슈가 1순위를 기록한 것과 일관된 결과로, 종속기업의 취약한 IT 역량 등으로 인한 종속기업의 In-Scope 시스템의 접근권한 관리·변경관리·운영관리 등 전산일반 영역에서의 통제 취약점이 연결 범위 전반에서 주요 과제로 부각되고 있음을 의미한다. 2순위는 재무보고·자금·투자 영역이 공동으로 위치하였다.

연결내부회계관리제도의 특성상 복수의 종속기업에서 발생하는 미비점이 집계되므로, 그룹 차원의 IT 통제 표준화 및 전산 일반 영역에 대한 통합적 관리 방안 수립이 시급하다. 전산 일반 미비점은 설계 수준의 결함 뿐만 아니라 운영 상의 결함으로 연결되는 경우가 많아, 종속기업 IT 인프라 현황 파악 및 그룹 공통 IT 통제 표준 수립과 그룹차원의 종속기업에 대한 ITGC 관리와 지원 등이 중장기 과제로 검토되어야 한다.

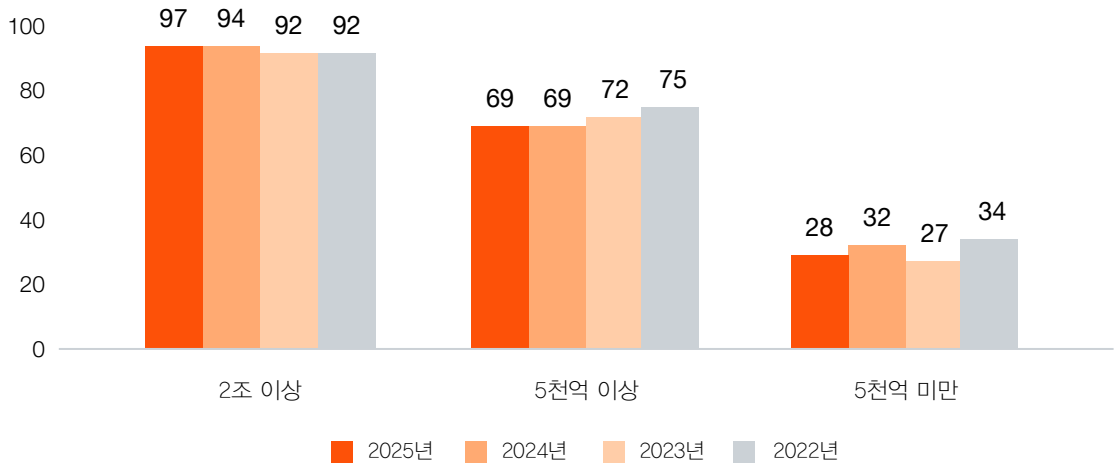
향후 2029년 별도자산 5천억 원 이상 회사로 연결 감사가 확대될 예정인데, 해당 회사들은 기존 별도자산 2조 이상 회사들에 비해 종속기업의 IT인프라 및 역량이 취약할 수 밖에 없는 구조인데 연결내부회계관리제도 구축 시 종속기업의 ITGC를 그룹차원에서 어떻게 실질적으로 관리하고 지원할지에 대한 사전적인 고려가 필요하다.

부정 위험 대응 현황

최근 계속적으로 발생하고 있는 횡령과 관련한 회사의 부정위험 관리 방안 및 자금 프로세스 관련 통제활동에 대한 현황을 확인해 보겠다.

1. 내부감사전문조직 설치 여부

도표 1. **자산규모별 내부감사전문조직 설치 여부** (단위: %)



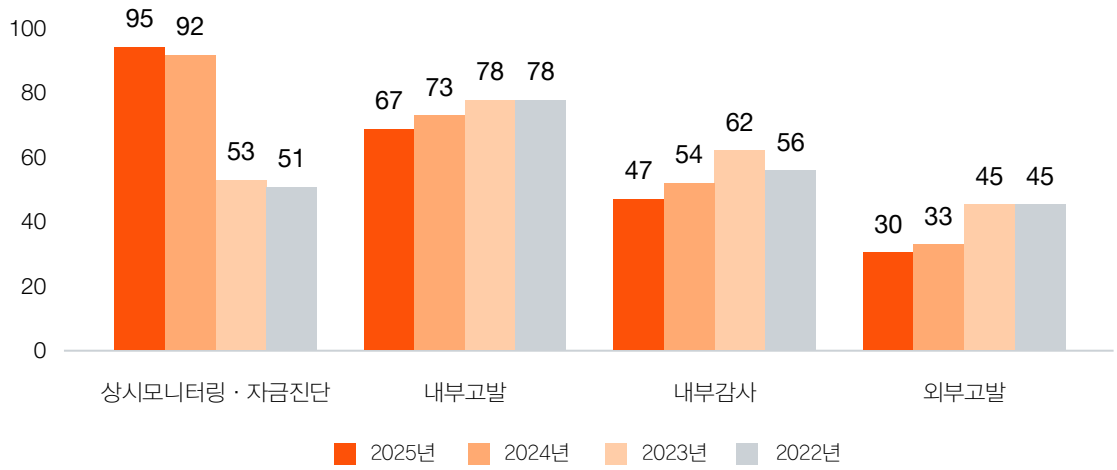
자산규모별 내부감사전문조직 설치 비율을 분석한 결과, 2조 원 이상 회사는 2025년 약 97%로 최근 4개년(2022~2024년) 동안 92~94% 수준을 유지하다가 2025년에는 소폭 상승하였다. 5천억 원 이상 회사는 약 69% 수준으로 전년과 동일한 수준을 유지하고 있다. 자산규모 5천억 원 미만 응답 기업의 경우 30%수준으로 매년 유사한 추이를 보이고 있다.

한편 최근 횡령 등의 부정 사건 그리고 이에 대응하는 사회적 책임 요구 및 상법개정 등 점차 기업 내부적인 통제를 강화하려는 움직임에 따라 실질적인 리스크 관리의 필요성은 증가하고 있다.

따라서 반드시 내부감사 조직이 아니더라도 자체적인 자정점검 기능에 대한 체계적인 프로세스 수립이 요구된다고 판단된다.

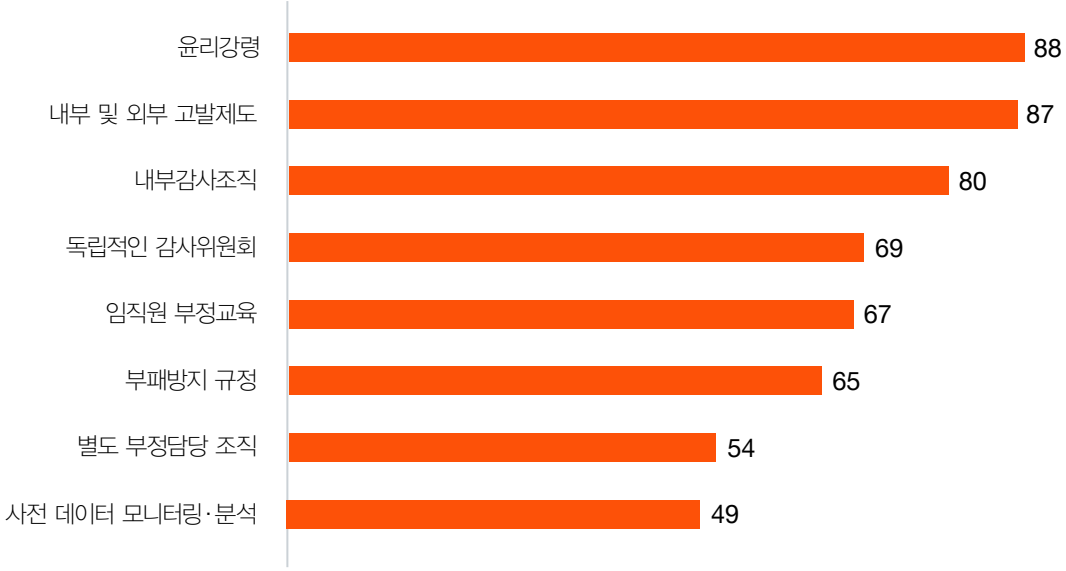
2. 운영 중인 부정 위험 관리 방안

도표 2. **운영 중인 부정위험 관리 방안** (단위: %)



운영 중인 부정 위험 관리 방안을 분석한 결과, 2025년에도 내부고발, 상시모니터링, 내부감사 순으로 가장 많은 회사에서 운영하는 것으로 나타났으며, 이는 전년과 유사한 흐름이다. 다만 4개년 추이를 보면 내부고발 비율은 2024년 약 73%에서 2025년 약 67%로 다소 감소, 내부감사 비율도 2024년 약 54%에서 2025년 약 47%로 다소 감소한 반면, 상시모니터링 및 자금진단 비율은 2024년 약 92%에서 2025년 약 95%로 증가하는 흐름을 보이고 있다. 이러한 증가는 최근 자금통제 공시 강화로 인해 다수의 회사들이 사전 예방차원의 상시모니터링 및 자금진단에 대한 높은 관심을 유지하고 있는 것으로 보인다. 또한 2025년은 의무적으로 대부분의 상장사가 자금통제 공시를 수행하면서 관련 통제를 개선한 효과가 반영된 것으로 보인다.

도표 3. **해외 부정위험 관리 방안** (단위: %)



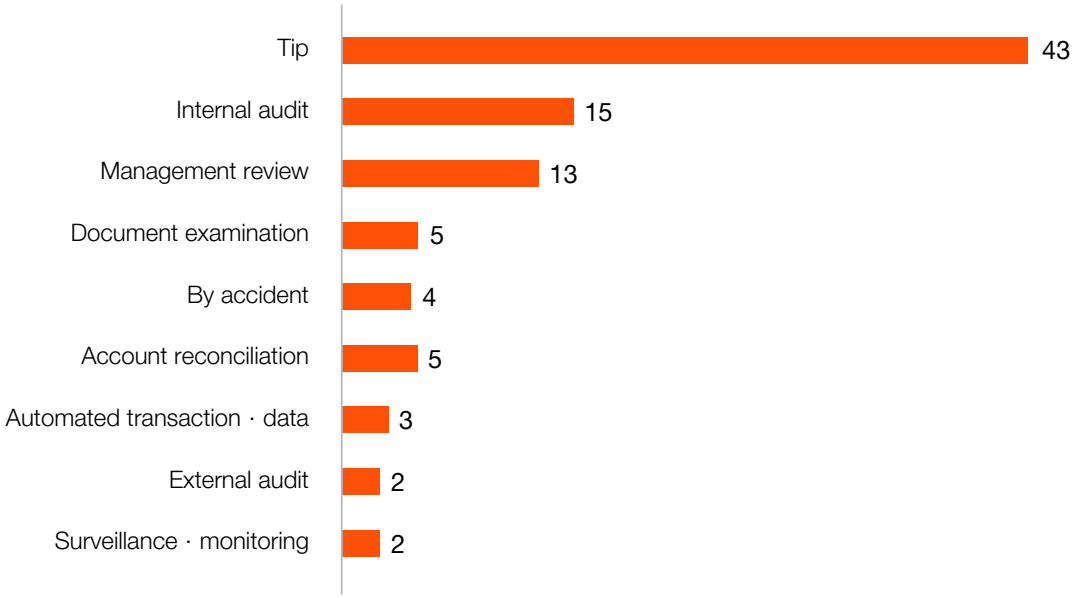
Source: ACFE, Occupational Fraud 2026 - A Report to the Nations, 2026, p.38 중 일부자료 발췌

최근 부정감사협회(ACFE) Occupational Fraud 2026 보고서에 따르면 해외 기업의 부정 위험 관리 방안은 윤리강령이 88%로 가장 보편적이며, 내부 및 외부고발제도, 내부감사조직, 독립적인 감사위원회 등이 상위권에 위치했다. 이는 국내 뿐만 아니라 해외에서도 기업 내부적으로는 윤리규범, 내부 및 외부고발제도, 내부감사 등이 가장 효과적인 부정위험 대응 방안으로 인식되고 있어 이에 대한 실효적인 운영이 강조된다.

특히, 내부 및 외부고발제도와 내부감사조직은 존재여부보다는 어떻게 실질적이고 실효적으로 제도 및 조직이 설계되고 운영되고 있느냐가 더 중요한 사항이다.

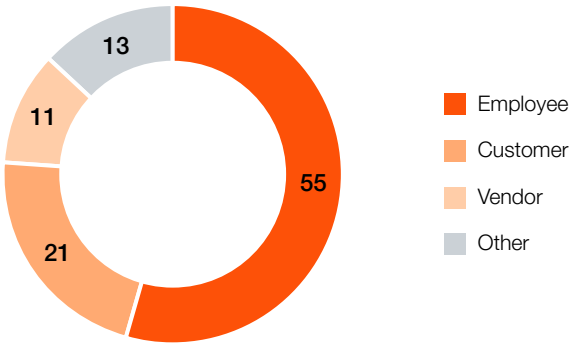
3. 부정적발 방법

도표 4. **해외 부정적발 방법** (단위: %)



Source: ACFE, Occupational Fraud 2026 - A Report to the Nations, 2026, p.24 중 일부자료 발췌

도표 5. **비율** (단위: %)



ACFE Occupational Fraud 2026 보고서에 따르면 실제 적발된 부정 중 내부고발(Tip)이 43%로 가장 많이 적발한 방안으로 조사되었으며, 내부감사가 15%로 2위, 경영진 검토가 13%로 3위를 유지하였다. 특히 내부고발 응답 중 직원의 비중이 55%로 가장 높았으며, Customer(21%), Vendor(11%) 등도 주요 정보 제공원이다. 흥미로운 점은 부정적발 자체는 제보를 통한 비율이 높으나 회사 자체적으로 능동적인 검토 조직을 갖춘 경우가 단순 제보에 의지하는 조직보다 부정 적발 가능성이 최대 4배 가량 높으며, 훨씬 조기에 적은 피해량으로 부정적발을 성공한 것으로 분석되었다. 위의 비율을 보아도 알 수 있듯, Tip을 제외하고 약 53%가 회사 자체적인 능동적인 적발 활동에 의해 발견되었다는 점을 알 수 있다. 따라서 실효적인 부정적발을 위해 Tip을 포함한 회사 자체적인 부정적발을 위한 실질적인 활동이 매우 중요함을 알 수 있다.

4. 내부고발제도 중 개선 필요사항

표 1. **내부고발제도 중 개선 필요사항**

구분	2025년	2024년
조사인원의 독립성	1순위	5순위
내부고발자 보호조치	2순위	4순위
인사조치의 투명성과 공정성	3순위	1순위
재발 방지 대책 마련	4순위	3순위
조사결과 보고의 투명성	5순위	2순위
조사인원의 전문성	6순위	6순위
내부고발 사건의 조직 내 공유	7순위	7순위
접수방식	8순위	8순위

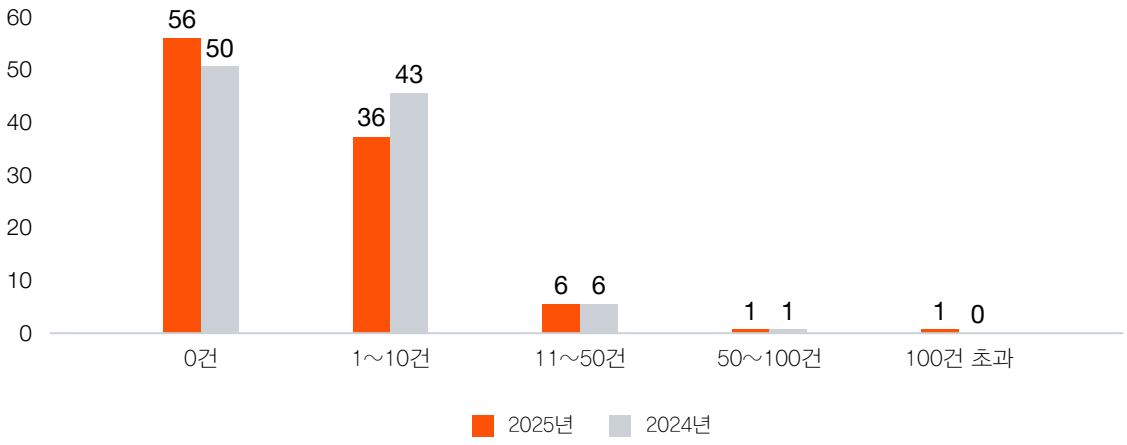
내부고발제도 개선에 가장 시급한 과제 분석 결과, 2025년 1순위는 '조사인원의 독립성'으로 나타났다. 이는 내부고발 접수 이후 조사 단계에서 조사자의 독립성·공정성에 대한 임직원들의 신뢰도 부족이 제도 실효성을 저해하는 핵심 요인으로 부상했음을 보여준다. 2순위는 '내부고발자 보호조치'로, 고발 이후 신분 보호 및 불이익 방지에 대한 신뢰도 제고 역시 중요한 개선 과제임을 확인할 수 있다.

내부고발제도의 실효성을 높이기 위해서는 전담 외부조사기관 활용, 감사위원회 직보 채널 운영 등을 통한 조사의 독립성 확보와 함께, 고발자 보호 절차의 구체화·공식화가 병행될 필요가 있다. 조사 과정의 독립성 부족은 잠재적 고발자의 신고 의지를 억제하는 선행 장벽으로 작용할 수 있어, 제도 설계 단계부터 독립적 조사 체계를 명문화하는 것이 우선 과제로 검토되어야 한다. 또한, 실효적인 재발방지 대책 마련, 사건 결과에 대한 명확한 설명과 후속조치 공지를 체계화하는 것도 내부고발제도가 실질적으로 운영되는데 중요한 요소이다.

최근 대내외 환경 변화 속에서 회사의 실질적인 부정위험 대응을 위해서 이러한 내부 및 외부 고발제도가 실효적으로 운영되도록 하는 임직원의 인식 전환과 기업 내부의 적극적인 노력이 필요한 시기이다.

5. 내부고발 건수 및 대륙별 현황

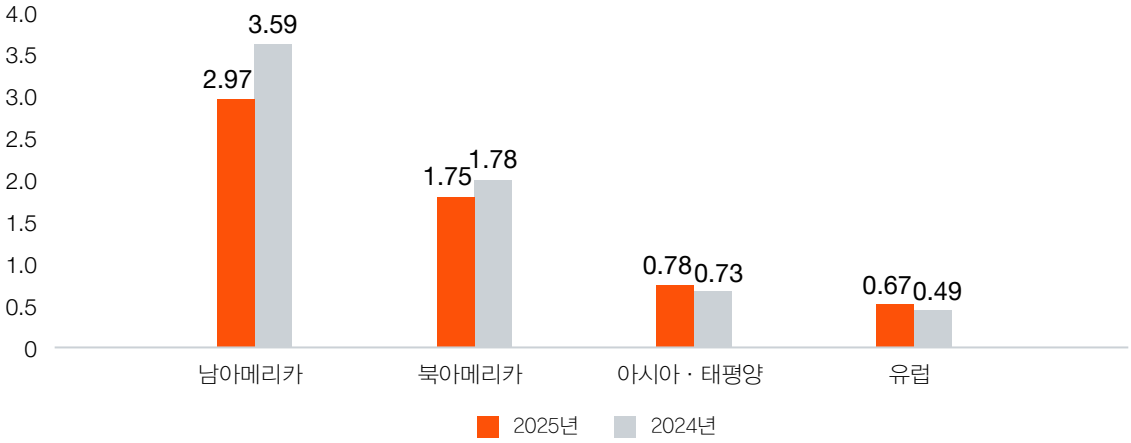
도표 6. **연간 내부고발 건수** (단위: %)



내부고발제도를 운영하고 있는 회사들의 연간 내부고발 건수를 질의한 결과 2025년에도 대부분의 회사(92%, 2024년은 93%)가 0건이거나 10건 이하로 발생 건수가 없거나 낮은 것으로 나타났다. 특히 0건이 약 56%로 전체의 절반 수준에 달하는 것은 내부고발제도가 존재는 하지만 실효성 있게 운영되지 않았음을 보여 준다.

특히, 최근 내부고발제도의 중요성이 높아지고 있는 사회적 분위기가 조성되고 있지만 내부고발제도의 개선 필요성 설문 응답결과에서 알 수 있듯이 여전히 조사인원의 독립성 및 내부고발자 보호조치 등이 미비한 사유로 기업의 내부고발제도가 실효적으로 운영되지 않고 있다는 것은 보여 준다. 이제는 내부고발제도의 개선및 고도화를 위해 국내 기업들의 지속적인 노력과 관심이 필요하다.

도표 7. **대륙별 임직원 100명당 고발 건수** (단위: 건수)



Source: NAVEX, Regional Whistleblowing & Incident Management Benchmark Report, 2025, p.7, 16

NAVEX 2025 Regional Whistleblowing Benchmark Report에 따르면 해외 임직원 100명당 내부고발 건수는 지역별 편차가 크지만 매우 높은 비율(남미 2.97건, 북미 1.75건, 아태 0.78건, 유럽 0.67건)을 보이고 있다. 특히 주목할 점은 유럽이 0.49 → 0.67건으로 큰 폭으로 증가한 점이다 (EU 내부고발자 보호 지침 시행 영향). 반면 남미는 3.59 → 2.97로 감소했으나 여전히 가장 높은 보고 수준이다.

보고서 내 흥미로운 점은 APAC은 유독 익명신고 비율이 높으며(APAC 67% vs 북미 52%), 신고되어 입증되어도 후속조치가 없는 비중이 20% 수준이라는 점이다. 북미와 유럽의 경우는 대부분이 조치된다는 점에서 대비된다.

이러한 통계치는 실질적으로 부정이 발생하여도 기업내에서 이를 덮는 경우가 적지 않아 제보자들로 하여금 제보의 동력, 즉, 부정을 적발할 기회를 잃게 만든다는 것이다. 윤리강령 및 교육을 더욱 강화하여 환경을 조성하고 실제 후속조치도 공정성 있고, 공개적으로 진행되어야 할 것이다.

6. 자금 관련 주요 통제활동

표 2. **자금 관련 주요 통제활동 운영 순위**

구분	2025년	2024년	2023년
자금일보에 대한 상위권자의 검토 및 승인	1순위	1순위	1순위
법인인감관리 (관리대장유지)	2순위	2순위	2순위
법인인감관리 (물리적보안)	3순위	4순위	4순위
OTP·공인인증서 관리	4순위	3순위	3순위
자금일보에 대한 상위권자의 주기적인 은행 잔액 대사	5순위	5순위	5순위
펌뱅킹·인터넷 뱅킹상에서 출금처리 시 2인 이상의 승인	6순위	6순위	5순위
주기적 또는 불시 기중은행거래 및 기말잔액 조회 수행	7순위	8순위	8순위
세부 업무 분장 (은행거래·전표 입력·승인·자금 집행 등)	8순위	7순위	7순위
주기적 또는 불시 거래처 채권·채무 기말잔액 조회 수행	9순위	9순위	9순위
자금담당자 신원조회	10순위	10순위	10순위
자금담당자의 주기적 교체	11순위	11순위	11순위
자금담당자에 대해 불시 휴가제도 등	12순위	12순위	13순위

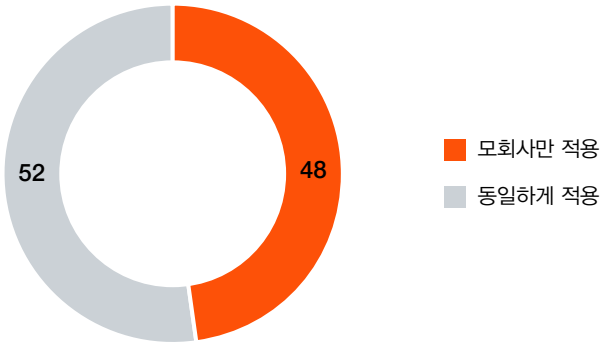
현재 수행 중인 자금 관련 주요 통제활동을 조사한 결과 2025년에도 전년과 유의미한 변경이 없음을 확인할 수 있다. '자금일보에 대한 상위권자의 검토 및 승인 – 1순위', '법인인감 관리(관리대장유지) – 2순위', '법인인감관리(물리적 보안) – 3순위', 'OTP·공인인증서 관리 – 4순위', '자금일보에 대한 상위권자의 주기적인 은행 잔액 대사 – 5순위' 등이 상위권을 유지하고 있다.

횡령 등 부정은 상존하는 잠재적인 위험이고 은밀하게 이루어진다는 점에서 불시 기중은행거래 및 기말잔액 또는 거래처 채권·채무 조회 등 이상징후에 대한 적극적인 모니터링 및 점검 등의 활동도 이러한 부정위험을 최소화하는데 도움이 될 수 있다.

자금관련 주요 통제활동은 통제의 존재 유무도 중요하지만 실효적으로 횡령 등 부정위험을 대응하도록 설계되었는지와 연간 지속적으로 예측 불가능성을 고려하여 적절하게 운영되는지에 대한 모니터링이 매우 중요한 사항이다.

7. 자금 관련 주요 통제활동 종속기업 확대 적용

도표 8. **자금 관련 주요 통제활동 종속기업 확대 적용 여부** (단위: %)



그룹관점에서 자금 관련 주요 통제활동의 종속기업 확대 적용 여부를 조사한 결과 2025년 응답 회사 중 약 52%가 동일하게 적용하고 있다고 응답한 반면, 약 48%는 모회사만 적용하고 있는 것으로 나타났다.

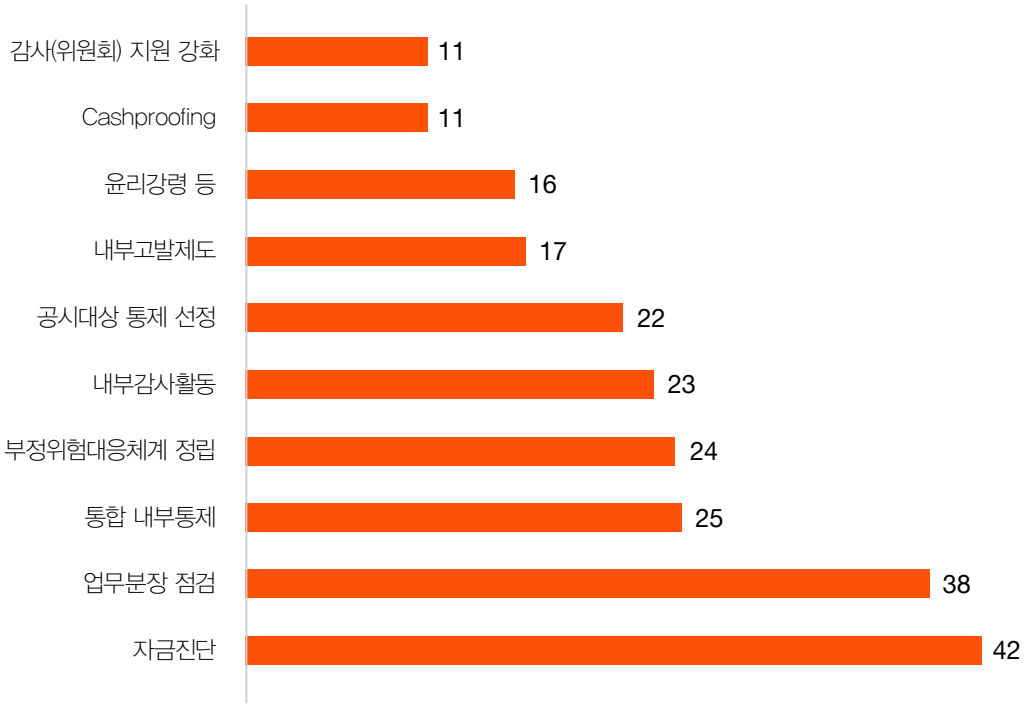
연결내부회계관리제도 뿐만 아니라 그룹관점에서 일관되고 체계적인 자금 관련 리스크를 관리하는 것은 매우 중요하고 이에 따라 모회사 뿐만 아니라 종속기업 전반으로 확대 적용하는 것은 최근 횡령사고 등이 빈번히 발생하는 상황에서 중요한 내역이다

이러한 상황에서도 종속기업에 확산하지 못하는 경우가 있는 경우는 종속기업의 인프라 및 역량 등의 미비한 면이 주요 사유일 것이다. 상대적으로 종속기업, 특히 해외 종속기업의 경우는 소규모 인원 및 권한의 집중 등으로 인한 업무분장의 취약, 국내와 상이한 자금이체 환경, 다수의 수기 조정 등으로 인해 횡령 등 부정위험이 더 높은 경우가 많고 그룹의 관리 측면에서 가시성이 떨어지는 경우가 많다.

통제는 위험에 대응하고자 수행하는 것으로, 위험에 기반하여 그룹 및 각 종속기업에 맞는 실질적인 횡령 등 부정위험에 대응하는 자금통제를 구성하고 운영할 수 있도록 기업의 많은 노력과 관심이 필요한 시점이다.

8. 점검·개선 고려 영역

도표 9. **2026년 부정위험 및 자금통제 공시 점검·개선 영역** (단위: %)

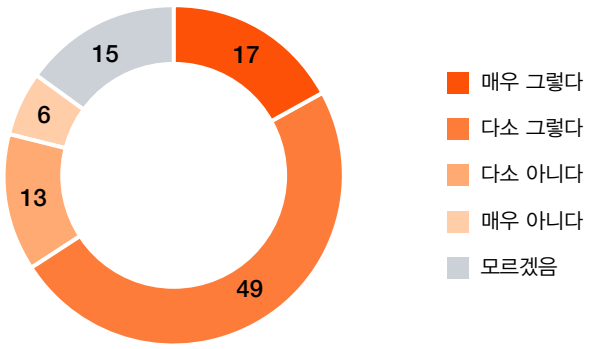


2025년부터 부정위험 및 자금통제 공시가 적용된 상황에서 관련 대응을 위해 점검 혹은 개선을 고려하는 영역을 질의한 결과, 2025년 자금진단(42%)이 가장 높은 응답률을 유지하였고, 업무분장 점검(38%), 통합 내부통제(25%), 부정위험대응체계 정립(24%), 내부감사활동(23%), 공시대상 통제 선정(22%) 등이 상위권에 위치한다. Cash Proofing은 11%로 상위 그룹보다는 낮으나 자금 진단과 함께 실질적인 자금 리스크 파악 수단으로 활용되고 있다.

회사들이 부정위험 및 자금통제 공시 대응을 위해 승인 위주의 통제 뿐만 아니라 자금진단 및 Cash Proofing 등의 자금프로세스 점검, 데이터 분석과 업무분장 점검 등을 통한 예외사항 파악 및 개선 활동 등을 통해 부정위험 및 자금과 관련한 실질 리스크를 관리하고자 하는 움직임으로 보여 진다. 부정위험대응체계 정립, 내부감사활동 및 통합 내부통제의 경우도 상위권에 위치한 점은 최근 회사의 지속가능한 성장과 존속을 위해 재무보고 목적의 내부통제와 운영 및 법규 준수 목적의 내부통제를 통합적으로 운영하는 것이 중요함을 보여 준다.

9. 운영 및 법규 준수 목적의 내부통제

도표 10. **운영 및 법규 준수 목적 내부통제를 통합 운영시 실질적인 리스크 관리에 실효적인지 여부** (단위: %)



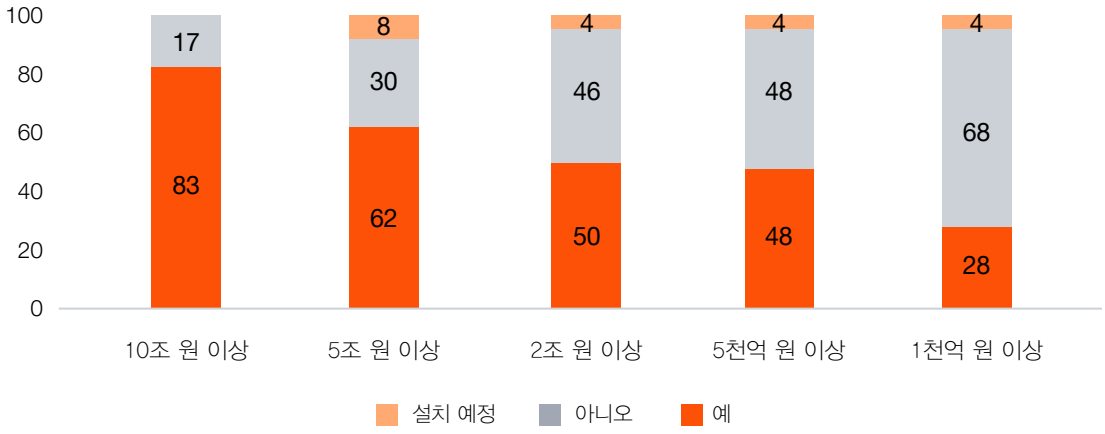
재무보고 목적의 내부통제인 내부회계관리제도 뿐만 아니라 운영 및 법규 준수 목적의 내부통제를 통합하여 운영 시 실질적인 전사 리스크 및 부정위험 대응 효과에 긍정적으로 답한 비율이 전체의 66%에 달한다. 최근 다수의 사건사고로 인한 기업들에 미치는 치명적인 영향, 상법 개정 등으로 소송 리스크 등 증대, 중대재해처벌법 등 법규 미준수에 대한 제재 강화 등 운영 및 법규준수 목적의 전사 리스크 관리체계 즉, 통합내부통제에 대한 관심이 높아지고 있음을 보여 준다.

이제는 재무보고 목적의 내부통제인 내부회계관리제도를 확대하여 전사적인 리스크 관리체계(통합 내부통제)의 정립 및 운영을 통해 기업의 지속가능한 성장 및 존속과 실질적인 리스크 관리에 대한 기업의 Due Care를 입증하는 체계를 내재화는 것이 중요한 시기이다.

신규 규제 환경 인식 현황

1. 전사 리스크 관리 총괄 부서

도표 1. **전사 리스크 관리 총괄 부서 존재** (단위: %)

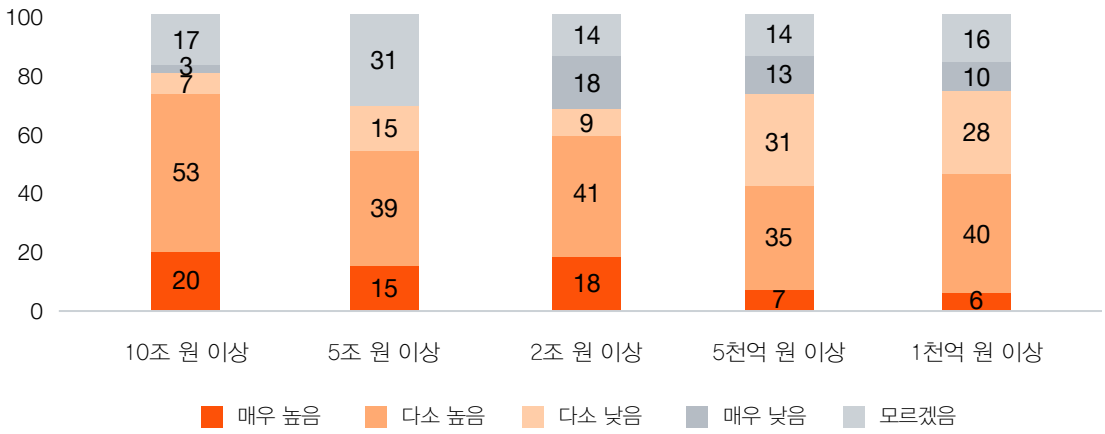


전사 리스크 관리를 위한 총괄 부서(Compliance 부서, 내부통제부서, 리스크 관리부서 등 명칭 무관)의 존재 여부를 조사한 결과, 회사 규모가 클수록 별도의 전사 리스크 관리 총괄 부서를 운영하는 비율이 높게 나타났다. 반면 중소규모 회사에서는 별도의 전사 리스크 관리 부서를 운영하지 않거나, 내부감사·재무 부서가 리스크 관리 기능을 함께 수행하는 경우가 상당하다.

전사 리스크 관리체계는 재무보고 목적의 내부통제인 내부회계관리제도를 넘어서 운영 목적 및 법규준수 목적의 리스크를 통합적으로 관리하는 핵심 체계이다. 최근 다수의 사건사고로 인한 기업들에 미치는 치명적인 영향, 상법 개정 등으로 소송 리스크 등 증대, 중대재해처벌법 등 법규 미준수에 대한 제제 강화 등의 리스크 및 관련 규제 환경이 빠르게 변화하는 상황에서 실질적인 전사 리스크 관리를 위해 부서별 분절된 리스크 관리가 아닌 전사 리스크 관리 총괄 부서를 통한 통합된 리스크 관리가 더욱 중요해지고 있다.

2. 상법 개정

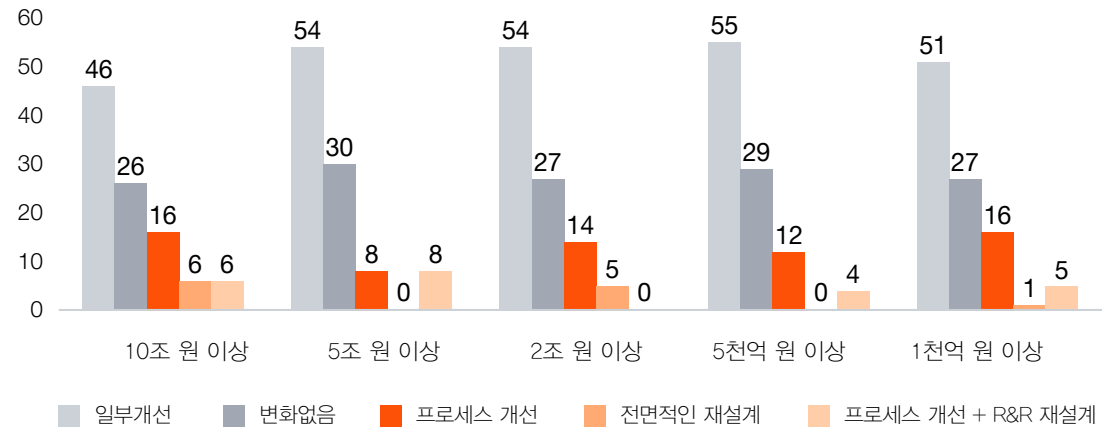
도표 2. **상법개정 거버넌스 영향** (단위: %)



상법 개정이 회사의 거버넌스(이사회·감사기구) 및 내부통제 운영에 미치는 영향을 평가한 결과, 응답 회사의 다수가 '다소 높음' 또는 '매우 높음'으로 답변하였다. 특히 자산규모 10조 원 이상 회사에서는 '매우 높음'과 '다소 높음' 응답 비율이 73% 수준으로 가장 높게 나타났으며, 회사 규모가 클수록 상법 개정의 영향을 더 크게 인식하는 경향이 확인된다.

이는 대규모 상장회사일수록 이사회 및 감사위원회 운영, 주주총회 의결권 행사, 내부거래 공시 등 상법 개정 사항이 거버넌스 운영에 직접적으로 미치는 영향이 크기 때문으로 해석된다. 한편 10조 원 미만 회사에서도 '매우 높음'과 '다소 높음' 응답 비율이 과반 정도 수준이며, 이는 회사 규모와 무관하게 상법 개정에 대한 영향 평가 및 대응 방안 마련이 필요함을 시사한다. 특히 상법 개정 내용이 전사 리스크 관리체계 정립과 이사회 의사결정의 정당성 확보라고 하는 중요한 과제를 회사에 준 상황에서 이에 대한 회사들의 구체적인 대응과 체계 정립이 필요한 시기이다.

도표 3. **상법개정 내부통제 변화 계획** (단위: %)

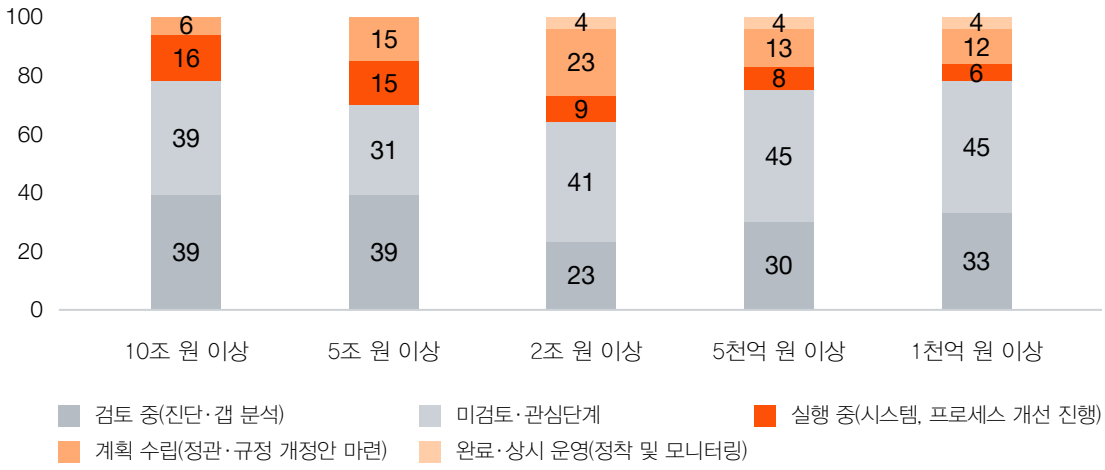


상법 개정에 따른 회사 전사 내부통제에 실질적 변화나 개선 계획 여부를 조사한 결과, 모든 자산 규모에서 70% 이상의 기업이 일부개선을 포함한 개선 계획을 가지고 있는 것으로 파악된다.

상법 개정은 단순한 법령 준수 차원을 넘어 회사의 거버넌스 구조, 이사회 운영, 감사기구 독립성 등 전사 내부통제 체계 전반에 영향을 미치는 사안으로 단순한 정관 변경 수준이 아닌 실질적인 운영 체계의 점검 및 개선이 필요하며, 향후 외부감사인 및 감독당국의 관심 영역이 될 가능성이 높아 사전적인 준비가 권장된다.

상법 개정으로 인해 요구되는 전사 리스크 관리체계 정립 및 이사회의 의사결정 정당성 확보는 결국 현업부서를 포함한 전사적인 체계 정립과 개선 노력을 필요로 하는 중요한 사항이므로 경영진 및 이사회를 포함한 기업의 적극적인 관심과 진행이 필요하다.

도표 4. **상법개정 공식 과제·로드맵** (단위: %)

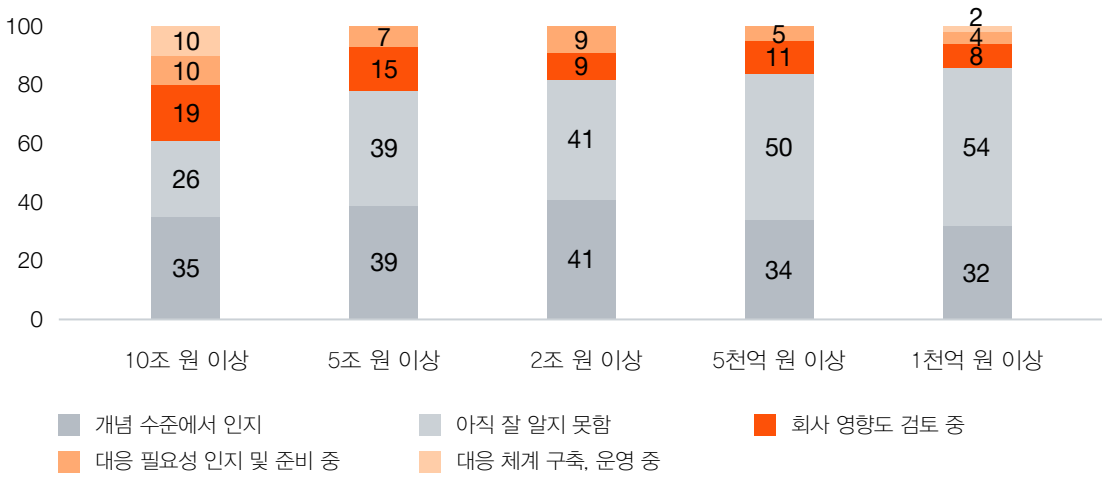


상법 개정 대응을 공식 과제로 정의하고 로드맵 또는 프로젝트로 추진 중인지 조사한 결과, 응답 회사의 과반 이상의 비율이 이미 완료, 실행 중, 계획 수립 및 검토 중 등 적극적인 관심과 관련된 추진 활동을 진행 중인 것으로 나타났다. 회사 규모가 클수록 공식 과제 정의 및 로드맵 추진 비율이 높게 나타나는 반면, 회사 규모가 작을수록 회사는 미검토 및 관심단계에 머무르고 있는 비율이 높다.

상법 개정의 영향은 거버넌스·내부통제·공시 등 다영역에 걸쳐 있어 일회성 대응이 아닌 내재화를 위한 중장기 로드맵 수립이 효과적이다. 사외이사 비율 강화, 감사위원회 독립성 확보, 이사회 운영 절차 정비 등 실질적 변화를 위해 공식 프로젝트화 및 경영진의 관심과 자원 배분이 필요하다.

4. AI 기본법

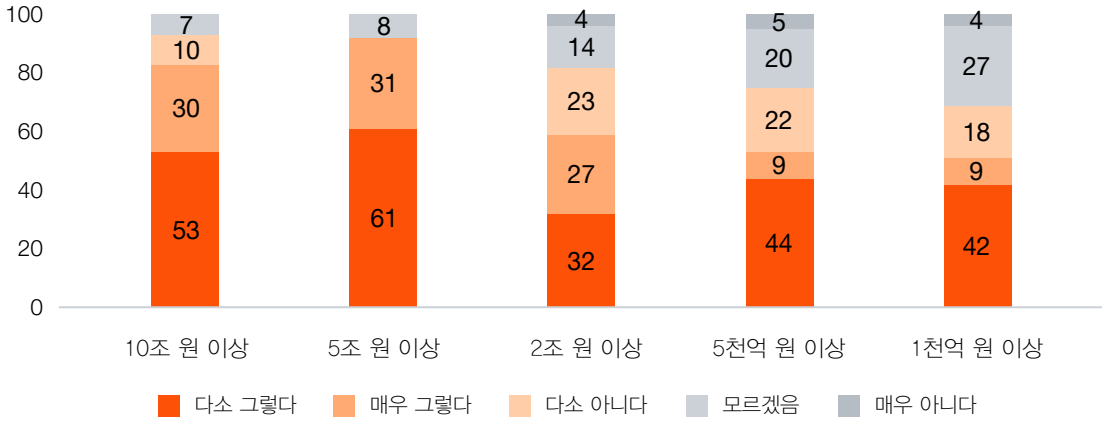
도표 5. **AI 기본법 인식 수준** (단위: %)



AI 기본법에 대한 회사의 현재 인식 수준을 평가한 결과, '개념 이해 단계'에 머무르는 회사가 가장 많은 비중을 차지하였으며, '실질적 대응 준비 단계'에 도달한 회사는 일부에 그쳤다. 회사 규모가 클수록 인식 수준이 상대적으로 높은 경향이 확인된다.

AI 기본법은 AI 시스템의 개발·활용에 대한 안전성 확보 및 윤리적 사용을 규율하는 신규 규제로, AI 도입이 확대되는 내부회계관리제도 영역에서도 향후 직접적인 영향이 예상된다. 특히 AI를 활용한 자동통제, 이상거래 탐지, 운영평가 자동화 등의 영역에서 AI 시스템의 신뢰성·설명가능성·편향성 관리 등이 새로운 통제 영역으로 부상할 가능성이 있어, 인식 단계를 넘어 사전적 준비가 필요한 시점이다.

도표 6. **AI 리스크 내부통제 인식** (단위: %)

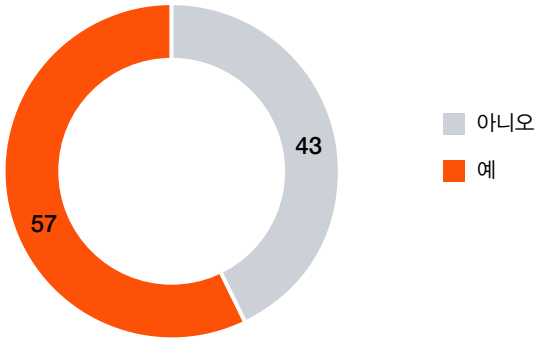


AI 사용과 관련된 리스크를 내부통제 또는 리스크 관리 대상으로 인식하고 있는지 조사한 결과, 회사 규모에 따라 인식 수준의 격차가 확인된다. 대규모 회사일수록 AI 리스크를 내부통제 대상으로 인식하는 비율이 높은 반면, 중소규모 회사에서는 아직 일반 리스크와 구분되지 않거나 별도 관리 대상으로 인식되지 않는 경우가 다수이다.

AI 리스크는 알고리즘 편향, 데이터 품질, 모델 안정성, 설명가능성 등 전통적 IT 리스크와는 구분되는 특수성을 갖고 있다. AI 활용이 단순한 업무 도구를 넘어 의사결정 지원 영역으로 확대됨에 따라 AI 리스크에 대한 별도의 평가·관리 체계 수립이 향후 내부통제의 핵심 과제로 부상할 것으로 예상된다.

5. 정보보호 공시

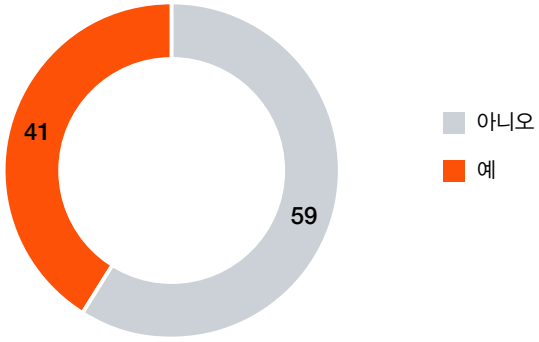
도표 7. **정보보호 공시 의무대상 확대 인식** (단위: %)



정보보호 공시 의무대상이 2027년부터 전체 상장사 등으로 대폭 확대되는 것에 대한 인식 여부를 평가한 결과, 응답 회사 중 57%만 이를 인식하고 있는 것으로 나타났다.

정보보호 공시는 단순한 정보 제공을 넘어 회사의 정보보호 거버넌스 및 통제 체계의 적정성을 대외적으로 공시하는 제도로, 공시 정확성 확보를 위한 내부통제 체계가 필수적이다. 2027년 의무대상 확대 시점이 임박한 가운데 사전적인 인식 제고와 준비가 시급하며, 특히 중소규모 상장사의 인식 강화가 필요하다.

도표 8. **정보보호 공시 정확성 내부통제** (단위: %)



정보보호 공시 정확성 확보를 위한 내부통제 절차(예: 기초자료 완전성 확인, 제3자 검토 등)가 설계 및 운영되고 있는지 조사한 결과, 응답 회사 중 41%만이 관련 내부통제 절차를 설계 및 운영 중이라고 답변하였다. 회사 규모가 클수록 관련 내부통제 운영 비율이 상대적으로 높으나, 전반적으로 정보보호 공시 정확성 확보를 위한 통제 체계는 초기 단계에 머무르고 있다.

정보보호 공시는 ESG 공시·자금통제 공시 등과 마찬가지로 공시 데이터의 정확성과 신뢰성이 중요한 영역이며, 향후 외부감사 또는 인증 대상으로 확대될 가능성도 있다. 따라서 정보보호 공시 데이터의 기초자료 완전성, 산출 로직 검증, 책임자 검토 등 공시 정확성을 확보하기 위한 내부통제 절차의 사전적 설계 및 운영이 권장된다.

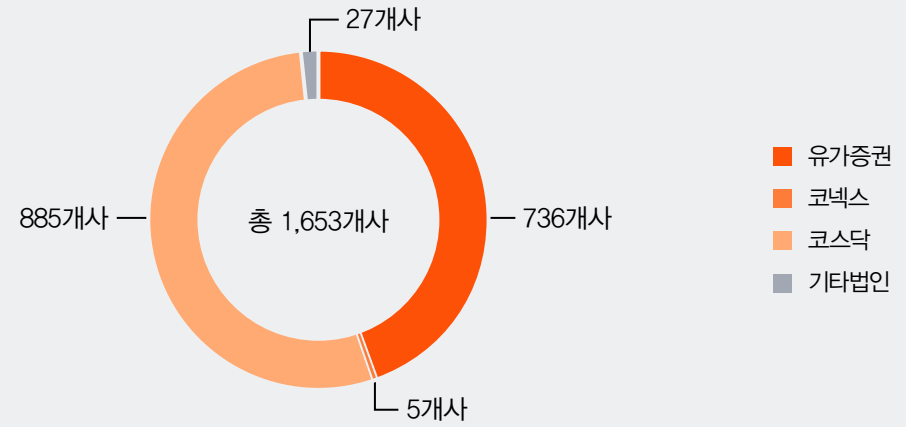
2025년 자금통제 공시 분석 및 시사점

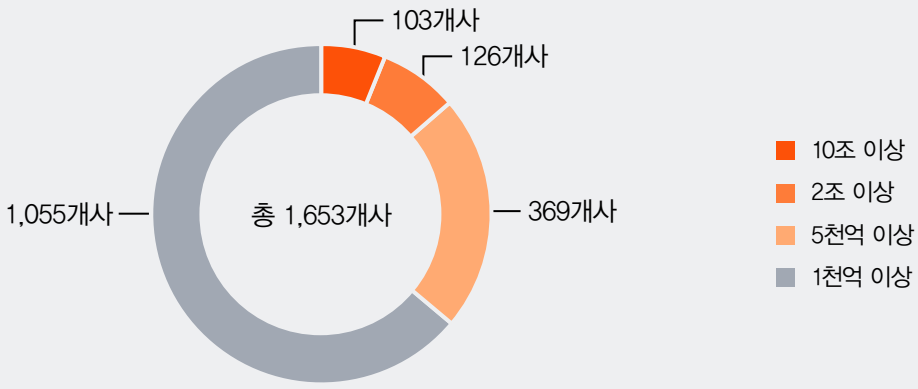
부정위험 평가 및 자금통제 공시 강화가 2025년 1년 유예를 거쳐 2025년 1,000억 이상 상장자 전체로 확대되었다. 실제 공시된 내역을 분석하고 그 시사점을 알아보고자 한다.

1. 자금통제 공시 현황

- **2025년 말 기준 자산규모 1,000억 이상의 상장사 및 기타주요법인 1,653개사에 대한 분석을 수행하였다.**

도표 1. **요약** (단위: 개사)





2. 자금통제 공시 분석

- 공시된 통제 현황을 분석하면 다음과 같다.

도표 2. **공시 항목별 구분** (단위: %)

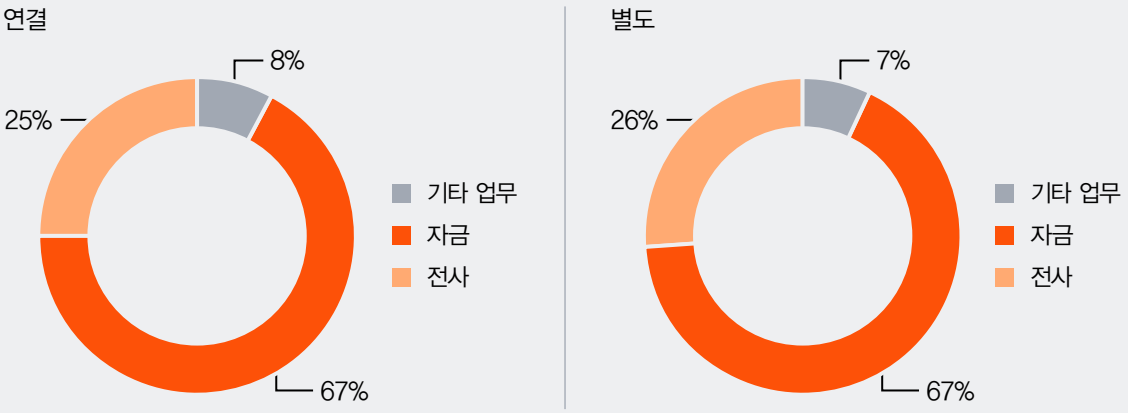
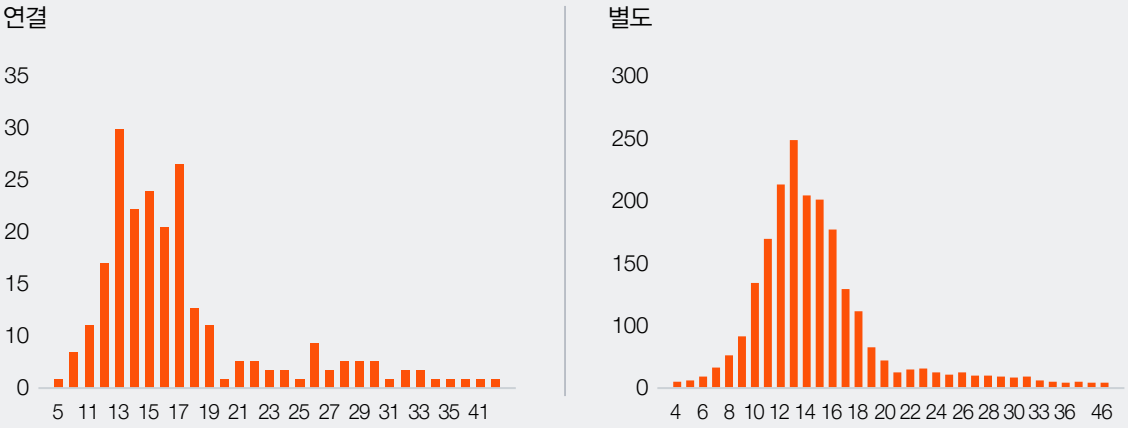


도표 3. **연결 및 별도 개수 분포** (단위: 개수)



- 평균적으로 별도의 경우 14개의 통제를 공시하였으며, 연결의 경우 17개의 통제를 공시하였다. 대부분의 경우 연결은 종속회사의 통제를 추가하는 경향이 있어 별도 대비 연결의 공시 개수가 증가한 것으로 보인다.

3. 2024년 공시 내역 vs 2025년 공시 내역

- **전기 공시를 수행한 상장사 31곳 중 2곳은 합병등의 사유로 2025년 공시가 수행되지 않았다. 따라서 총 29개사를 대상으로 통제활동 변동 내역을 확인하였다.**

표 1. **2024년 vs 2025년 공시 내역** (단위: 개사)

연결

구분	2024년	2025년	증감
전사	97	94	(3)
자금	255	264	9
기타업무	30	27	(3)
합계	382	385	3

별도

구분	2024년	2025년	증감
전사	106	102	(4)
자금	285	292	7
기타업무	38	35	(3)
합계	429	429	–

- **전체적으로 전기 대비 거의 변동은 없는 것으로 확인되었다. 다만 문구를 다듬어 회사별 특색을 보이기보다 일반화하여 통제를 표현하는 방식으로 변경된 것들이 다수 존재하였다. 실질적인 추가·삭제 사항은 다음과 같다.**

– **전사수준 통제활동:** 내부회계관리제도 평가 보고 및 전결관리 등의 통제활동이 삭제되었다. 금융감독원 공시사례에 맞추어 공시가 진행된 것으로 판단된다.

– **자금 통제활동:** 미등록 계좌 이체 제한, Vendor master 생성 변경 검토, 휴면계좌 모니터링 통제 등이 주로 추가되었다.

– **기타업무:** 위탁재고 실사 등 회사별 특성이 존재하는 통제활동들이 재고실사로 통합되는 등의 조정이 나타났다.

4. 산업별 공시 현황

- **각 산업별로 통제 분류에 따른 경향을 검토한 결과 대체로 유사하였으며, 금융감독원의 공시사례를 준용하였기 때문으로 보인다. 다만 금융사의 경우 기타업무 지주사의 경우 자 공시가 전체적인 경향 대비 높게 나타났다.**

표 2. **산업별 공시 현황** (단위: 개수, %)

산업 구분	공시회사 수	전사	자금	기타 업무
소비재	886	27%	65%	8%
기술 및 통신	304	28%	65%	7%
제약바이오	133	28%	64%	8%
수주	117	27%	67%	6%
금융	87	28%	54%	18%
지주	55	28%	68%	4%
에너지	41	29%	63%	8%
엔터 및 게임	30	28%	65%	7%
합계	1653	28%	64%	8%

- **전체적인 비율은 유사하나 구성내역은 각 산업별로 특색이 보이는 경우가 존재하였다. 관련 통제활동이 비중이 산업별로 높은 경우를 고려하였다.**

– **소비재산업:** 자금지급보류 승인, 출하물량 검토 통제 → 실물 판매 방식의 산업특성 그리고 다수의 B2B 거래처에 대한 자금거래가 타 산업군 대비 빈번하기 때문으로 보인다.

– **기술 및 통신산업:** 예산한도 내 자금 집행 통제 → 프로젝트 업무를 영위하는 경우가 다수 존재하여, 전체적인 예산 내 활동관리가 중요하기 때문으로 보인다.

– **제약 바이오산업:** 출고 승인 및 미등록거래처에 대한 출고 제한 → 타 산업 대비 재고의 출고가 바로 현금화 가능하고 유통구조가 복잡한 편이여서 출고와 관련한 통제활동이 단순 재고통제가 아니라 '부정·자금유출 리스크 방지' 관점과 연계가 된 점이 반영된 것으로 보인다.

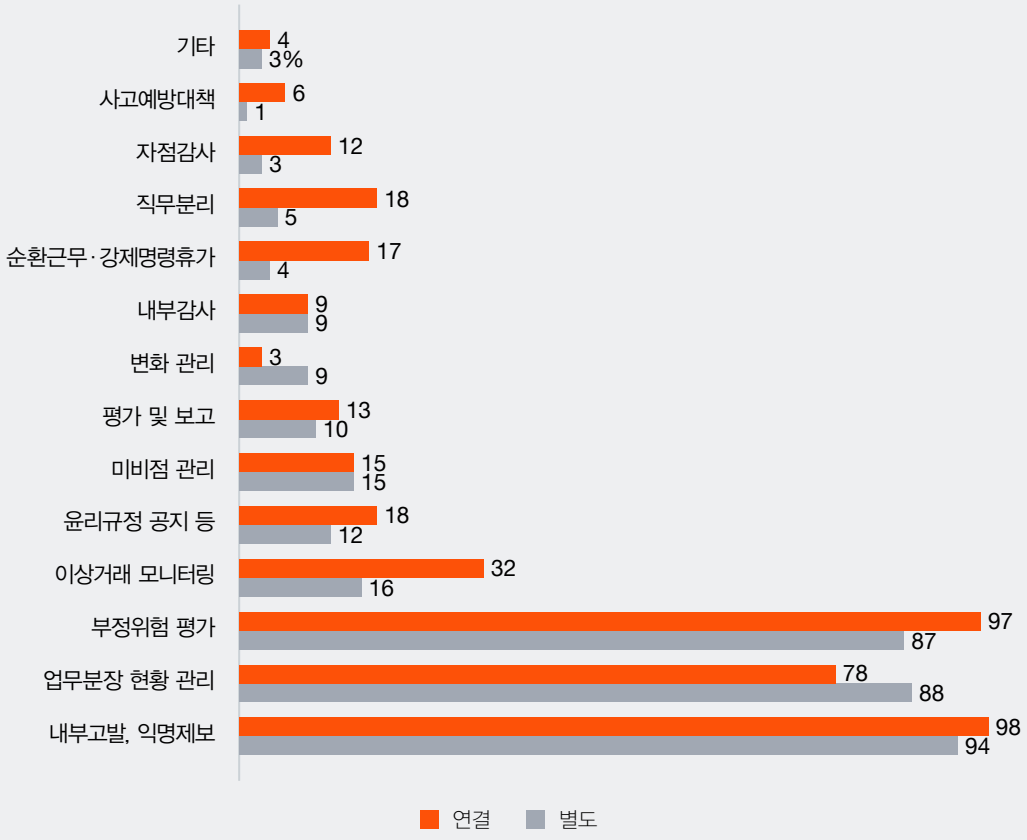
– **수주산업:** 해외지사 자금 모니터링 관리, 전도금 관리 → 수주 산업의 특성상 해외 지사 등 사업현장이 해외에 다수 분포해 있고, 장기간 프로젝트가 진행되어 해외지사 혹은 사업장에 대한 자금리스크 관리가 중요한 특성이 반영된 것으로 보인다.

– **금융산업:** 여신 관련 통제, 수신업무 통제, 파생상품 거래 승인 통제 → 금융업의 특성이 반영된 통제활동이 다수 포함되어 있다. 금융업의 경우 금융감독원 공시 사례 또한 별도로 존재하는 만큼 타 산업 대비 차이점이 명확히 나타났다.

- **지주회사:** 차입원리금 상환 승인 → 지주사의 특성상 투자가 활성화 되어 있고, 이에 따른 자금 조달은 항상 동반되므로, 이에 대한 사후관리 통제가 타 산업대비 횡령 등 부정위험관련 자금통제에서 중요한 항목이므로 높은 비율로 공시되었다.
- **에너지산업:** 자금 관련 시스템 접근제한, 권한부여 승인, 중복거래방지 → 에너지산업의 경우 다른 산업 대비 대규모·집중화된 조직, 대량 반복 거래가 많은 환경이어서 사람보다 시스템 통제가 더 중요한 경우가 많으며 권한 관리 실패 시 부정 영향 범위가 매우 큰 산업이다. 따라서, 에너지 산업은 거래 규모와 시스템 의존도가 높아, 사람 중심 매뉴얼 통제보다는 '권한·시스템 중심 통제'가 더 중요하게 여겨지며 접근제한·권한승인·중복거래 방지가 관련한 가장 핵심적인 사항인 점이 반영된 결과로 보여진다. 특히 권한 부여 승인 통제의 경우 자동통제의 신뢰성을 높일 수 있는 시작이라는 점에서 타 산업군에서도 주요공시 통제로 충분히 고려할 수 있는 성격이라고 판단된다.
- **엔터 및 게임산업:** 예산한도 내 자금 집행, 법인카드 관련 통제 → 엔터·게임 산업은 '프로젝트·비용 중심 산업'이라서, 자금 통제의 핵심이 '지출 통제(예산·카드)'에 집중되기 때문에 예산한도 및 법인카드 등에 대한 관리가 타 산업군 대비 높은 경향을 보인다. 즉, 엔터·게임 산업은 '돈을 어떻게 벌까'도 중요하지만 '비용을 얼마나 통제할 수 있느냐'가 핵심이기 때문에, 자금통제도 예산과 법인카드 중심으로 설계되는 경향이 있다.

5. 전사수준 통제 공시 현황

도표 4. **전사수준 통제활동 공시율** (단위: %)



- **업무분장, 내부고발 및 부정위험평가는 90% 수준으로 공시되었다. 그외 순환근무 강제명령휴가, 직무분리, 지점감사 등은 금융업에서 대부분 공시가 수행되었다. 거의 대부분의 경우 연결에서 공시비율이 높게 나타나고 있는데 이는 연결의 경우 2조 이상 상장사에서 공시를 진행하여 상대적으로 통제 인프라가 잘 갖추어져 있기 때문으로 판단된다.**

- **주요 통제별 공시 특성 및 고려할 사항**

– **내부고발제도:** 공시 사례들을 보면 '부정 방지 제도 운영'을 제목으로 하고 있으나, 익명성 등 실질적인 운영을 언급하지 하지 않는 사례들이 특히 별도 법인 공시 내역에 존재하였다. 이는 각 사에서 아직 실질적인 운영이 활성화되지 않아, 표현의 수위를 낮춘 것으로 판단된다. 익명 제보는 전사수준 통제활동에서 회사의 부정 방지를 위한 가장 직접적이고 강력한 통제인 점을 고려할 때 더욱 활성화가 필요할 것으로 여겨진다.

– **부정위험 평가:** 부정위험 평가 공시내역을 살펴보면 재무제표가 왜곡표시 될 위험과 부정위험은 다른 영역임에도 다수의 공시 사례에서 이를 혼용하는 경우가 많았다. 부정위험평가는 내부감사팀과 내부회계관리제도 전담팀 모두가 수행해야 하는 업무로 여겨진다. 그러나 실무적으로 소규모 법인일수록 이러한 평가에 소극적인 경향이 있다. 이로 인해 일반적인 위험평가를 준용하여 기재한 것으로 여겨진다.

– **(상시) 모니터링:** 모니터링 관련된 내역 또한 부정위험평가와 비슷한 공시양상을 보였다. 모니터링 관련 실제 공시사례는 이상거래가 아닌 대부분 통제수행활동여부에 대한 모니터링이었으며, 내부감사 수행에 대한 언급 또한 적지 않았다. 이상거래 모니터링은 범위가 광범위하여 선뜻 회사가 나서서 시스템을 구축하기에는 어려울 수 있다.

  실질적인 모니터링을 수행한다고 공시한 비율은 자산규모별로 차이가 컷는데, 10조 이상 54%, → 1천억 이상 13% 수준으로 나타났다. 어떤 특정한 광범하고 치밀한 계획하에 이상거래를 모니터링 해야 한다고 생각할 수 있으나, 특정한 지점 몇 개 포인트만을 1년에 한 번씩 점검하는 것 또한 큰 의미가 있을 수 있다. 외국 사례에서 보듯, 기업이 적극적으로 부정징후에 적극적인 절차를 수행하는 경우 적발 시점이 최대 4배가 앞당겨지고, 피해규모 또한 훨씬 낮아진다는 보고가 존재한다.

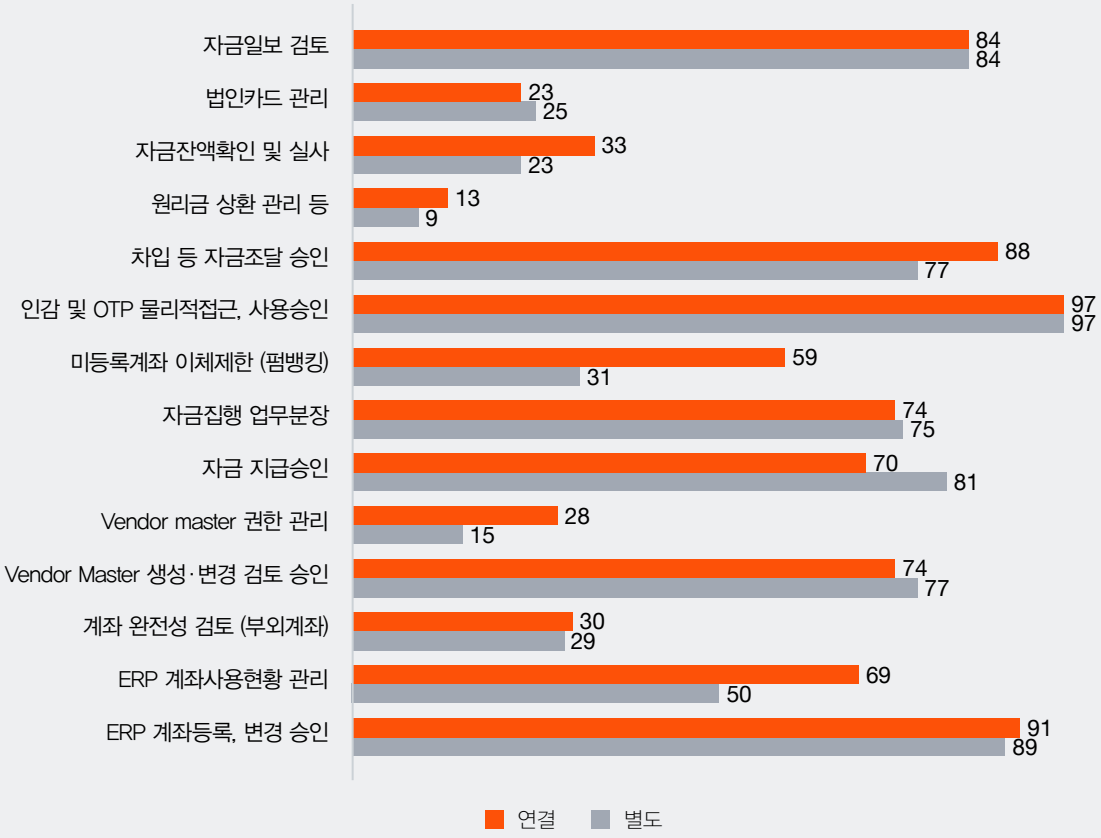
  따라서 이상징후 모니터링은 많은 자본적 지출을 수반하는 것이 아닌 단순한 점검부터 그 시작이며, 1회라도 하는 것과 전혀 하지 않는 것은 부정을 방지 효과에 있어 그 차이는 상당할 것으로 여겨진다.

– **순환근무·강제명령휴가:** 과거 사례로 볼 때 부정이 발생하는 경우 대부분이 특정인원이 특정 역할을 지속적으로 수행함에 따라 장기간 은폐가 가능하였기에 발생한 사건이 대부분이었다. 본 통제활동의 공시는 거의 대부분 금융산업에서 진행 되었는데, 자산 규모 별로 편차가 존재하였다. 10조 이상의 경우 90% 수준, 1천억 원 이상 10% 수준이었다. 부정은 발생한 사건을 조사하는 것보다 예방이 중요한 점을 고려할 때 위험을 근본적으로 낮출 수 있는 예방통제활동에 대해 자산규모 및 산업군과 무관하게 더욱 관심을 가질 필요가 있다.

6. 자금통제 공시 현황

(1) 자금 관련 일반 주요 통제 활동

도표 5. **전사수준 통제 활동 공시율** (단위: %)



- **자금일보, 인감 관련 통제의 경우 거의 대부분의 회사에서 수행하고 있는 것으로 파악 되었다. 전반적으로 거래 단위의 통제, 일단위의 통제는 높은 수준의 공시율을 보였으나, 운영현황을 모니터링하는 통제의 경우는 공시 비율이 전반적으로 낮았다.**

- **주요 통제별 공시 특성 및 고려할 사항**

– **부외계좌 검토:** 회사의 ERP에 등록되지 않은 계좌를 모니터링하는 통제로 모든 금융회사를 토대로 계좌 리스트를 조회하고 회사가 보유하고 있는 계좌리스트와 대사하는 통제이다. 공시 내역 상 계좌의 완전성을 언급한 통제는 다수 존재하나, 구체적인 검증 방법론에 있어 ERP상 계좌리스트와 금융기관 잔고증명서를 대사하는 경우 대부분이었다. 이는 계좌의 실재성을 검토하는 방법이며, 완전성 검토 효과는 제한적일 수 있다. 각 회사별 여건에 따라 부외계좌 모니터링에 어려움이 있을 수 있다. 그러나 연 1회 이상 검증을 수행한다면, 발생할 수 있는 사고를 미연에 최소화 혹은 방지 할 수 있을 것이다.

- **ERP 계좌사용현황 관리:** 사용현황은 결국 입금전용, 출금전용, 미사용계좌를 검토하고 사용 용도에 맞게 관리가 되고 있는지, 미사용계좌는 예측불가능한 이슈를 사전에 방지하고자 해지하였는지를 검토하는 절차이다. 부외계좌와 마찬가지로 대부분의 회사가 계좌검토 관련 공시는 진행하였으나, 용도에 대한 세밀한 점검에 집중하지 않고 잔액만을 맞춰보는 통제의 공시가 주를 이루었다. 미사용계좌를 논외로 하더라도 입금전용, 출금전용 계좌의 관리 중요한 사유는 각 계좌별 이체권한 관리가 현실적으로 어려울 수 있기 때문이다.

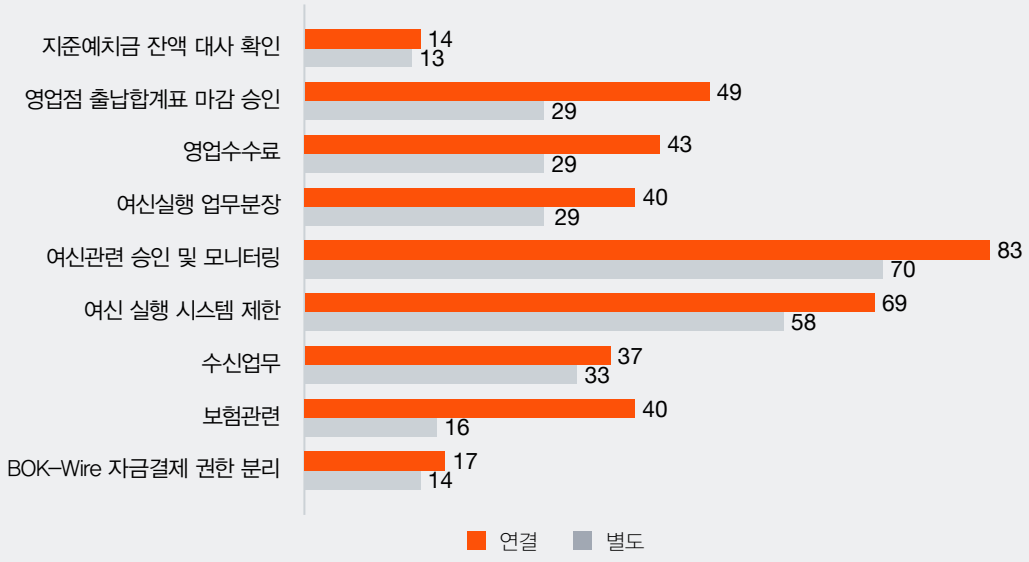
  이런 경우를 방지할 수 있는 것이 처음부터 해당계좌 자체가 출금이 되지 않도록 설정하는 것이다. 본 통제는 사용현황은 이러한 원칙이 지켜지고 있는지 또는 거래 및 금융기관과의 이해관계로 관리범위에서 벗어난 계좌가 있는지를 검토하여 발생할 수 있는 부정위험을 사전에 차단할 수 있으므로, 부외계좌 대비 공수는 적으면서 위험을 확실히 방지할 수 있는 소위 가성비가 높은 통제로 여겨진다.

- **미등록계좌 이체 제한:** 본 통제는 자동통제의 영역으로 자금 관련 사고를 근본적으로 차단할 수 있는 통제이다. 시스템이 구비되어야만 정상적인 운영이 가능하며, 2조 원 이상 자산규모를 분기점으로 2조 원 이상 그룹은 50% 이상, 미만 그룹을 36%, 25% 수준이었다. 회사의 영업방식 상 이를 운영하는데 애로사항이 있는 경우도 존재할 것으로 사료된다. 한편 펌뱅킹을 활용하지 않더라고 인터넷뱅킹 또한 계좌를 지정하여 관리할 수 있을 것이다. 비단 회사의 시스템이 반드시 선결 조건은 아닌 것이다.

- **계좌 등록 변경 승인:** 본 통제는 ERP에 또는 각 사 관리하는 별도의 계좌 Master에 대한 등록 승인 통제로 판단된다. 즉, Master 관리 통제이다. 그러나 많은 회사에서 이 통제와 계좌개설·해지 통제를 명확히 구분하여 공시하지 않았다. 계좌개설은 원시거래라면, Master 관리는 이후 반복적으로 발생하는 거래의 위험을 낮추기 위한 사전 통제이다. 2개를 하나의 통제로 운영하기 보다는 각각 구분하여 Test 하는 것이 각각 본연의 목적에 맞다고 여겨진다.

(2) 자금 관련 금융산업 특화 주요 통제활동

도표 6. **금융산업 주요 통제활동 공시율** (단위: %)



• **주요 통제별 공시 특성 및 고려할 사항**

– **여신실행 업무분장:** 여신실행 업무분장의 경우 별도 30%, 연결 40% 수준이다. 여신실행 업무분장의 경우 이미 많은 회사에서 단독처리 자체가 시스템으로 관리되어 여러 단계를 거쳐 확정되므로 업무분장 통제활동이 회사의 시스템적 관리현황을 고려했을 때 유의미하지 않다고 판단했을 것으로 여겨진다.

그러나 모든 통제활동은 특정 위험에 대한 검토가 수반되어야 하며, 회사의 영업실적 및 부정위험에 직접적인 영향을 주는 여신 실행 업무분장에 대한 시스템 상 가능여부에 대한 면밀한 검증이 필요하다고 판단된다.

– **지준예치금 잔액 대사 확인:** 일부 은행업 쪽에서만 공시를 진행하였다. 그러나 보험업등 다른 금융업종 또한 책임준비금 등 유사제도가 존재할 것이다. 금융감독원 공시 사례에 영향을 받은 것으로 판단되는 바, 통제는 위험에 대응한 활동으로 결국 금융업에서 지준예치금은 보통명사로 판단하여 각 회사가 법에서 요구받고 있는 고객관련 지급 준비 또는 책임 준비 등의 목적을 갖는 잔액 대사 통제의 공시를 고려할 필요가 있다.

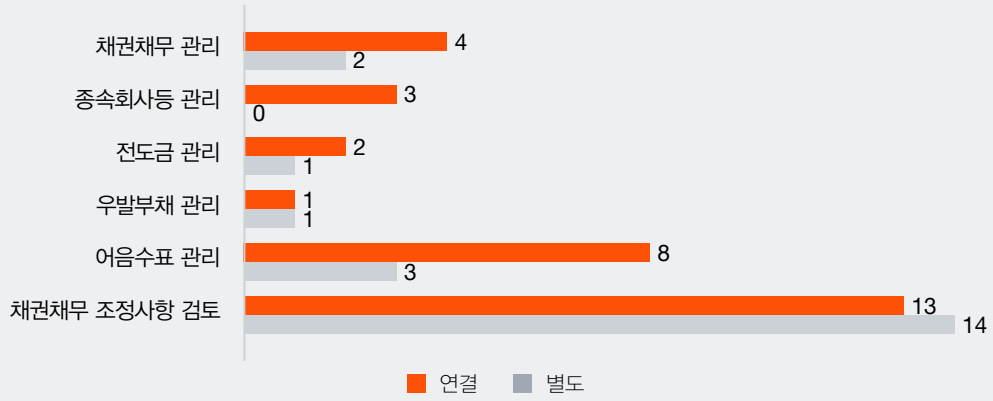
– **BOK-WIRE 자금결제 권한 분리:** 거래수준 통제활동은 광범위한 위험을 대응하는 것이 아닌 특정 위험을 구체적으로 정의하고 이에 대응한 통제를 설계하고 평가해야 한다. 각 회사에서 이미 다양한 루트로 자금결제 권한을 분리하고 있을 것으로 판단된다. 그러나 권한 분리 내역 중 BOK-WIRE 자금결제가 별도의 프로세스로 다루어진다면, 별도의 통제로서 공시 필요여부에 대한 고려가 필요하다.

– **영업수수료 관련 통제:** 영업수수료는 상대적으로 소규모로 다수에게 지급되는 회사의 비용성격으로 비단 금융회사 뿐만 아니라 일반회사에서도 이를 소재로 부정사건은 얼마든지 발생할 수 있다. 또한 다양한 종류의 영업수수료가 존재하고 매 시점별로 산정기준이 지속적으로 변경되어, 관리가 필요한 항목이다.

– **보험금 수납관련 통제:** 금융업은 다수의 보험사가 존재하여 이러한 현황이 반영된 결과이다. 대형 금융사의 경우 보험사를 종속회사로 두고 있는 경우가 많아 연결 40%, 별도 16%의 공시율이 보였다. 각 금융업에서는 보험금 수납 프로세스를 별도의 자금 프로세스로 인식하고 있다는 점을 확인할 수 있으며, 광의의 자금프로세스가 아닌 프로세스 단위별로 위험을 식별하여 설계된 통제로 판단된다.

(3) 기타 자금 통제 공시 현황

도표 7. **기타 자금 통제활동 공시율** (단위: %)



- **기타 항목들이므로 각 통제의 특성 보다는 모든 회사에서 다시한번 고려하면 좋은 통제활동을 언급한다.**

- **주요 통제별 공시 특성 및 고려할 사항**

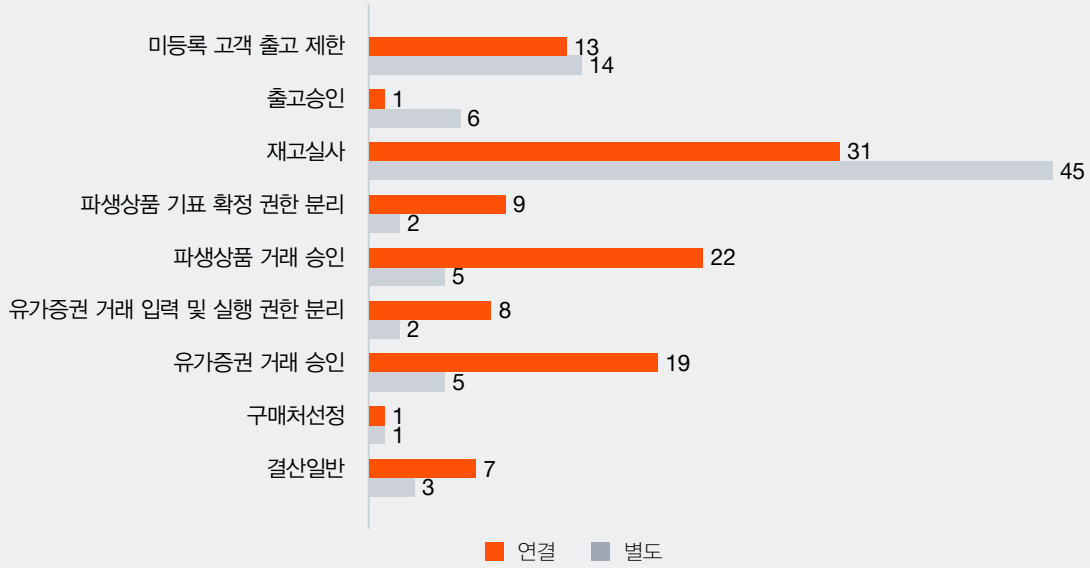
– **종속회사 등 자금관리현황 검토:** 일부 연결회사에서 종속회사 관리 통제활동을 공시하였다. 비단 종속회사 뿐만이 아니라, 국내외 사무소, 지점 등 각종 형태로 본사 외부에 존재하나, 평가대상 범위에 속하는 영역들이 있을 것이다. 본사의 규모 대비 이들 회사들의 규모는 작다. 따라서 경상적인 테스트 시 모집단에 포함이 되어도 평가되지 않거나, 혹시 모집단 자체에서 제외되어 있는 경우도 허다하다. 공시한 회사들은 이러한 문제점을 인지하고 이를 개별 모집단을 구성하고 통제를 테스트하였을 것이다.

이는 실무적으로 놓치기에 매우 쉬운 부분이다. 또한 별도이든 연결이든 모두 해당하는 사항이다. 따라서 각 자금 통제 평가 시, 특히 설계평가 시 회사 안에서 발생하는 모든 자금거래 형태에 대해서 회사의 통제가 적용되고 평가되고 있는지 반드시 확인해야 할 필요가 있다.

– **우발부채관리:** 회사에 잠재적인 피해를 줄 수 있는 약정사항에 대한 검토 통제가 소수의 회사에서 공시되었다. 대부분의 경우 우발부채는 계약조건에 따른 검토가 통제의 대상이지 우발부채의 약정사항을 검토하는 활동을 통제로 식별한 회사는 적은 것으로 여겨진다. 문서화 부담과 자금부정에 직접적으로 관련이 있는지에 대한 고민 있었을 것으로 여겨진다. 그러나 금액적으로 중요하고 복잡한 거래일수록 부정과 오류의 위험은 상존할 수 밖에 없다. 따라서 최소한의 검증절차를 별도로 테스트하는 것으로 고려할 필요가 있을 것이다.

7. 기타 업무 수준 통제 공시 현황

도표 8. **기타 업무 통제활동 공시율** (단위: %)



- **일반적인 거래수준프로세스에서는 재고실사 및 재고출고 관련 통제가 압도적으로 비율이 높았다. 자금 이외 직접적으로 사외 반출이 가능하고 환급성이 높은 재화에 해당하여 중요도가 높기 때문으로 여겨진다.**

- **주요 통제별 공시 특성 및 고려할 사항**

– **결산일반 등 통제활동:** 자가승인 전표 모니터링, 전표입력과 승인 업무 분장, 결산체크리스트 승인 등, 일반적인 FR(재무보고)프로세스의 통제활동들의 공시가 1,000억 이상 일부 법인들에서 확인되었다. 이러한 통제들은 일반적인 위험에 모두 대응하는 통제이다. ELC가 전사수준에서 위험을 통제하는 영역이면, FR프로세스는 업무수준프로세스의 일반위험을 모두 포괄하는 프로세스이다. FR프로세스의 통제활동이 담당하는 여러 영역 중 일부가 부정과 관련되어 이를 부정 대응 통제로 판단가는 경향이 있다. 그러나 특정한 위험에 직접대응하고, 구체적인 통제 즉, 부정을 예방하기 위해 무엇을 하였는지 명확히 확인할 수 있는 통제를 설계 및 운영하는 것이 부정을 예방하고 관리하는데 더 효율적일 것이다.

8. 연결 vs 별도 비교 분석

표 3. **연결공시법인 대상 연결 VS 별도 비교** (단위: %)

산업군	회사 수	별도 통제합계	연결 통제합계	별도 평균 (건/사)	연결 평균 (건/사)	평균 증감	연결 확대/축소
소비재	93	1019	1028	11.0	11.1	0.1	▲연결확대
금융	36	585	640	16.3	17.8	1.5	▲연결확대
지주	17	182	186	10.7	10.9	0.2	▲연결확대
기술 및 통신	16	189	186	11.8	11.6	−0.2	▼연결축소
에너지	14	152	149	10.9	10.6	−0.2	▼연결축소
수주	11	127	118	11.5	10.7	−0.8	▼연결축소
제약바이오	5	53	57	10.6	11.4	0.8	▲연결확대
엔터 및 게임	3	33	33	11.0	11.0	0.0	동일
합계	195	2340	2397	12.0	12.3	0.3	▲연결확대

- **총 8개의 산업군으로 분류하여 공시 통제 수를 검토한 결과 금융산업군을 제외하고는 대부분 대동소이하였다. 각 세부적인 통제활동을 확인하바 산업별로 특성이 엿보였는데 특징은 다음과 같다.**

- **주요 특성 및 고려할 사항**

– **소비재 산업:** Vendor Master 통제의 경우 모회사에서는 공시하였으나, 연결에서 제외된 경우가 가장 많았다. 반대로 ERP계좌사용현황은 증가하였는데, 통제의 신뢰성 관점에서 채택가능한 부분을 공시한 것으로 여겨진다.

– **금융 산업:** 금융산업의 경우 보험업 및 캐피탈등 다양한 산업을 영위하는 경우가 많아 가장 많은 증가를 보였다. 특히 채권채무조정, 여신실행시스템제한, 파생상품 거래승인등의 통제가 별도 대비 연결 공시에서 많은 증가를 보였다.

– **지주 산업:** 미등록계좌 이체제한, 부정위험평가 등이 증가 하였는데, 사업을 영위하지 않은 경우 많은 지주사의 특성 상 다양한 산업군을 종속회사로 두고 있어 대표적인 종속회사들의 자금 관리 통제를 추가한 것으로 보인다.

– **수주 산업:** 세부적으로 가장 많은 변동을 보였다. 별도의 경우 전도금 등의 관리통제가 촘촘하게 공시가 이루어진 반면 연결 공시의 경우 자금 모니터링 등 종속회사 관리 방식으로 통제가 통합되는 경향을 보였다.

- 전반적으로 연결공시 대상 법인들의 별도 공시내역을 비교한 결과 유의적인 차이는 없었다. 다만 연결 관점에서 추가되는 산업에 대한 공시가 추가되었으며, 별도 목적으로 유효하나 연결 목적으로 유효하지 않다고 판단되는 경우(실제 연결집단 내 운영되지 않는 통제인 경우)에는 제외한 것으로 여겨진다.

- 연결 공시가 각 종속회사의 합산을 기준으로 작성되다 보니 위와 같은 현상이 나타나는 것은 자연스러운 결과일 것이다. 다만, 연결관점에서 그룹을 모니터링하는 통제들도 공시된다면 전체적인 완전성이 더욱 높아질 것으로 여겨진다.

9. 주요 시사점 요약

- **부정위험 평가:** 회사 통제 수행 환경이 결정되는 핵심 통제이다. 금번 공시 내역을 검토한 결과 부정위험 평가와 관련하여 공시 사례만을 놓고 보았을 때, 직접적인 부정위험에 대응하기 보다는 내부회계관리제도 전반을 운영하는 과정에서 파악되는 부정을 검토하는 사례가 많았다. 부정은 거래의 유형이 아니며, 다양한 요소들이 겹쳐서 발생하는 위험 또는 사건이다. 따라서 전사수준에서 다양한 요소를 고려하여 통제 운영 전 사전 위험 평가를 수행하는 것은 매우 중요한 업무이다. 이 과정을 통해 잠재적인 부정위험의 징후를 파악하고 그 결과로서 식별된 세부 위험별로 거래수준통제활동 설계하여 방어할 수 있기 때문이다.

- **내부감사와의 직접적인 소통의 중요성:** 대부분의 통제활동의 내부감사 관련된 기술을 보면 내부감사팀의 독립적 업무만을 언급하고 있다. 내부감사는 부정과 직결된 업무를 수행하므로 내부통제활동에 부정의 요소가 적절히 고려되려면, 내부감사팀과의 효과적인 커뮤니케이션은 필수이다. 비단 내부감사팀 뿐만 아니라 조직간 사일로 현상을 방지하고 효과적으로 정보가 공유되도록 시스템을 갖추어야 부정을 효과적으로 예방할 수 있다.

- **승인 통제** vs **모니터링 통제:**

표 4. **공시 통제 Top 5**

구분	전사수준	자금
1순위	내부고발, 익명제보	인감 및 OTP 물리적접근, 사용승인
2순위	업무분장 현황 관리	ERP 계좌등록, 변경 승인
3순위	부정위험평가	자금일보 검토
4순위	이상거래모니터링 (300건 미만)	자금 지급승인
5순위	직무분리 (100건 미만)	Vendor Master 생성·변경 검토 승인

- 위의 전사수준과 자금관련 통제 Top 5를 보면 대부분이 승인 중심의 통제활동이다. 전사수준의 경우 4위인 이상거래모니터링은 3위인 부정위험평가 대비 1,100여건이 차이가 난다. 자금의 경우 계좌사용현황, 계좌완전성검토 통제들은 순위권에 없다.

- 최근 발생하고 있는 부정사례를 보면 승인자체를 우회하거나, Blind approval이 발생하여 부정을 놓치는 경우가 많다. 거래 단위 승인 통제는 부정을 직접적으로 예방하는데 이미 한계를 보이고 있다. 내부회계관리제도가 2019년에 감사로 전환되어 어느덧 7년의 지났다. 대부분의 회사는 통제가 어느정도 안착되었을 것으로 여겨진다. 좀 더 발전적인 내부회계관리제도나 내부통제의 운영을 위해서 모니터링과 관련된 통제활동이 활발히 논의되는 분위기가 조성되었으면 한다.

- 자산규모별 통제현황: (금융산업 제외)

표 5. **자산규모별 전사수준, 자금 공시율**

구분	10조 이상	2조 이상	5천억 이상	1천억 이상
전사수준	78%	75%	71%	71%
자금	75%	71%	67%	63%

- 대표적인 통제들을 기준으로 공시율을 검토한 결과 자산 규모에 따라 공시율은 반비례하였다. 그러나 내부회계관리제도 상의 통제로 식별되지 않았을 뿐 모든 회사들은 각 회사별 절차가 존재한다. 이는 내부회계관리제도를 고려하지 않더라도 각 사의 상황에 맞추어서 위험을 고려한 결과 일 것이다. 자산규모 별로 통제수준의 차이는 필연적일 것이나, 한편으로는 자산규모에 작을수록 내부회계관리제도 구축 당시 간소화한 방식을 채택한 결과가 현재 자산규모별로 통제 공시율이 반비례한 사유 중 하나 일수도 있을 것이다. 내부회계관리제도는 지속적으로 유지 관리가 수반되어야 효과적으로 운영될 수 있다. 시작은 회사의 현실적 운영 포인트에 맞추어 졌다면 앞으로는 식별되는 위험에 대한 각 회사 역량에 맞는 통제를 운영하는 방향으로 포인트가 맞추어지길 기대한다.

02

내부회계관리제도 의견변형

- 내부회계관리제도 의견변형에 대한 분석
- 경영진과 감사(감사위원회)의 고려사항

Executive Summary

본 보고서는 2019년 이후 최근 7개년간 국내 상장회사의 내부회계관리제도 의견변형 현황을 공시자료에 기반하여 분석하고, 이를 토대로 경영진과 감사위원회에서 고려해야 할 시사점을 정리하였다. 분석 결과, 내부회계관리제도 의견변형은 제도 도입 초기의 일시적 현상이 아니라 여전히 지속되는 구조적 신호로 확인되며, 취약점의 중심은 단순 부정 방지보다 재무보고 통제의 설계 및 운영, 손상평가, 계속기업, 특수관계자거래, 투자자 약정 등 판단과 추정이 개입되는 영역으로 이동하고 있다. 또한 외부감사인이 핵심감사항목으로 식별한 영역과 내부통제 미비가 상당 부분 중첩되고, 내부회계관리제도 비적정의견이 재무제표 감사의견 및 사후 상장폐지 위험과도 일정 수준 연계된다는 점에서, 내부회계관리제도는 더 이상 형식적 준수 이슈가 아니라 기업 리스크 관리와 재무보고 신뢰성의 핵심 관리과제로 보아야 한다. 본 보고서는 2026년 5월 15일 기준으로 조회된 자료를 바탕으로 작성되었다.

핵심 시사점 1. 의견변형은 감소보다 구조적 취약성에 주목해야 한다

최근 7개년간 내부회계관리제도 의견변형 회사 수는 대체로 유사한 수준에서 증감을 반복하고 있으며, 2025년의 일부 감소만으로 구조적 개선을 단정하기는 어렵다. 특히 코스닥시장에서는 자산규모 1천억원 미만 기업에 의견변형이 집중되는 반면, 유가증권시장에서는 규모가 큰 기업도 복잡한 사업구조와 판단 영역 확대로 인해 취약점이 지속적으로 식별되고 있다. 이는 내부회계관리제도 리스크가 단지 중소형 회사 고유의 문제가 아니라 기업 규모에 따라 서로 다른 형태로 나타나는 구조적 이슈임을 보여준다.

핵심 시사점 2. 취약점의 중심이 판단·추정 영역으로 이동하고 있다

공시된 의견변형 사유를 보면 오류 관련 통제가 전체의 큰 비중을 차지하고 있으며, 그 중에서도 재무보고 통제활동의 설계 및 운영 미비가 핵심 이슈로 부각된다. 회계처리 및 재무제표 구성요소별로는 손상평가, 계속기업, 특수관계자거래, 종속·관계기업 투자, 투자자 약정 등 경영진의 판단과 추정이 크게 개입되는 영역에서 통제 미비점이 반복적으로 나타난다. 이는 내부회계관리제도의 관리 초점이 단순한 증빙 확보나 사후 수정 대응을 넘어, 주요 회계판단의 근거·검토·승인·모니터링 체계까지 확장되어야 함을 의미한다.

핵심 시사점 3. 내부회계관리제도 이슈는 재무제표 감사와 거버넌스 이슈로 연결된다

핵심감사항목과 내부통제 미비는 절반 수준에서 중첩되며, 특히 손상평가, 특수관계자거래, 부정사건 등은 높은 연계성을 보인다. 또한 내부회계관리제도 비적정의견 회사 중 상당수는 재무제표 감사의견도 비적정의견으로 나타났고, 과거 의견변형 회사 일부는 이후 상장폐지로 이어졌다. 반면 경영진 및 내부감시기구의 자체평가와 외부감사인의 최종 판단 사이의 일치율은 여전히 낮아, 기업 내부의 리스크 인식과 외부 검증 결과 사이에 유의미한 간극이 존재한다. 이는 내부회계관리제도가 회계부서만의 과제가 아니라 경영진, 감사위원회, 내부감사, 외부감사인이 함께 다루어야 할 거버넌스 의제임을 시사한다.

경영진 및 감사위원회에 대한 시사점

첫째, 경영진은 내부회계관리제도를 단순한 준법 또는 감사 대응 체계로 보지 말고, 재무보고 리스크를 사전에 식별·평가·통제하는 경영관리 체계로 재정의할 필요가 있다. 둘째, 감사위원회는 자금통제나 전표 점검 수준의 확인을 넘어, 손상평가, 계속기업, 특수관계자거래, 투자자 약정 등 판단영역에 대해 어떤 통제가 설계되어 있고 실제로 어떻게 운영되는지 질문할 수 있어야 한다. 셋째, 기업은 외부감사인이 주목하는 핵심감사항목과 내부통제 취약영역을 분리해서 보기보다, 양자를 통합한 리스크 맵을 구축하여 경영진 보고와 감사위원회 감독에 활용할 필요가 있다. 향후 내부회계관리제도의 실효성은 통제의 존재 여부보다 판단영역에 대한 통제의 정합성, 증빙 가능성, 지속가능한 운영 수준에 의해 좌우될 것이다.

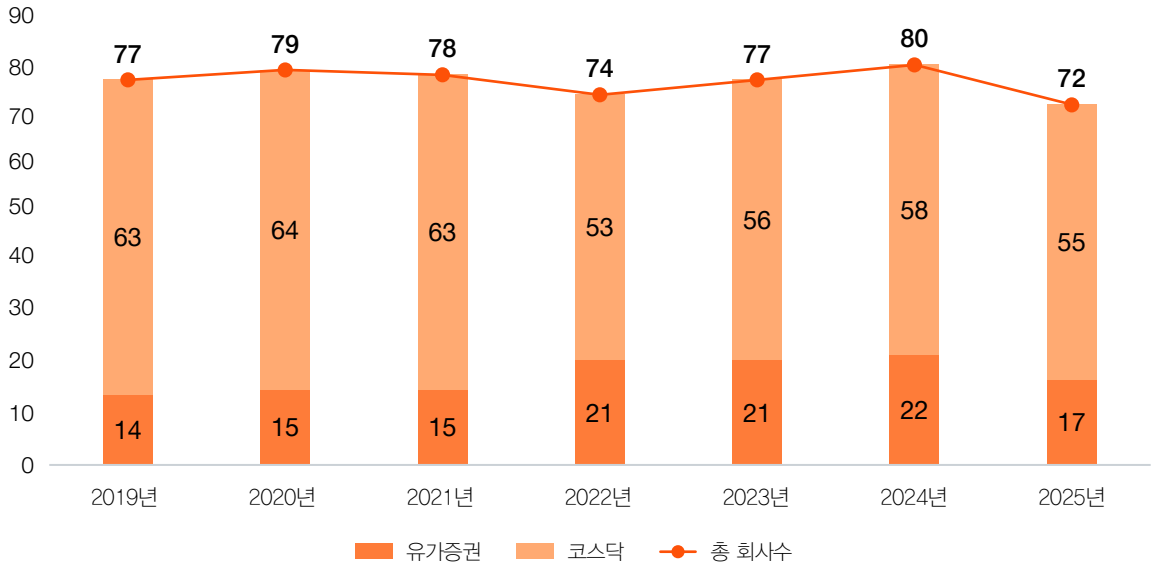
내부회계관리제도 의견변형에 대한 분석

2025년은 내부회계관리제도 감사가 제도 도입 여부를 논의하는 단계를 지나, 그 결과가 보여주는 구조적 취약점을 본격적으로 해석해야 하는 시점이다. 제도 도입 7년차, 연결기준 감사 시행 3년차, 자산총액 1천억 원 이상 상장회사에 대한 감사 적용 4년차에 접어들면서, 이제 시장의 관심은 제도의 정착 여부 자체보다 어떤 기업에서 어떤 취약점이 왜 반복적으로 드러나는가에 집중되고 있다. 최근 7개년간의 의견변형 추이는 단순한 수치의 변화가 아니라, 기업의 재무보고 통제체계가 어느 영역에서 반복적으로 흔들리고 있는지를 보여주는 중요한 신호다. 본 파트에서는 이러한 변화 양상을 공시자료를 바탕으로 분석하고, 이를 토대로 경영진과 감사위원회가 내부회계관리제도를 보다 실효적으로 내재화하기 위해 고려해야 할 시사점을 제시하고자 한다.

1. 2019년 이후 7개년간 내부회계관리제도 의견변형 현황

2019년 개정 외부감사법에 따라 내부회계관리제도에 대한 인증수준이 검토에서 감사로 상향된 이후, 상장회사의 내부회계관리제도 의견변형 추이는 제도 정착의 정도와 재무보고 통제체계의 구조적 취약점을 함께 보여주는 기초 지표로 기능해 왔다. 아래에서는 유가증권시장 및 코스닥시장 상장회사를 대상으로 최근 7개년의 의견변형 추이를 살펴보고, 이어서 미국 사례와의 비교 및 자산규모별 분포를 통해 그 의미를 보다 입체적으로 해석하고자 한다.

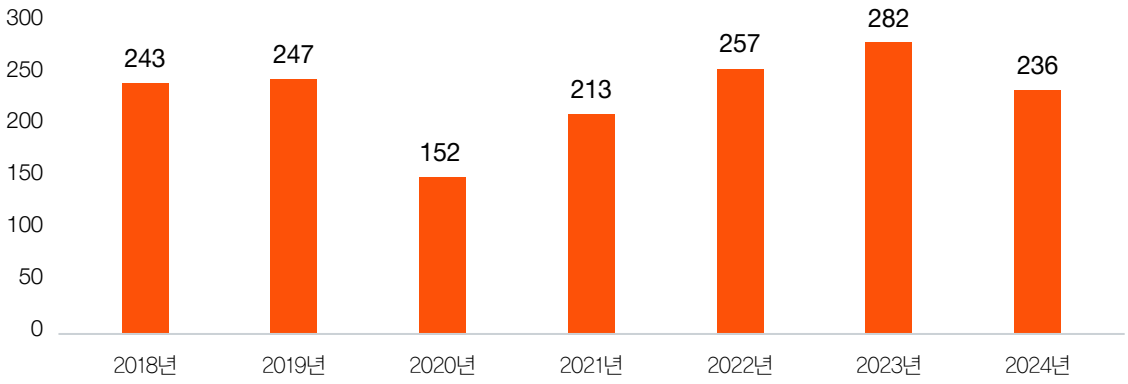
도표 1. **최근 7개년 내부회계관리제도 유가증권 및 코스닥시장 의견변형 회사 추이** (단위: 개수)



최근 7개년의 연도별 추이를 보면, 내부회계관리제도 의견변형 회사 수는 대체로 70개사 내외 수준에서 증감을 반복하며 유사한 흐름을 유지하고 있다. 이는 제도 도입 초기의 일시적 충격이 상당 부분 완화되었음에도 불구하고, 재무보고 통제체계의 취약점이 특정 기업군과 특정 영역에서 반복적으로 나타나고 있음을 시사한다. 2025년에는 의견변형 회사 수가 전년 대비 다소 감소하였으나, 이를 곧바로 구조적 개선으로 단정하기보다는 기업의 선제적 개선 노력, 감사 대응 강화, 표본 특성 및 감사환경 변화 등 복합적 요인을 함께 고려해 해석할 필요가 있다. 따라서 최근 감소는 개선의 가능성을 시사하는 신호로 볼 수 있으나, 그 의미는 후속 연도 추이까지 함께 확인할 때 보다 안정적으로 판단할 수 있다.

한국의 최근 추이를 보다 입체적으로 해석하기 위해, 내부통제에 대한 외부감사 제도가 장기간 운영되어 온 미국의 사례를 참고할 필요가 있다. 이에 따라 미국의 리서치 기관인 Audit Analytics가 집계한 자료를 바탕으로 유사한 기간 동안 미국 내 Internal Control over Financial Reporting (이하 ICFR) 감사 의견변형 회사 수의 연도별 추이를 함께 살펴본다. 다만 양국은 제도 역사, 적용 범위, 시장 구조, 공시 관행 및 집계 기준에 차이가 있으므로, 아래 비교는 절대적 우열 판단보다는 취약점의 성격과 제도 성숙도의 차이를 이해하기 위한 참고자료로 해석하는 것이 적절하다.

도표 2. **미국의 최근 7개년 ICFR 감사 의견변형 회사 추이** (단위: 개수)



미국의 경우, 2020년을 제외하면 ICFR 의견변형 회사 수가 대체로 200건 내외 수준에서 유지되고 있다. 분석 대상 기간 중 가장 최근인 2024년 회계연도에는 전체 ICFR 감사 대상 3,306건 중 236건이 의견변형에 해당하여 비율은 약 7.1%로 집계되었다. 이는 국내 2025년 기준 의견변형 비율인 2.5%보다 높은 수준이지만, 전년도 미국 수치인 8.4%와 비교하면 하락한 흐름을 보인다. 다만 이러한 차이는 제도 성숙도뿐 아니라 적용 대상, 공시 범위 및 시장 특성의 차이도 함께 반영할 수 있으므로 단순 비교보다는, 미국에서는 내부통제 의견변형 비율이 국내에 비해 높은 수준으로 지속적으로 유지되고 있다는 점을 주목할 필요가 있다.

도표 3. **최근 7개년간 연도 말 자산 규모별 내부회계관리제도 의견변형 추이** (단위: 개수)

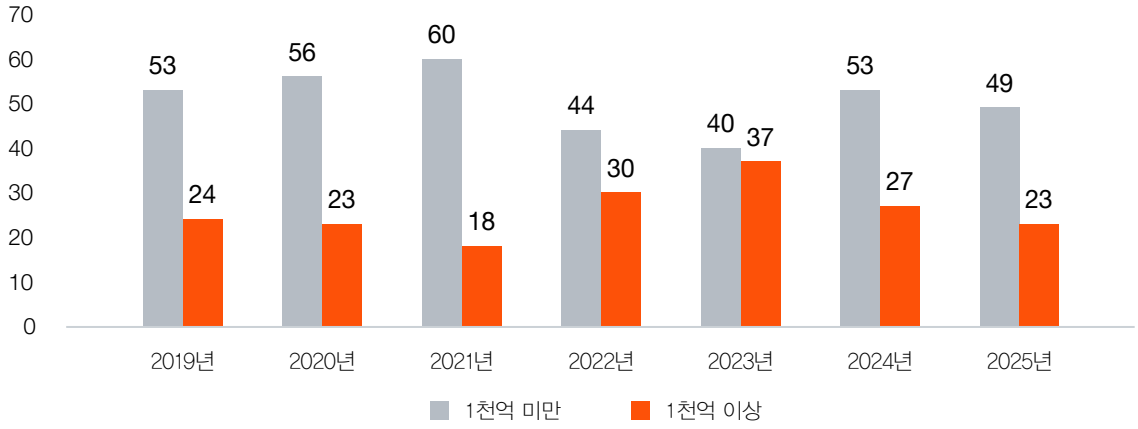
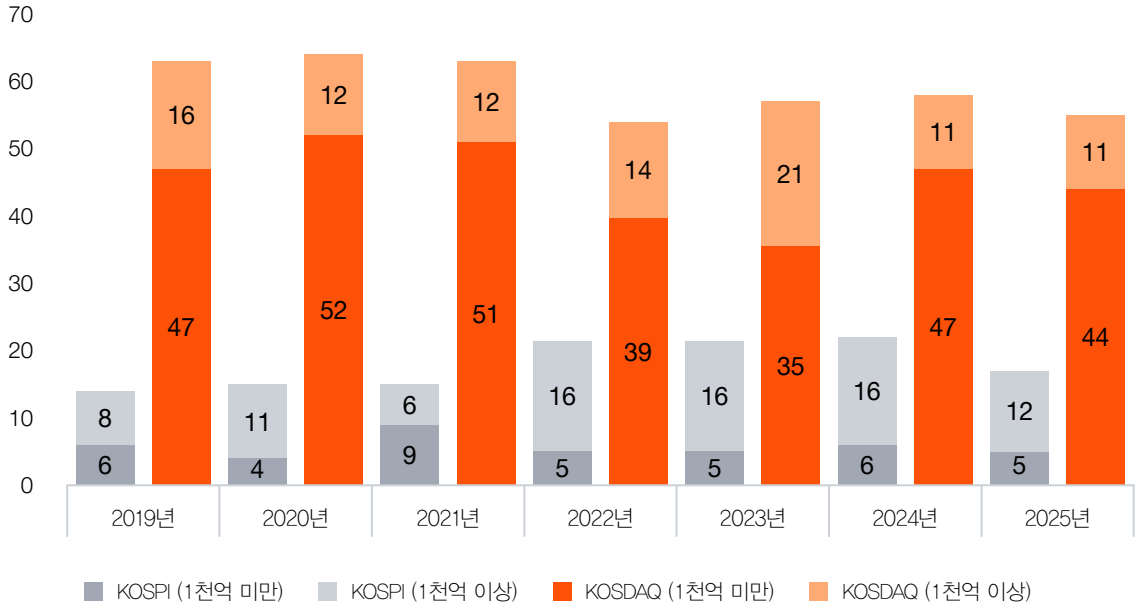


도표 4. **최근 7개년간 연도 말 시장(유가증권시장 및 코스닥시장) 및 자산 규모별 내부회계관리제도 의견변형 추이** (단위: 개수)



최근 7개년 추이를 보면, 자산규모에 따른 내부회계관리제도 의견변형의 양상은 시장별로 뚜렷한 차이를 보인다. 코스닥시장에서는 자산총액 1천억 원 미만 기업에 의견변형이 집중되는 경향이 지속되고 있으며, 2025년에도 코스닥 의견변형 회사 중 해당 구간이 약 80%를 차지하였다. 이는 상대적으로 규모가 작은 기업일수록 내부통제 인프라와 운영체계의 안정성이 취약할 가능성이 높음을 시사한다.

반면 유가증권시장에서는 의견변형 대상 회사 중 자산총액 1천억 원 이상 기업의 비중이 상대적으로 높게 유지되고 있으며, 2025년에도 해당 비중은 약 71%를 차지하였다. 이는 규모가 큰 기업이라 하더라도 복잡한 사업구조, 주요 회계판단 및 추정의 증가에 따라 내부회계 리스크가 여전히 유의미하게 존재함을 보여준다. 종합하면 내부회계관리제도 리스크는 전체적으로는 중소형 상장사에 더 많이 집중되지만, 시장과 기업 규모에 따라 취약점이 나타나는 방식은 다르며, 이에 따라 관리 초점 역시 차별화될 필요가 있다.

결론적으로 최근 7개년 분석 결과, 내부회계관리제도 의견변형은 횟수 기준으로는 큰 변동 없이 유지되고 있으나, 특정 시장(코스닥)과 중소규모 기업에 집중되는 구조적 특징이 확인된다. 또한 미국 대비 의견변형 비율은 낮은 수준이나, 이는 제도 성숙도 차이 및 적용 범위 영향으로 해석되며, 국내 역시 취약영역 개선을 위한 지속적인 관리 및 제도 내실화 노력이 요구된다.

2. 내부회계관리제도 의견변형 사유인 '중요한 취약점' 관련 Keyword 분석

공시된 내부회계관리제도 의견변형 사유를 ① 부정을 예방하거나 적발하기 위한 통제와 ② 재무제표 오류를 감소시키거나 발견하기 위한 통제로 구분하여, 통제 미비점과 관련된 키워드를 분석하였다. 분석 결과, 부정과 관련된 미비점은 약 34%, 재무제표 오류와 관련된 미비점은 약 66%를 차지하는 것으로 나타났으며, 이러한 비중은 최근 연도들 사이에서 큰 차이 없이 유사한 흐름을 보이고 있다. 다만 하나의 의견변형 회사가 복수의 취약점 유형에 동시에 해당할 수 있으므로, 항목별 건수는 개별 회사 수와 일대일로 대응되지 않을 수 있다.

표 1. **내부회계관리제도 중요한 취약점 Keyword 분석 – 부정 및 오류** (단위: 건수, %)

대분류	소분류	2025년		2024년		2023년		2022년		2021년		2020년		2019년	
		항목	비중	항목	비중	항목	비중	항목	비중	항목	비중	항목	비중	항목	비중
부정을 예방하거나 적발하기 위한 통제 (34%)	자산횡령: 자금 및 법인인감 등	17	13%	16	11%	16	10%	22	15%	22	18%	23	18%	24	20%
	부패: 고위경영진, 특수관계자거래 등 타당성	15	12%	16	11%	28	17%	24	16%	10	8%	17	13%	19	16%
	허위보고: 이사회 등의 기능미비	4	3%	8	5%	7	4%	9	6%	7	6%	7	5%	4	3%
	통제환경 및 내부감시 기구의 충분성	8	6%	8	5%	8	5%	6	4%	3	3%	1	1%	3	2%
	소계	44	34%	48	32%	59	36%	61	41%	42	35%	48	37%	50	41%
오류를 감소시키거나 발견하기 위한 통제 (66%)	재무제표 재작성 및 중요한 감사수정사항	17	13%	19	13%	30	18%	30	20%	29	24%	26	20%	21	17%
	재무보고 통제활동 설계 및 운영 미비	47	36%	43	29%	46	28%	32	22%	28	24%	33	25%	30	25%
	자산의 평가 및 회수가능성	20	15%	35	24%	30	18%	20	14%	18	15%	19	15%	16	13%
	정책 및 인력부족	2	2%	2	2%	–	0%	4	3%	2	2%	5	4%	5	4%
	소계	86	66%	99	68%	106	64%	86	59%	77	65%	83	63%	72	59%
합계		130	100%	147	100%	165	100%	147	100%	119	100%	131	100%	122	100%

내부회계관리제도 관련 주요 취약점 키워드를 살펴보면, 횡령 및 자금통제와 같은 부정 관련 통제와 오류 관련 통제는 일정 수준을 유지하고 있다. 다만, 최근에는 재무보고 통제활동의 설계 및 운영 미비와 같은 구조적 통제 취약점이 보다 중요한 이슈로 부각되고 있다. 2025년에는 해당 항목의 비중이 36%로 나타나 전년도보다 상승하였으며, 이는 의견변형의 중심이 단순한 사건 대응이나 개별 오류 수정에서 재무보고 통제체계 전반의 실효성 점검으로 이동하고 있음을 시사한다. 특히 재무보고 통제 관련 항목의 비중 확대는 외부감사인의 감사 대상이 개별 거래나 계정 오류를 넘어, 오류를 예방·탐지하는 통제 설계와 운영의 정합성까지 확장되고 있음을 보여준다. 결국 향후 의견변형 여부는 개별 회계처리의 적정성뿐 아니라, 통제 환경 자체의 정합성과 지속가능한 운영 수준에 의해 더 영향을 받을 가능성이 높음을 보여준다.

최근 상법 개정 등으로 이사회 의사결정의 정당성이 더욱 중요해진 만큼, 향후에는 이사회 등의 기능 미비로 인한 의견변형 비중이 높아질 가능성이 있다.

종합하면 1.2의 키워드 분석은 내부회계관리제도 의견변형의 중심이 부정 위험뿐만 아니라, 재무보고 통제의 설계 및 운영과 같은 구조적 취약점에 있으며, 관리 초점 또한 개별 오류 대응에서 통제체계 전반의 실효성 확보로 이동하고 있음을 보여준다.

3. 내부회계관리제도 의견변형 회사의 지적사항(Keyword) 평균 항목 수

연도별 내부회계관리제도 의견변형 회사 중 범위제한이나 내부회계관리제도 설계·평가자료 미제시 등으로 통제 미비점에 대한 실질적 분석이 어려운 회사를 제외하고, 유의미한 분석이 가능한 회사를 대상으로 회사당 지적항목의 평균 개수를 산출하였다. 또한 2025년에는 범위제한 등으로 인해 하단 분석 대상에서 제외되는 의견변형 회사의 비중이 전기 대비 크게 증가하였다.

이 지표는 해당 회사들에서 식별된 총 키워드 항목 합계를 분석대상 의견변형 회사 수로 나누어 계산하였으며, 의견변형이 특정 영역의 단일 미비에 그치지 않고 복수 영역의 통제 취약점이 동시에 나타나는지를 보여주는 보조지표로 활용할 수 있다.

2025년의 경우 의견변형 회사당 지적사항 평균 건수는 3.9건으로 분석기간 중 가장 높은 수준을 기록하였다. 이는 개별 기업의 의견변형 사유가 단일 이슈에 그치지 않고 복수의 통제 취약점이 동시에 존재하는 방향으로 전개되고 있음을 시사한다. 다만, 이러한 증가에는 전년도 대비 분석대상 의견변형 회사 수 감소(55개사 → 33개사)에 따른 분모 축소의 영향이 일부 반영된 측면도 있는 것으로 판단된다. 즉, 최근의 의견변형은 단편적인 오류나 특정 사건보다 통제체계 전반의 복합적 취약성과 연계되어 나타날 가능성이 높아지고 있다고 볼 수 있다.

표 2. **내부회계관리제도 의견변형 회사 지적사항 평균 건수** (단위: 개수)

구분	2025년	2024년	2023년	2022년	2021년	2020년	2019년
전체 의견변형 회사 수	72개	80개사	77개사	74개사	78개사	79개사	77개사
범위제한 의견변형 회사 차감	39개사	25개사	22개사	22개사	27개사	26개사	26개사
차감 후 분석대상 의견변형 회사	33개사	55개사	55개사	52개사	51개사	53개사	51개사
총 키워드 항목 합계	130	147	165	147	119	131	122
의견변형 회사당 지적사항 평균 건수	3.9	2.7	3.0	2.8	2.3	2.5	2.4

요약하면 1.3의 평균 지적항목 수 분석은 최근 의견변형이 단일 미비보다 복수의 통제 취약점이 중첩되는 방향으로 전개되고 있음을 보여주며, 내부회계관리제도 리스크가 점차 복합적이고 구조적인 성격을 띠고 있음을 시사한다.

4. 회계처리 및 재무제표 구성요소 관점의 주요 Keyword 분석

외부감사인이 언급한 주요 취약점 중 회계처리 및 재무제표 구성요소와 직접적으로 연관되는 항목을 회계영역별로 재분류하여 살펴보면, 내부회계관리제도 의견변형이 어떤 계정과 판단영역에서 반복적으로 발생하는지를 보다 구체적으로 확인할 수 있다. 이는 단순한 통제미비의 존재 여부를 넘어, 실제 재무보고 과정에서 어떤 회계 이슈가 내부통제의 핵심 취약영역으로 작용하고 있는지를 보여준다는 점에서 의미가 있다.

표 3. **중요한 취약점 관련 키워드 – 회계처리 및 재무제표 구성요소 영역 관점** (단위: 건수, %)

대분류	소분류	2025년		2024년		2023년		2022년		2021년		2020년		2019년	
		항목	비중	항목	비중	항목	비중	항목	비중	항목	비중	항목	비중	항목	비중
평가 및 회수가능성	금융자산 및 금융상품	11	18%	18	23%	12	14%	10	17%	7	16%	7	13%	5	10%
	CGU 및 유무형자산	3	5%	6	8%	7	8%	1	2%	6	13%	5	10%	4	8%
	종속기업, 관계기업투자	6	10%	11	14%	11	13%	9	15%	5	11%	7	13%	7	14%
특수관계자 거래 인식 및 공시	특수관계자 거래 - 인식	2	3%	6	8%	15	17%	9	15%	6	13%	8	16%	9	18%
	특수관계자 거래 - 범위 및 공시	4	7%	3	4%	3	3%	5	8%	2	4%	4	8%	12	24%
특정 계정 관련	수익인식	7	12%	8	10%	10	11%	6	10%	8	19%	7	13%	2	3%
	재고, 리스 등	7	12%	9	11%	16	18%	5	8%	6	13%	8	15%	6	12%
계속기업 관련	계속기업 존속능력에 대한 평가 관련	16	27%	14	18%	10	11%	9	16%	2	4%	1	2%	2	3%
기타	비경상거래, 회계정책 등	4	6%	6	4%	4	5%	5	9%	3	7%	5	10%	4	8%
계		60	100%	81	100%	88	100%	59	100%	45	100%	52	100%	51	100%

회계처리 및 재무제표 구성요소별 취약점 분포를 보면, 금융자산, 수익인식, 재고자산과 같은 전통적인 계정 중심 이슈는 전반적으로 일정 수준에서 반복되고 있다. 반면 최근 불확실한 국내 경영환경 및 기업들의 둔화된 재무상황과 연계하여 계속기업 존속능력에 대한 평가 관련 통제가 유효하게 작동하지 않았다는 미비점의 지적률이 2022년부터 지속적으로 증가하면서 2025년 27%로 역대 최고치를 기록했다. 이는 단순한 계정 수준 오류를 넘어, 기업의 지속가능성과 주요 가정의 타당성 검토가 내부통제의 핵심 이슈로 부각되고 있음을 시사한다.

향후 내부회계관리제도의 관리 초점은 개별 계정의 정확성 확보뿐만 아니라, 손상평가, 계속기업, 투자약정, 특수관계자거래와 같이 경영진 판단이 크게 개입되는 영역의 실질적인 내부통제를 얼마나 정교하게 운영하느냐에 의해 좌우될 가능성이 높다.

이를 종합하면 회계처리 및 재무제표 구성요소 관련 취약점은 금융자산, 수익인식 등 전통적 계정 중심 이슈가 지속되는 가운데, 손상평가·계속기업 등 경영진 판단이 개입되는 영역으로 확대되는 흐름이 확인된다. 특히 비계정 기반의 재무적·비재무적 지표 관련 취약점이 증가하고 있어, 향후 내부통제는 판단 영역 중심의 관리 정교화가 중요해질 것으로 판단된다.

표 4. **금융감독원 발표 재무제표 중점심사 회계이슈별 의견변형 해당 회사 수** (단위: 개수, %)

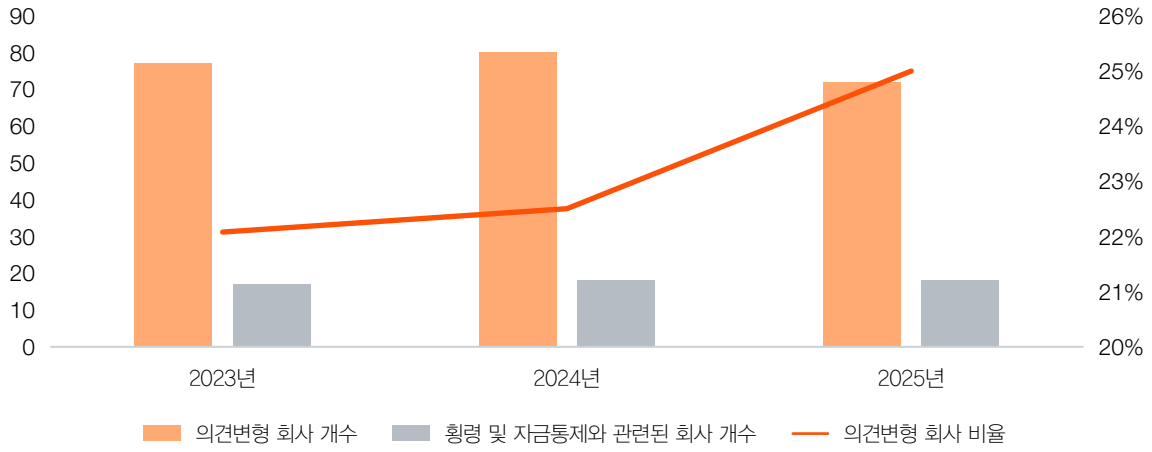
2025년 재무제표에 대한 중점심사 회계이슈	의견변형 해당 회사 수	의견변형 회사(총 72건) 중 비율
투자자 약정 회계처리	12	17%
전환사채 발행 및 투자 회계처리	1	1%
공급자금융약정 공시	0	0%
종속·관계기업 투자주식에 대한 손상처리	6	8%
합계	19	26%

2025년 의견변형 사유와 2025년 금융감독원이 선정한 재무제표 중점심사 회계이슈와 연관성을 검토한 결과 약 26%의 높은 비율로 상관관계를 보이고 있다. 그리고 의견변형 현황을 보면, 투자자 약정 회계처리와 종속·관계기업 투자주식 손상과 같이 경영진의 판단과 추정이 크게 개입되는 영역에 의견변형이 상대적으로 집중되는 경향이 나타난다. 이는 감사인들이 금융감독원이 선정한 재무제표 중점심사 회계 항목에 대해 더욱 강화된 감사절차를 수행한 결과이며 단순한 회계처리 오류보다 계약조건 해석, 권리·의무의 식별, 회수가능성 평가 등 판단 중심의 회계 이슈가 감사상 주요 위험요소로 부각되고 있음을 보여준다. 특히 투자자 약정 관련 이슈가 가장 높은 비중을 차지하는 점은 최근 자금조달 및 투자 구조가 복잡해지면서 계약조건에 따른 회계처리 적정성과 공시의 완결성에 대한 검증 필요성이 확대되고 있음을 시사한다.

표 5. **횡령 및 자금통제와 관련된 의견변형 비율** (단위: 개수, %)

구분	의견변형 회사 개수	횡령 및 자금통제와 관련된 회사 개수	비율
2023년	77	17	22%
2024년	80	18	23%
2025년	72	18	25%

도표 5. **횡령 및 자금통제와 관련된 의견변형 회사 개수 및 비율** (단위: 개수, %)



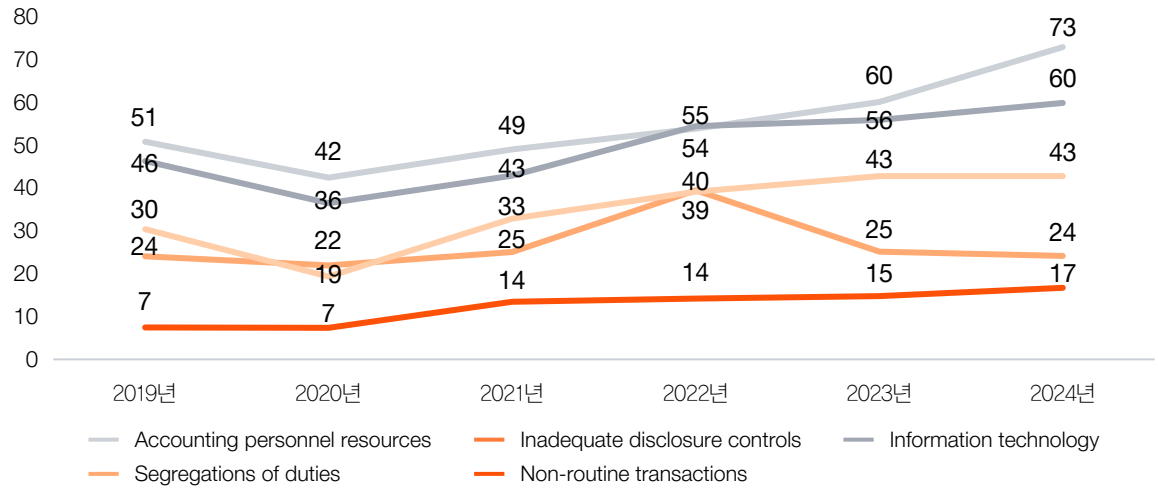
최근 자금통제 공시가 의무화가 된 상황에서 전체 의견변형 회사 중에 횡령 및 자금통제와 관련된 회사의 비율에 대한 분석은 의미가 있다. 최근 3년 동안 해당 비율은 20%를 넘는 높은 수준으로 부정위험과 관련한 자금통제의 미비가 의견변형의 중요한 사유임을 확인할 수 있다. 특히 2025년에도 관련 비율이 확대된 점을 고려하면, 자금 및 횡령 관련 통제는 단기적 사건 대응 이슈가 아니라 여전히 구조적으로 관리가 필요한 핵심 리스크 영역으로 볼 수 있다. 또한, 자금통제 공시가 의무화된 시점에 향후 공시 내역의 적정성뿐만 아니라 횡령 및 부정위험과 관련한 자금통제의 실효적인 관리 및 운영이 필요하다.

결론적으로 금융감독원 중점심사 회계이슈와의 연계 분석 결과, 의견변형은 특정 회계이슈와 상당 부분 연관되어 나타나며 복잡한 회계처리 영역에 집중되는 경향이 확인된다. 특히 단순 회계처리 오류보다는 계약조건 해석, 회수가능성 검토 등 경영진의 판단이 개입되는 영역의 중요성이 점차 확대되고 있다. 한편 횡령 및 자금통제 관련 의견변형 비중은 상승하는 추세를 보이며, 자금통제 및 부정 리스크 관리의 중요성이 지속적으로 커지고 있다.

5. 내부통제 미비점 사유에 있어서의 한국과 미국 간의 비교

아래 분석은 미국 ICFR 제도하에서 외부감사인이 내부통제 의견을 변형한 기업들의 주요 사유와 그 추이를 정리한 것이다. 해당 자료는 미국의 리서치 기관인 Audit Analytics가 집계한 내부통제 미비점 사유를 바탕으로 하며, 미국 외부감사인이 어떤 유형의 내부통제 취약점을 중점적으로 식별하고 있는지를 파악하는 데 의미가 있다. 다만 한국과 미국은 제도 도입 시기, 적용 범위, 공시 관행, 시장 구조에 차이가 있으므로, 아래 비교는 절대적 우열 판단보다는 내부통제 미비의 성격 차이를 이해하기 위한 참고자료로 해석할 필요가 있다.

도표 6. **미국의 최근 6개년(2019년~2024년) 내부통제 미비점 지적 순위** (단위: %)



Source: Audit Analytics August, 2025

표 6. **한국 및 미국의 내부통제 미비점 사유 분석** (순위)

구분	한국				미국	
	2025년	2024년	2023년	2022년	2024년	2023년
통제활동 미비	1	1	1	1	4	4
범위제한, 자료 미제출	2	2	2	2	–	–
중요한 수정사항, 비경상거래	3	3	3	3	5	5
업무분장	4	4	4	4	3	3
인력 적정성	5	5	5	6	1	1
정보기술	6	6	5	5	2	2

Source: Audit Analytics August 2025

한국과 미국의 내부통제 미비 사유를 비교해보면, 양국의 내부회계관리제도 운영 초점과 제도 성숙도에서 일정한 차이가 관찰된다. 미국의 경우 인력 적정성, 정보기술, 업무분장과 같이 내부통제 운영을 뒷받침하는 인프라 요소가 주요 미비 사유로 나타난다. 이는 내부통제 체계가 일정 수준 이상 구축된 이후, 운영 효율성과 지속가능성, 시스템 기반 통제의 안정성을 점검하는 단계의 이슈가 상대적으로 부각되고 있음을 시사한다.

반면 한국은 통제활동 미비, 자료 제출 제한, 재무제표 작성 과정에서의 중요한 수정사항 등 감사 수행 과정에서 직접적으로 드러나는 실행 단계의 미비가 상위 사유로 나타난다. 이는 내부통제의 설계와 운영이 아직 완전히 내재화되지 않은 상태에서, 절차의 실제 이행 여부와 증빙 확보, 재무보고 통제의 수행 정합성이 여전히 핵심 점검 영역으로 남아 있음을 보여준다. 다시 말해 한국의 내부통제 리스크는 운영 인프라 자체의 문제라기 보다, 통제의 실행과 검증 과정에서 드러나는 취약성이 상대적으로 두드러지는 양상으로 해석할 수 있다.

종합하면 미국에서는 내부통제 운영 기반의 적정성과 지속가능성을 점검하는 성격이 상대적으로 강한 반면, 한국에서는 통제활동의 실제 수행과 재무보고 통제의 실행력에 대한 점검이 보다 중심적으로 이루어지고 있다. 따라서 국내 기업은 단순한 통제 수행 여부를 넘어 인력, 정보기술, 업무분장, 문서화 체계 등 운영 기반 전반을 함께 강화함으로써 내부회계관리제도의 관리 수준을 한 단계 고도화할 필요가 있다.

요약하면, 미국은 통제 미비점의 사유로 내부통제 인프라와 운영의 안전성 측면 등 통제 미비점 이면의 Root cause 중심의 분석이 중심이고, 한국은 통제활동의 실제수행과 재무보고 과정에서의 실행 미비 등 외형상 드러나는 관리 및 통제상 이슈가 중심이다.

6. 결론

1부의 분석 결과, 내부회계관리제도 의견변형은 제도 도입 초기의 일시적 충격을 넘어 여전히 반복적으로 나타나는 구조적 리스크 신호로 확인된다. 최근 7개년 동안 의견변형 회사 수가 큰 폭으로 감소하지 않았고, 의견변형 사유 역시 부정 관련 이슈뿐만 아니라, 재무보고 통제의 설계 및 운영, 손상평가, 계속기업, 투자약정, 특수관계자거래 등 경영진의 판단과 추정이 크게 개입되는 영역에 집중되는 경향을 보였다. 또한 회사당 지적항목 수가 증가하고 있다는 점은 최근 의견변형이 단일한 통제 실패보다 복수의 취약점이 중첩된 복합적 현상으로 전개되고 있음을 시사한다.

이러한 결과는 내부회계관리제도가 법제화되고 자금통제 공시가 의무화된 현시점에서 내부회계관리제도를 더 이상 형식적 준수 체계로 볼 수 없으며, 재무보고 신뢰성과 기업 리스크 관리 수준을 가늠하는 핵심 관리체계로 이해해야 함을 보여준다. 특히 시장과 기업 규모에 따라 취약점의 양상은 다르게 나타나고, 한국과 미국 간 비교에서도 운영 기반의 성숙도와 통제 실행력의 차이가 확인되는 만큼, 기업은 획일적인 대응보다 자사의 사업구조와 리스크 특성에 맞춘 통제 고도화 전략을 마련할 필요가 있다. 결국 향후 내부회계관리제도의 실효성은 통제의 존재 여부뿐만 아니라 실질적인 변화관리, 운영 및 모니터링 등을 통한 지속가능하고 실효적인 운영 수준에 의해 좌우될 것이다.

경영진과 감사(감사위원회)의 고려사항

내부회계관리제도 감사가 정착 단계에 접어들면서, 단순한 제도 준수 여부를 넘어 어떻게 평가하고 무엇을 중점적으로 고려할 것인가에 대한 논의의 중요성이 커지고 있다. 특히 재무제표 감사와 내부회계관리제도 감사 간의 연계, 핵심감사항목과 내부통제 이슈 간 관계, 그리고 이에 대한 경영진 및 감사(위원회)의 관심과 참여는 내부회계관리제도의 실효성을 좌우하는 핵심 요소로 자리 잡고 있다. 본 파트에서는 이러한 관점에서 경영진과 감사(위원회)가 내부회계관리제도를 바라보고 대응하는 과정에서 고려해야 할 주요 쟁점을 중심으로, 보다 실질적인 시사점을 도출하고자 한다. 이를 통해 단순한 사후적 대응이 아닌, 리스크를 사전에 인지하고 예방 중심의 통제 수준을 제고하는 방향의 실무적 기준을 제시한다.

1. 핵심감사항목과 내부회계관리제도 의견변형 사유

2020년부터 모든 상장회사에 적용되고 있는 핵심감사제도는 외부감사인이 재무제표 감사 과정에서 특히 중요하게 판단한 사항을 공시하고, 이에 대해 수행한 주요 감사절차를 설명함으로써 정보이용자의 이해를 높이기 위해 도입된 제도이다.

핵심감사항목(KAM)은 재무제표 감사에서 감사인의 전문가적 판단에 따라 가장 유의하다고 판단된 사항을 의미한다. 이러한 항목은 감사인이 중점적으로 검토한 재무보고 위험영역을 보여준다는 점에서, 내부통제의 설계 및 운영과도 밀접한 관련을 가질 수 있다.

표 1. **핵심감사항목과 내부통제 미비점 지적 일치율 (2022년~2025년)** (단위: 건수, %)

구분	수익 인식	공정가치 평가	손상 평가	재고 자산	부정 사건	특수관계자 거래	합계
핵심감사항목*	31	16	37	9	3	10	106
핵심감사항목 중 미비점 지적건수	10	7	20	5	3	8	53
핵심감사항목과 미비점 지적 일치율	32%	44%	54%	56%	100%	80%	50%

* 상기 핵심감사항목 개수는 내부회계관리제도 의견이 변형된 회사 중 재무제표에 대한 감사의견 거절인 회사, 그리고 내부회계관리제도에 대한 자료제출 미비로 인한 내부회계관리제도 의견이 거절인 회사를 제외한 회사의 핵심감사항목 합계임.

최근 4개년 분석 결과, 핵심감사항목으로 식별된 영역 중 절반 수준이 내부통제 미비와 함께 나타나고 있다. 이는 외부감사인이 중요하게 판단한 재무보고 위험영역이 실제 통제 취약성과 상당 부분 중첩되고 있음을 보여준다.

특히 부정사건과 관련해서는 핵심감사항목으로 선정된 3건 모두에서 미비점이 지적되어 지적 일치율이 100%에 달하였다. 그리고 손상평가와 재고자산은 비교적 높은 미비율을 보여, 추정과 가정의 합리성 검토가 필요한 영역일수록 내부통제의 설계 및 운영 수준이 감사 품질에 직접적인 영향을 미친다는 점을 시사한다. 또한 특수관계자거래와 부정사건은 내부통제 미비와의 연계성이 높아, 해당 영역이 단순한 회계처리 이슈를 넘어 거버넌스와 모니터링 체계 전반의 성숙도를 반영하는 영역임을 보여준다.

추가로 2025년에는 핵심감사항목 가운데 손상평가가 가장 높은 비중을 차지하고 있어, 경기 변동성과 사업환경 변화 속에서 기업의 추정과 판단 중심 영역이 지속적으로 감사의 핵심에 위치하고 있음을 보여준다.

결과적으로, 핵심감사항목과 내부통제 미비는 구조적으로 상당한 연계 관계를 보이고 있으며, 이는 외부감사인이 위험이 높은 영역에 대해서는 핵심감사항목으로 확정함과 동시에 내부통제의 신뢰성에 대한 판단을 병행하고 있음을 시사한다. 이에 경영진 및 감사(위원회)는 기중부터 위험이 높은 항목에 대한 외부감사인과의 선제적 의사소통을 통해 연말 감사 시점 이전에 통제상 미비점 또는 재무정보의 왜곡 가능성을 사전에 식별하고 구체적인 대응을 할 필요가 있다.

2. 경영진 및 감사(위원회)의 내부회계관리제도 의견 일치율

내부회계관리제도의 효과성에 대한 평가는 정보이용자에게 세 가지 경로를 통해 제공된다. 즉 경영진의 운영실태보고서, 외부감사인의 감사 또는 검토의견, 그리고 내부감시기구인 감사 또는 감사위원회의 운영실태평가보고서를 통해 각각의 판단이 공표된다.

내부회계관리제도 모범규준과 감사기준상 경영진, 외부감사인, 내부감시기구가 미비점을 판단하고 평가할 때 적용하는 원칙 자체에는 본질적인 차이가 없다. 그럼에도 실제 공시 결과에서는 최종 결론이 서로 다르게 나타나는 경우가 적지 않으며, 이는 동일한 기준 아래에서도 중요성 판단, 증빙 수준, 평가 시점 및 관찰 범위에서 인식 차이가 존재할 수 있음을 보여준다.

표 2. **외부감사인과 경영진 내부회계관리제도 운영실태보고서 의견 일치율** (단위: 개수, %)

구분	2025년	2024년	2023년	2022년	2021년	2020년	2019년
외부감사인 내부회계 의견변형 회사 수	72	80	77	74	78	79	77
경영진 내부회계 의견변형 회사 수*	13	7	12	13	8	2	7
외부감사인과 경영진 의견 일치율	18%	9%	17%	18%	10%	3%	9%

* 경영진의 내부회계관리제도 운영실태보고서상 중요한 취약점이 포함된 회사의 수이며, 운영실태보고서가 제출되지 않은 경우는 포함되지 않은 수치임.

외부감사인의 의견변형 회사 수가 최근 7년간 대체로 70~80개 수준에서 유지되는 가운데, 2025년에는 다소 감소한 반면 경영진의 운영실태보고서상 의견변형 회사 수는 전년 대비 증가하였다.

이와 함께 외부감사인과 경영진 간 의견 일치율도 일부 개선되는 흐름을 보인다. 다만 절대 수준은 여전히 낮아, 내부 평가와 외부 검증 결과 사이의 인식 격차가 구조적으로 존재함을 보여준다. 이는 운영실태보고가 형식적 보고 절차에 머무르기보다, 미비점의 식별, 중요성 평가, 개선조치의 이행 여부와 실질적으로 연계될 필요가 있음을 시사한다.

표 3. **내부감시기구의 내부회계관리제도 운영실태평가보고서 의견** (단위: 개수, %)

구분	2025년	2024년	2023년	2022년	2021년	2020년	2019년
외부감사인 의견변형 회사 수	72	80	77	74	78	79	77
감시기구(감사·감사위원회)의 비적정의견 비율*	21%	11%	16%	19%	11%	11%	14%
비적정의견	15	9	12	14	8	8	10
적정의견	55	70	64	58	68	68	63

* 감사(위원회)의 내부회계관리제도 운영실태평가보고서상 중요한 취약점이 포함된 회사의 수이며, 운영실태평가보고서가 제출되지 않은 경우는 제외 후 계산한 비율임.

감사(위원회)의 운영실태평가보고서상 비적정의견 비율 역시 최근 연도에 걸쳐 10%대 수준에 머물고 있어, 외부감사인의 비적정의견 비율과 비교할 때 여전히 상당한 괴리가 존재한다. 이는 내부감시기구의 관리·감독 수준과 외부감사인의 독립적 평가 사이에 인식 차이가 지속되고 있음을 보여주며, 감사(위원회)가 경영진 보고에 의존하는 수준을 넘어 중요 취약점의 판단 근거와 개선조치의 실효성을 보다 직접적으로 점검할 필요가 있음을 시사한다.

3. 내부회계관리제도 비적정의견과 재무제표 감사의견 연관성

외부감사인은 기업의 재무보고 신뢰성에 대해 두 가지 경로로 정보이용자에게 의견을 제시한다. 하나는 재무제표 수치의 적정성을 평가한 재무제표 감사의견이고, 다른 하나는 그 수치를 산출하는 과정의 신뢰성을 평가한 내부회계관리제도에 대한 감사 또는 검토의견이다.

두 의견은 각각 별개의 감사 대상에 대한 의견이지만, 실제 외부감사인의 판단 과정에서는 상호 밀접하게 연계되는 경향이 나타난다. 특히 재무제표 감사의견이 비적정의견인 경우 내부회계관리제도 역시 비적정의견이 제시되는 사례가 적지 않으며, 이는 내부회계관리제도를 재무제표와 독립된 별개의 체계로만 보기보다 재무제표상 오류나 왜곡을 예방·발견하기 위한 재무보고 통제체계의 관점에서 함께 이해할 필요가 있음을 시사한다.

한편, 2019년부터 2025년까지 내부회계관리제도에 대해 비적정의견을 받은 상장회사의 재무제표 감사의견 현황은 아래와 같다.

표 4. **내부회계 비적정 상장회사의 재무제표에 대한 감사의견 현황** (단위: 개수, %)

재무제표 감사의견	2025	2024	2023	2022	2021	2020	2019	합계
적정의견	19	23	22	33	29	24	27	177
비적정의견	53	57	55	41	49	55	50	360
합계 – 내부회계관리제도 비적정 회사	72	80	77	74	78	79	77	537
재무제표 감사 비적정의견 비율	74%	71%	71%	55%	63%	70%	65%	67%

최근 3개년 동안 내부회계관리제도 비적정 회사의 재무제표 감사 비적정의견 비율이 점진적으로 높아지고 있는 흐름은 내부통제 미비가 재무보고 결과와 점차 분리되지 않고 연계성이 증가하고 있음을 보여준다. 이는 내부통제의 취약성이 단순한 관리 이슈를 넘어 재무제표 신뢰성에 직접적인 영향을 미치는 요소로 인식되면서, 감사의 판단 기준 또한 보다 통합적으로 작동하고 있음을 시사한다.

다만, 내부회계관리제도 비적정 회사 중에 재무제표 감사 적정 비율이 2025년에 여전히 약 26%인 점은 재무보고 결과가 적정하더라도 관련 내부통제 미비가 중요한 경우에는 재무보고 결과와 관계없이 내부회계관리제도 비적정의견이 될 수 있음을 보여준다.

시계열 분석 결과, 내부회계관리제도 비적정 회사의 재무제표 비적정 의견 비율은 전반적으로 상승하는 흐름을 보인다. 특히 2019년 약 65% 수준에서 2025년 74%까지 일부 등락은 있었으나 전반적으로 상승하는 추세를 보이며, 내부통제 미비가 재무보고 결과에 미치는 영향이 점차 확대되고 있음을 시사한다.

4. 내부회계관리제도 의견변형 회사의 사후 상장폐지 여부

유가증권시장과 코스닥시장에 상장된 기업은 일정한 요건에 해당하는 경우 상장폐지 대상이 될 수 있다. 이는 기업의 재무건전성, 공시 신뢰성, 계속기업으로서의 지속가능성 등에 중대한 문제가 발생하여 투자자 보호와 시장 신뢰를 훼손할 우려가 있는 경우를 의미하며, 장기간 감사의견 거절, 부도, 영업정지 등 다양한 사유가 이에 포함된다.

내부회계관리제도에 대한 감사 또는 검토의견이 변형되는 것만으로 상장폐지의 직접 사유가 되는 것은 아니다. 다만 내부회계 의견변형이 재무제표 신뢰성 저하, 계속기업 관련 불확실성, 지배구조 및 공시 통제의 취약성과 함께 나타나는 사례가 적지 않다는 점에서, 해당 의견변형은 기업의 종합적 위험수준을 보여주는 경고 신호로 해석될 수 있다. 이에 본 절에서는 상장폐지까지 통상 일정 기간이 소요된다는 점을 고려하여, 2019년부터 2022년까지 내부회계관리제도 의견이 변형된 회사들의 현재 상장 유지 여부를 함께 살펴본다.

표 5. **내부회계관리제도 의견변형 회사의 상장폐지 여부** (단위: 개수, %)

구분	2019년			2020년			2021년			2022년		
	유가증권	코스닥	계	유가증권	코스닥	계	유가증권	코스닥	계	유가증권	코스닥	계
상장유지	10	25	35	13	27	40	13	34	47	16	29	45
상장폐지	4	38	42	2	37	39	2	29	31	5	24	29
계	14	63	77	15	64	79	15	63	78	21	53	74
상장폐지회사 비율	29%	60%	55%	13%	58%	49%	13%	46%	40%	24%	45%	39%

과거 내부회계관리제도 의견변형 회사 중 상당수 회사가 이후 상장폐지로 이어진 사실은 내부회계 의견변형이 단기적 절차 미비를 넘어 기업의 재무보고 신뢰성과 지속가능성에 대한 조기경보 신호로 기능할 수 있음을 보여준다. 따라서 경영진과 감사(위원회)는 의견변형을 일회성 오류나 감사 이슈로 보기보다, 사업 지속성·재무건전성·거버넌스 수준과 연결된 전사적인 리스크 신호로 해석할 필요가 있다.

다만 시장 간 차이는 비교적 일관되게 나타난다. 코스닥시장에서 상장폐지 비율이 유가증권시장 대비 지속적으로 높게 나타나는 점은, 동일한 내부통제 이슈라도 기업 규모, 지속가능성, 지배구조 안정성 등의 수준에 따라 그 영향이 다르게 전개될 수 있음을 시사한다. 즉, 특히 코스닥시장 상장사의 경우 내부회계관리제도 의견변형의 의미는 향후 상장폐지로 이어질 수 있는 가능성이 더 높기 때문에 내부통제 개선 등에 더 전사적인 노력을 통한 치유가 필요함을 시사한다.

참고로 2025년도에 상장폐지된 분석대상 상장사 13개 회사 중에 7개 회사(약 54%)가 과거 내부회계관리제도 의견변형이 된 회사인 점은 내부회계관리제도 의견변형과 상장폐지와의 상당한 연관성을 보여준다. 다만 전체 상장폐지 사례를 충분히 설명하지는 못하는 만큼, 의견변형 발생 여부를 단일 판단 기준으로 보기보다는 잠재 리스크를 조기에 포착하는 관리 지표로 활용할 필요가 있다.

표 6. **2019년 ~ 2022년 4개년 내부회계 의견변형 회사의 취약점 언급 요소별 상장유지 여부** (단위: 개수, %)

구분	상장유지		상장폐지	
	회사수	구성비	회사수	구성비
부정요소만 언급	20	12%	12	9%
오류요소만 언급	69	41%	28	20%
부정오류 동시 언급	50	30%	35	25%
범위제한	30	18%	64	46%
계	**169**	**100%**	**139**	**100%**

취약점 언급 유형에 따라 상장 유지 여부는 비교적 뚜렷한 차이를 보인다. 상장유지 기업에서는 '오류 중심' 취약점의 언급 비중이 약 41%로 상대적으로 높게 나타난 반면, 상장폐지 기업에서는 '범위제한' 비중 및 '부정 및 오류 동시 언급'이 각각 46% 및 약 25%로 크게 높게 나타났다. 이는 감사범위 확보의 실패가 단순한 절차상 제약을 넘어 기업의 재무보고 신뢰성과 정보접근 가능성에 대한 보다 직접적인 위험 신호로 작용할 수 있음을 시사한다. 또한 부정 사건 등으로 부정위험이 높고 중요한 회계처리 오류가 함께 수반되는 경우에는 단일한 통제 미비를 넘어 전사적인 내부통제 체계 전반의 신뢰 훼손과 연결될 가능성이 더 크기 때문에 상장유지에 보다 높은 수준의 개선 노력과 리스크 관리가 실질적으로 필요함을 보여준다. 이는 내부통제 취약점이 복합적으로 나타날수록 사후 리스크 역시 보다 구조적으로 확대될 수 있음을 시사한다.

상장 유지 여부에 따른 내부회계관리제도 의견변형 회사들의 중요한 취약점 키워드 중심으로 분석해보면 다음과 같다.

표 7. **2019년 ~ 2022년 4개년 내부회계 의견변형 회사의 취약점 키워드 분석** (단위: 건수, %)

분류	상장유지		상장폐지	
	항목	비중	항목	비중
자산횡령: 자금 및 법인인감 등	39	14%	38	27%
부패: 고위경영진, 특수관계자거래 등 타당성	31	11%	25	18%
허위보고: 이사회 등의 기능미비	15	5%	9	6%
통제환경 및 내부감시기구의 충분성	9	3%	3	2%
부정 관련 키워드 소계	**94**	**34%**	**75**	**53%**
재무제표 재작성 및 중요한 감사수정사항	68	24%	19	13%
재무보고 통제활동 설계 및 운영 미비	64	23%	27	19%
자산의 평가 및 회수가능성	44	16%	17	12%
정책 및 인력부족	8	3%	4	3%
오류 관련 키워드 소계	**184**	**66%**	**67**	**47%**
총 키워드 항목 합계	**278**	**100%**	**142**	**100%**

내부회계관리제도 의견변형 회사의 취약점 유형별 분포를 보면, 상장유지 기업과 상장폐지 기업 사이에는 취약점의 성격에서 뚜렷한 차이가 관찰된다. 상장유지 기업에서는 오류 중심 항목의 비중이 66%로 상대적으로 높게 나타난 반면, 상장폐지 기업에서는 부정 관련 항목의 비중이 53%로 더 크게 나타났다. 이는 상장유지 기업의 경우 재무제표 재작성이나 통제 미비 등 비교적 개선 가능성이 있는 오류 성격의 이슈가 주로 식별되는 반면, 상장폐지 기업에서는 재무보고 신뢰성과 거버넌스에 보다 근본적인 영향을 미치는 취약점이 상대적으로 더 많이 나타난다는 점을 시사한다.

특히 부정은 개별 통제 미비를 넘어 거버넌스, 내부감시, 조직문화 등 보다 구조적인 문제로 확장될 가능성이 높다는 점에서, 기업의 지속가능성에 보다 직접적인 영향을 미치는 핵심 위험 신호로 해석될 필요가 있다.

이러한 맥락에서, 2019년부터 2022년까지 내부회계관리제도 의견변형을 받은 후 상장폐지된 기업을 대상으로 자금통제 미비 관련 지적사항을 추가로 살펴보면 다음과 같이 분류된다.

표 8. **내부회계관리제도 의견변형 이후 상장폐지 회사의 자금 통제 미비 관련 지적사항 사례**

분류	미비점 지적사례
자금·투자거래의 타당성 검토 및 승인	• 자금·투자 및 자산 취득·처분 거래의 타당성 및 회수가능성 검토 통제 미흡 • 주요 거래에 대한 내부 승인절차 부재
특수관계자 및 관련 자금거래 관리	• 특수관계자 범위 및 거래내역 식별·관리 미흡 • 관련 거래의 성격·조건 및 회수가능성·공시 적정성 검토 부족
자금거래의 회수가능성 및 사후관리	• 자금대여·선급금 거래의 회수가능성 검토 및 사후 관리 미흡 • 자금 사용 목적 불명확 거래에 대한 회수 모니터링 부족
자금 인출·집행 및 지출 프로세스	• 자금 인출·지출 승인 절차 및 관련 통제 미흡 • 결산 및 재무보고 과정에서 자금거래의 인식·측정 및 재무제표 반영 적정성 저해
법인인감 및 인증수단 관리	• 법인인감 및 관련 증빙 사용 이력 관리 미흡 • 인감 사용에 기반한 자금집행 통제 부족

전반적으로 내부회계관리제도 의견변형이 상장폐지의 직접적인 원인이라고 단정하기는 어렵다. 다만 내부회계관리제도 의견변형 이후 상장이 폐지된 회사의 비율이 매우 높다는 사실은 자금·투자거래의 타당성 검토, 특수관계자거래 관리, 감사범위 확보와 같은 핵심 통제 영역에서 반복적으로 식별되는 미비는 상장폐지와 같은 사후 리스크와 상당 부분 연계되는 중요한 경고 신호로 해석될 수 있다. 특히 이러한 미비점은 자금의 회수가능성, 재무보고의 신뢰성, 계속기업가정 등과 밀접하게 연결된다는 점에서 기업의 지속가능성에 미치는 영향이 상대적으로 크다.

최근 다수의 횡령 등 자금통제와 연관된 사건사고로 인한 기업에 미치는 치명적인 영향을 고려할 때 부정위험에 대한 실효적인 내부통제의 적절한 운영과 이에 따른 리스크 관리가 상장 유지에 중요한 요소가 되고 사후약방문식의 대응이 아닌 예방 중심의 일관성 있고 체계적인 리스크 관리체계의 정립과 운영이 필요한 시기이다. 이와 관련하여 실질적인 내부회계관리제도의 운영은 횡령 등 자금 관련 부정위험에 대응하는데 있어 중요한 토대가 되고, 기업이 지속가능한 성장을 하기 위해서는 해당 제도의 지속적인 점검과 개선이 필요하다는 점은 내부회계관리제도의 효익을 다시 한번 시사하는 지점이다.

또한 내부회계관리제도 법제화 및 자금통제 공시가 의무화된 상황에서 자금 통제가 미비하거나 자금 관련 내부통제가 적절하게 설계 및 운영되지 않을 경우, 상장회사의 존속 여부에 중대한 영향을 미칠 수 있다는 점에서 그 중요성은 더욱 부각된다. 궁극적으로 회사의 생존 및 기업의 지속 성장에 있어서 실질적인 리스크 관리체계를 운영함이 필요한 시대가 도래하였다.

5. 결론

2부의 분석 결과, 내부회계관리제도 의견변형은 단순한 감사 결과를 넘어 재무보고 위험, 경영진과 감사(위원회)의 인식 수준, 그리고 기업의 사후 리스크와 연결되는 종합적인 관리 신호로 해석될 필요가 있다. 핵심감사항목과 내부통제 미비가 상당 부분 중첩되고, 내부 평가와 외부감사인의 최종 판단 사이에 여전히 유의미한 간극이 존재하며, 내부회계 비적정의견이 재무제표 감사의견 및 일부 기업의 사후 상장폐지와도 상당 부분 연계된다는 점은 내부회계관리제도가 회사의 지속성장가능성과 거버넌스 수준을 함께 비추는 지표임을 보여준다.

이러한 결과는 경영진과 감사(위원회)가 내부회계관리제도를 단순한 준수 체계나 회계부서의 운영 과제로만 보아서는 충분하지 않음을 시사한다. 향후에는 핵심감사항목과 내부통제 취약영역을 통합한 리스크 관점에서 중요 판단영역을 선제적으로 점검하고, 경영진의 운영실태보고와 감사(위원회)의 평가가 외부감사인의 시각과 실질적으로 연결될 수 있도록 감독 체계를 고도화 할 필요가 있다. 결국 내부회계관리제도의 실효성은 통제의 존재 여부보다 재무보고 리스크 및 내부통제에 대해 얼마나 적절하게 변화관리하고 운영하며 모니터링하는지 등 전반적인 내부회계관리제도의 실효성 있는 운영에 의해 그 성과가 좌우될 것이다.

이제 리스크 관리, 즉 내부통제는 선택이 아닌 생존의 문제이고 새로운 기회이자 성장의 전환점이 될 수 있으며 기업 및 임직원의 충분한 주의 의무(Due care)를 입증하는 최적의 솔루션이다.

03

사이버시큐리티와 내부통제

- 왜 지금, '사이버시큐리티와 내부통제'인가?
- 내부통제 패러다임의 전환
- 보안사고가 내부통제 목적에 미치는 영향
- 내부통제 목적별 사이버시큐리티 관련 고려사항
- Reporting 목적의 IT Dependency 식별: 완전성·정확성 확보 방안
- 예방–적발–대응(회복) 단계별 내부통제 재구성
- 정보보호 인증체계 비교: ISMS–P vs ISO/IEC 27001 vs SOC 2
- 정보보호목적 SOC 2 인증보고서의 발행 목적과 활용 방안
- 정보보호공시와 내부통제 연계점에 대한 제언
- 맺는말

디지털 전환의 가속화로 기업의 업무 프로세스 전반이 IT 시스템에 의존하게 되면서, 사이버 위협은 더 이상 'IT 부서만의 이슈'가 아닌 재무보고의 신뢰성, 사업의 연속성, 법규 준수 전반을 위협하는 전사적 리스크로 자리잡았다. 그러나 국내 기업의 내부통제는 여전히 재무보고내부통제(ICFR) 중심의 Process-level Control에 머물러 있어, 고도화되는 사이버 위협에 대응하기에 구조적 한계를 드러내고 있다.

본 장에서는 다음 세 가지 핵심 메시지를 제시하고자 한다.

첫째, IT 내부통제의 고도화가 시급하다. 전통적 ITGC(IT General Control)에서 나아가 Cybersecurity Control, IT Application Control(ITAC), IPE(Information Produced by the Entity), IT Dependency를 포괄하는 Cyber-inclusive IT 내부통제로 확장되어야 하며, 이는 COSO 2013, COBIT 2019, NIST CSF 2.0의 통합적 적용을 통해 실현될 수 있다.

둘째, 목적별 통제의 재설계가 필요하다. COSO가 제시하는 세 가지 목적 – Reporting, Operations, Compliance – 각각에 대해 사이버 위협이 영향을 미치는 경로가 상이하기 때문에 통제의 설계 관점·테스트 방식·증적 요건 또한 달라져야 한다. 특히 통제의 구조는 예방(Preventive) – 적발(Detective) – 대응·회복(Corrective/Recovery) 전 주기에 걸쳐 균형 있게 구축되어야 한다.

셋째, 정보보호 인증 및 공시와의 유기적 연계가 요구된다. ISMS-P, ISO/IEC 27001, SOC 2 인증의 특성을 전략적으로 활용하고, 특히 정보보호공시의 신뢰성 제고를 위해 재무보고에 준하는 수준의 통제가 설계·운영되어야 한다.

이러한 변화를 통해 기업은 감사계획의 최적화, 사이버 복원력 제고, 정보보호공시의 신뢰성 확보를 달성하고, 궁극적으로 이해관계자의 신뢰(Trust)를 증대시킬 수 있을 것이다.

왜 지금, '사이버시큐리티와 내부통제'인가?

사이버 위협 환경의 변화와 내부통제의 한계

기업의 내부통제는 2001년 Enron 사태 이후 SOX법 제정을 계기로 재무보고의 신뢰성 확보에 초점을 맞추어 발전해 왔다. 국내에서도 2018년 외부감사법 전면 개정 이후 내부회계관리제도(ICFR)가 감사 대상으로 전환되면서 Process-level Control과 이를 지원하는 ITGC가 정착되었다.

그러나 지난 수년간 기업 환경은 근본적으로 달라졌다.

- Digital Transformation의 가속화: 클라우드, SaaS, AI, RPA의 광범위한 도입으로 업무의 IT 의존도가 급증하였다. 과거 ERP 중심이었던 In-scope 시스템은 수십 개의 클라우드 서비스, API 연계 시스템, End-User Computing(EUC)으로 확장되었다.
- Threat Landscape의 고도화: Ransomware[1], Supply Chain Attack[2], Insider Threat[3], Zero-day 공격[4] 등 위협의 유형과 파급력이 과거와 비교할 수 없을 만큼 진화하였다. 한 건의 사고가 수일간의 업무중단, 수백억 원의 피해, 주가 하락으로 이어지는 사례가 빈발하고 있다.
- Regulatory Pressure의 강화: 개인정보보호법, 전자금융거래법, GDPR, 미국 SEC의 사이버보안 공시 규정, 국내 정보보호공시제도 등 규제가 다층화되고 있다.
- Stakeholder Demand의 변화: 투자자와 고객은 기업의 ESG 및 Cyber Resilience를 평가 요소로 본격 반영하기 시작했으며, B2B 거래에서 공급망 실사(Third-Party Risk Management) 요구가 표준화되고 있다.

이러한 환경 변화에도 불구하고 다수 기업의 내부통제는 여전히 재무보고 신뢰성에 한정된 정적(static) 체계에 머물러 있어, 빠르게 진화하는 동적(dynamic)·지능형 사이버 위협에 효과적으로 대응하지 못하는 한계를 보이고 있다.

1. Ransomware: 시스템 또는 데이터 암호화 후 복호화를 대가로 금전 요구
2. Supply Chain Attack: S/W 개발사 또는 협력업체 등 신뢰하는 공급망을 통한 표적 공격
3. Insider Threat: 내부직원, 협력사 등 정당한 접근권한을 가진 사람이 일으키는 보안 위협
4. Zero-day 공격: 아직 패치가 공개되지 않은 미공개 취약점을 악용하는 공격

내부통제 패러다임의 전환

1. 기존 내부통제(내부회계관리제도)의 구조적 한계

국내 기업이 운영 중인 내부회계관리제도는 COSO Framework를 기반으로 Entity-level Control, Process-level Control, ITGC로 구성되어 있으나, 각각의 통제활동은 재무보고 목적으로 설계 및 운영되고 있기 때문에 실무에서 다음과 같은 한계가 나타나고 있다.

첫째, 통제의 초점이 '재무제표 숫자의 왜곡 방지'에 국한되어 있다. 따라서 보안사고로 인한 업무중단, 개인정보 유출, 영업비밀 침해 등과 같은 운영 또는 준법과 관련된 리스크는 기존 내부통제(내부회계관리제도)의 직접적 관심 대상에서 제외되어 왔다.

둘째, ITGC의 범위가 전통적 4대 영역(접근관리·변경관리·운영관리·개발관리)에 한정되어 있다. 접근관리 또는 운영관리 영역에 포함될 수 있는 네트워크 보안, Endpoint 보안[5], 위협탐지(SIEM[6]/EDR[7]), Cloud 보안 구성, Supply Chain 보안 등은 ITGC 평가에서 제대로 다루어지지 않는 경우가 많다.

셋째, IT Dependency 식별의 일관성·완전성 부족이다. 자동화통제와 IPE가 사용되는 통제활동에 대해 IT 의존성의 유형과 수준이 체계적으로 정밀하게 식별되지 않아, In-scope Application 선정이 불완전해지고 감사 증거의 신뢰성이 저하되는 사례가 발생한다.

5. Endpoint 보안: 네트워크에 연결된 최종사용자 기기 보안
6. SIEM: Security Information and Event Management
7. EDR: Endpoint Detection and Response

2. IT 내부통제의 고도화 방향

이러한 한계를 극복하기 위해서는 내부통제의 대상과 관점을 지금까지의 재무보고 중심의 IT내부통제에서 사이버 보안 통제를 통합하는 Cyber-inclusive IT내부통제로의 전환하는 것이 필요하다.

구분	As-Is (전통적 내부통제)	To-Be (Cyber-inclusive IT내부통제)
통제 대상	Process 위주	Process + Cyber + Data + Infrastructure
IT 통제 범위	전통적 ITGC 4대 영역 + ITAC	ITGC (+ Cybersecurity Control) + ITAC
목적	Reporting(ICFR) 중심	Reporting + Operations + Compliance
Cyber 반영	제한적	전면적
프레임워크	COSO 중심	COSO × COBIT × NIST CSF 통합

통합 프레임워크의 관점에서 COSO 2013은 내부통제의 목적과 구성요소를 정의하고, COBIT 2019는 IT 거버넌스의 프로세스 참조 모델을 제공하며, NIST CSF 2.0은 Govern·Identify·Protect·Detect·Respond·Recover의 6대 기능을 통해 사이버 리스크 관리를 위한 구체적인 통제 항목 체계를 제공한다. 이 세가지 프레임워크를 상호보완적으로 적용함으로써, 기업은 '재무보고 신뢰성'이라는 종래의 목적을 넘어 보안사고 발생 시 대응 과정, 그리고 사고의 영향을 최소화하는 사이버 복원력(Cyber Resilience)까지 확보할 수 있다.

보안사고가 내부통제 목적에 미치는 영향

1. COSO 3대 목적별 영향 경로의 차별성

보안사고가 발생했을 때 그 영향은 COSO의 세 가지 목적에 대해 서로 다른 경로와 강도로 나타난다.

1.1 Reporting(ICFR) 영향

재무정보의 신뢰성은 ① 데이터 무결성(Integrity), ② 데이터 가용성(Availability), ③ IPE의 신뢰성(Report Reliability), ④ 권한 통제(Authorization)를 통해 확보된다. 보안사고는 이 네 가지 축 중 하나 이상을 훼손함으로써 재무보고의 신뢰성에 영향을 미치게 된다. 예를 들어 Ransomware로 인해 원장 데이터가 암호화되면 가용성·무결성이 동시에 훼손되고, Insider의 권한 남용은 승인통제의 실효성을 무력화한다.

1.2 Operations 영향

COSO Framework상 Operations 목적은 운영의 효과성·효율성, 자산 보호, 사업 연속성 확보를 지향하며, 보안사고는 이 네 가지 차원 모두에 직접적 충격을 가한다. Reporting 영향이 결산·공시 시점에 평가되는 정적·불연속적인 성격을 갖는 반면, Operations 영향은 사고 발생 즉시부터 진행되는 동적·연속적 성격을 가지며, 정량적 손실(매출 감소·복구 비용)과 정성적 손실(평판·고객 신뢰)이 복합적으로 작용한다.

구체적으로는 ① 생산·서비스·결제 시스템 중단으로 인한 사업 단절, ② 포렌식·복구·법률자문 등 직간접 대응 비용, ③ 영업비밀·고객정보·OT 설비 등 자산 손실, ④ 고객 이탈과 브랜드 가치 하락에 따른 평판 훼손, ⑤ M&A·해외진출 차질 등 전략적 경쟁력 저하의 다섯 가지 경로로 영향이 전이되며, 이러한 영향은 산업 특성에 따라 강도와 형태가 달라지게 된다. 제조·에너지는 OT 정지와 설비 손상이, 금융은 거래 중단과 시장신뢰 훼손이, SaaS·유통은 다수 고객 동시 영향이 핵심 리스크로 부각될 수 있다.

또한 Reporting 영향이 재공시·정정으로 일부 회복 가능한 반면, Operations 영향은 시장점유율과 고객 신뢰의 영구적 손실로 이어질 수 있어 회복 비용의 비대칭성이 크다는 점에서 본질적으로 구분된다. 따라서 Operations 목적의 통제는 '침해는 반드시 발생한다'는 'Assume Breach' 전제 하에 Resilience-by-Design 원칙[8]으로 설계되어야 하며, 복구시간(RTO) 및 복구시점(RPO) 기반의 차등 복구 체계, 24×7 실시간 탐지·대응, 사이버 시나리오를 포함한 BCP(사업연속성계획) 통합운영, 제3자·공급망 운영 리스크 관리가 핵심 통제 요소로 자리잡아야 한다.

8. Resilience-by-Design(설계 단계의 복원력 내재화) 원칙: 시스템 또는 프로세스를 처음 설계할 때부터 '장애와 침해가 발생하더라도 핵심 기능은 지속되고, 신속히 회복될 수 있도록' 복원력을 내장(built-in)하는 원칙

1.3 Compliance 영향

COSO Framework상 Compliance 목적은 기업 활동이 관련 법령·규제·내부정책을 준수하도록 보증하는 것을 지향하며, 보안사고는 다층적 규제 의무를 동시다발적으로 촉발시킨다는 점에서 Reporting 및 Operations 영향과 본질적으로 구별된다. Reporting 영향이 재무수치의 신뢰성에, Operations 영향이 사업 연속성에 집중되는 반면, Compliance 영향은 법적 의무 이행의 적시성과 적정성에 좌우되며, 위반 시 금전적 제재(과징금)뿐 아니라 행정처분, 형사책임, 집단소송 등으로 확장된다는 특징을 갖는다.

구체적 영향 경로는 ① 개인정보보호법상 정보주체 통지(72시간) 및 감독기관 신고 의무, ② 전자금융거래법·신용정보법상 사고보고 및 이용자 보호조치 의무, ③ GDPR·CCPA 등 역외 규제의 통지·과징금(글로벌 매출의 최대 4%) 의무, ④ 미국 SEC의 사이버사고 4영업일 내 공시 의무 등 국내외 규제, ⑤ 계약상 비밀유지·SLA 위반에 따른 손해배상 책임의 다섯 가지로 요약된다. 또한 보안사고는 단일 규제가 아닌 복수 규제의 동시 적용을 야기하므로, 사고 발생 시점부터 통지·신고·증적 보존·이해관계자 커뮤니케이션을 병행 수행할 수 있는 통합 대응 역량이 요구된다.

특히 Compliance 영향은 사고 자체의 규모보다 대응의 적시성과 문서화 수준에 따라 제재 강도가 크게 달라지므로, 사고 대응 과정 전반의 증적이 곧 규제 방어의 핵심 자료가 된다는 점에 유의해야 한다. 따라서 Compliance 목적의 통제는 ① 적용 규제의 사전 식별 및 의무 매핑(Regulatory Inventory), ② 사고 유형별 통지·신고 Playbook과 법무 협업 체계, ③ 증적의 자동수집·보존 체계, ④ 정기적 규제 변화 모니터링과 통제 업데이트 절차를 포함하여, 사고 발생 시 '무엇을, 누구에게, 언제까지, 어떻게 보고할 것인가' 가 즉시 작동되도록 설계되어야 한다.

2. 사고 유형별 영향 매트릭스

사이버 보안 사고는 그 유형에 따라 조직에 미치는 영향의 성격과 강도가 상이하므로, 단일한 관점이 아닌 재무보고 내부통제(ICFR), 운영(Operations), 컴플라이언스(Compliance) 등 다차원적 관점에서 영향도를 평가할 필요가 있다. 동일한 사고라 하더라도 어떤 영역에서는 치명적인 영향을 초래하는 반면, 다른 영역에서는 상대적으로 영향이 제한적일 수 있기 때문이다. 따라서 각 사고 유형별로 영향이 집중되는 영역을 사전에 식별하고, 이에 부합하는 통제 활동과 대응 자원을 차등적으로 배분하는 것이 중요하다. 아래 표는 대표적인 사이버 보안 사고 유형별로 세 가지 관점에서의 영향도를 High·Medium·Low 수준으로 구분하여 정리한 것이다.

사고 유형	Reporting (ICFR)	Operations	Compliance
Ransomware	◐ 데이터 가용성·무결성 훼손	● 업무중단·복구비용	◐ 신고의무·피해통지
Data Breach	○ IPE 신뢰성 일부	◐ 서비스 영향	● 개인정보·GDPR 위반
Insider Threat	● 권한남용·부정보고 위험	◐ 자산유출	◐ 규정위반
Supply Chain Attack	◐ 외부위탁 데이터 신뢰성	● 연쇄장애	● 3rd Party 규제

범례: ● High ◐ Medium ○ Low

3. 시사점

위 매트릭스는 동일한 보안사고라도 어떤 목적에 더 큰 영향을 미치는지가 사고 유형과 시스템의 성격에 따라 달라진다는 것을 보여준다. 따라서 통제는 "어느 하나의 목적만을 위한 일원적 통제"가 아니라, "목적별 레이어(Layered)로 중첩 설계된 통제"로 구축되어야 한다. 이는 곧 하나의 통제 조치(예: 접근권한 관리)가 세 가지 목적 각각에서 어떤 Assertion과 Risk에 대응하는지를 명확히 매핑하는 작업을 요구한다.

내부통제 목적별 사이버시큐리티 관련 고려사항

1. Reporting 목적 통제

보고 목적의 통제는 재무정보의 신뢰성을 지향한다. 따라서 사이버 통제 역시 '재무보고에 영향을 줄 수 있는 시스템과 데이터'에 초점을 맞춘다.

- In-scope System 내 Cyber 통제: 재무보고 관련 시스템(General Ledger, Sub-ledger, Consolidation 등)과 그에 연계된 Interface·Feeder System에 대한 보안통제 적용
- 데이터 무결성 및 IPE 신뢰성 확보: Input·Processing·Output 전 단계의 무결성 통제, Report Logic·Parameter의 정확성 검증
- 변경관리·접근권한·로깅·직무분리: 재무시스템에 대한 변경의 사전 승인, 권한 부여·회수, 권한 남용 탐지, SoD(Segregation of Duties) 운영
- 자동화통제(ITAC) 효과성: 자동계산, 자동승인 규칙의 설계·운영 효과성 테스트

2. Operations 목적 통제

운영 목적의 통제는 연속성과 복원력을 지향한다.

- BCP / DR / Cyber Resilience: 재해복구계획, 백업·복구 테스트, RTO/RPO 관리
- Security Operation Center, SOC, 24×7 운영: 실시간 보안관제, Alert Triage, Escalation Process
- Threat Intelligence 연동: 외부 위협정보를 SIEM과 연동하여 신속한 탐지·차단
- Incident Response Playbook: 사고 유형별 대응 시나리오, Crisis Communication 프로토콜
- 취약점·패치 관리: 정기 취약점 스캐닝, 우선순위 기반 패치 적용

3. Compliance 목적 통제

준법 목적의 통제는 규제 준수와 증적 관리를 지향한다.

- 개인정보보호법·전자금융거래법 대응 통제: 개인정보 처리방침 관리, 접근기록 보존, 암호화 등
- GDPR·해외이전·국외규제 대응: 국외이전 적법근거, SCC(Standard Contractual Clauses) 관리, 72시간 통지 프로세스
- 증적관리 및 감사대응: 통제 증적의 자동수집·저장, 규제당국 제출 자료 준비 체계
- 내부신고·Whistleblowing: 독립적 신고 채널, 제보자 보호, 조사 절차

Reporting 목적의 IT Dependency 식별: 완전성·정확성 확보 방안

1. IT Dependency 식별의 중요성

IT Dependency란 통제활동이 IT 시스템·데이터·산출물에 의존하는 정도와 유형을 의미한다. 이는 내부회계관리제도 운영의 출발점이며, 동시에 외부감사인의 감사계획을 결정하는 핵심 요소이다.

IT Dependency 식별이 불완전하거나 부정확할 경우, 중요한 시스템이 In-scope에서 누락되고, 자동화통제의 유효성이 잘못 평가되며, IPE의 신뢰성에 대한 근거가 약화된다. 그 결과 감사인은 통제의존(reliance on controls) 수준을 낮추고 실증절차(substantive test)의 범위를 확대하게 되어, 감사 범위와 비용이 증가한다.

2. 완전성(Completeness) 확보 방안

완전성은 '누락되지 않음'을 의미하며, 이를 확보하기 위해서는 다음과 같은 네 가지 접근을 병행할 필요가 있다. 첫째, Top-down 접근 방식을 통해 재무제표에서 출발하여 계정과목, Assertion(실재성·완전성·정확성·평가 등), Process, System 순으로 역추적함으로써 각 Assertion에 영향을 미치는 시스템을 체계적으로 식별한다. 둘째, 업무기술서에 기재된 시스템과 실제 Data Flow Diagram상의 시스템을 상호 비교·검증하는 교차검증을 수행하여 인벤토리 상의 누락을 탐지한다. 셋째, 공식 IT 인벤토리에 등재되지 않은 Shadow IT, EUC(End User Computing), SaaS 등의 자산을 식별하기 위해 네트워크 디스커버리 도구를 활용하거나 SaaS 구독료 등 지출계정을 분석하고, 사업부 대상 설문을 병행하는 등 다각적인 식별 체계를 구축한다. 마지막으로, 사업부·IT·재무·내부감사 부서가 공동으로 참여하는 합동 인벤토리 검증을 연 1회 이상 정기적으로 수행하여 In-scope 시스템 인벤토리의 완전성을 최종적으로 확인한다.

3. 정확성(Accuracy) 확보 방안

정확성은 'IT Dependency의 유형이 올바르게 분류됨'을 의미한다.

3.1 IT Dependency 유형 분류 체계

유형	설명	검증 초점
Automated Control	시스템이 자동으로 수행하는 통제	Configuration 설정, Change Log
System-generated Report	시스템이 생성한 IPE 기반 정보	Report Logic, Parameter, Source Data
Interface	시스템 간 데이터 연계	전송 완전성·정확성
Calculation	시스템 자동계산	계산 로직, 입력 데이터
RA/SoD	시스템, 프로그램 및 데이터 접근	권한보유자 적정성 및 업무분장

3.2 IPE 완전성·정확성 테스트

통제 수행 과정에서 활용되는 시스템 산출물(IPE)에 대해서는 해당 자료가 모집단을 누락 없이 포함하고 있는지(완전성)와 추출된 데이터가 원천 시스템의 값과 일치하는지(정확성)를 검증한다. 이를 위해 보고서 생성 시 사용된 추출 조건(쿼리, 파라미터, 기준일자 등)의 적절성을 확인하고, 원천 데이터와 산출물 간 건수 및 주요 금액 항목의 대사(Reconciliation)를 수행한다. 또한 보고서를 생성하는 프로그램의 변경 이력 및 접근 권한 통제가 적절히 운영되고 있는지를 함께 점검하여, IPE 산출 과정 전반의 신뢰성을 확보한다. 필요 시 표본을 추출하여 원천 데이터(예: ERP 원장, 거래 로그 등)와의 일치 여부를 재수행 테스트(Re-performance)하며, 테스트 결과는 증빙과 함께 문서화하여 감사 추적이 가능하도록 관리한다.

4. In-scope Application 선정 및 감사계획 연계

IT Dependency 식별 결과는 다음의 순차적 의사결정으로 이어진다.

- Step 1. IT Dependency 식별 → Process와 System 간 Mapping
- Step 2. Key Report / Key System 선정 → In-scope Application 확정
- Step 3. ITGC 테스트 범위 결정 → 설계·운영 효과성 테스트
- Step 4. 전반 감사계획 수립 → Scope·Resource·Timeline 확정

결과적으로 IT Dependency 식별의 품질은 In-scope Application 선정 → ITGC 테스트 범위 → 감사계획 전반으로 파급되므로, 이를 연초 감사 프로세스의 출발점으로 위치시키고 감사인과의 사전 공유 및 합의 과정을 제도화하는 것이 바람직하다.

예방-적발-대응(회복) 단계별 내부통제 재구성

기존의 내부통제가 '재무보고 신뢰성'이라는 단일 목적에 집중해왔다면, 앞으로의 내부통제는 사업의 연속성과 법규 준수까지 포괄해야 하며, 이를 위해 통제의 구조를 예방(Preventive)–적발(Detective)–대응·회복(Corrective/Recovery)의 전 주기로 재편할 필요가 있다. 이는 NIST CSF 2.0의 Identify, Protect, Detect, Respond, Recover 프레임과 본질적으로 동일한 접근이다.

1. Preventive Controls (예방)

예방 통제는 '사고가 발생하지 않도록' 하는 사전 차단 장치이다. 운영 및 준법 목적의 통제 설계에서 가장 기본적이면서도 핵심적인 축이다.

- IAM(Identity & Access Management) / PAM(Privileged Access Management): 계정 생애주기 관리, 최소권한 원칙, 특권계정의 별도 관리·모니터링
- 변경관리/SDLC 보안: 개발–테스트–운영 환경 분리, 보안 설계 검토(Security by Design), 코드 리뷰 및 SAST[9]/DAST[10] 적용
- 네트워크·Endpoint 보안: Zero Trust 기반 네트워크 분할, EDR 배포, 단말 암호화
- 보안 아키텍처 설계: 클라우드 보안 기준(CSP Baseline), 제로 트러스트 원칙의 내재화
- 보안 교육 및 인식 제고: 피싱 모의훈련, 임원진 대상 Tabletop Exercise, 전사 의무교육

9. SAST: Static Application Security Testing(정적분석) – 소스코드 분석 방식
10. DAST: Dynamic Application Security Testing(동적분석) – 실행중인 어플리케이션에 대한 모의공격을 통해 분석 방식

2. Detective Controls (적발)

적발 통제는 '이상(abnormal)'을 신속히 감지하는 장치이다. 위협이 실제 피해로 이어지기 전에 탐지하고 대응 프로세스를 가동하는 Trigger 역할을 수행한다.

- SIEM/UEBA(User and Entity Behavior Analytics)/EDR: 로그 통합 수집·상관분석, 사용자·엔티티 행위 기반 이상탐지
- 로그·이상징후 모니터링: 권한남용, 비정상 시간대 접근, 대용량 데이터 이동 등 Trigger Rule 운영
- 취약점 점검/모의해킹: 정기 VA(취약점평가)/PT(침투테스트), Red Team 평가, Bug Bounty(취약점신고 시 포상금 지급)

구분	수행 주체	방식	주기
VA/PT	내부팀·전문 컨설팅사	정형화된 점검	정기(분기/연 단위)
Red Team	전문 공격팀(내·외부)	시나리오 기반 실전 모의	비정기(연 1회 등)
Bug Bounty	불특정 외부 연구자	상시 제보·포상	상시 운영

- 내부감사·통제 테스트: Continuous Auditing, Key Control의 운영 효과성 테스트
- Threat Hunting: 알려진 위협뿐 아니라 Unknown Threat에 대한 가설 기반 능동 탐색

3. Corrective/Recovery Controls (대응·회복)

대응·회복 통제는 '사고가 발생한 후'의 피해 최소화와 정상화를 지향한다. 최근 규제당국과 이해관계자는 예방·적발뿐 아니라 Recovery 능력을 별도로 평가하고 있다.

- Incident Response Plan: 사고 유형별 대응 시나리오, 역할·책임(RACI), 의사결정 권한
- BCP/DR/백업 복구: Immutable Backup(불변백업), 연 1회 이상 실제 복구 훈련
- Crisis Communication: 규제기관·고객·언론 대상 커뮤니케이션 프로토콜, 대변인 사전 지정
- Cyber Resilience: 사고 발생을 전제로 한 복원력 중심 설계(Assume Breach)
- Lessons Learned & 개선: 사후검토(Post-Incident Review), 재발방지 계획의 이사회 보고

4. 3단계 통제의 통합 운영 모델

세 단계 통제는 독립적으로 운영되는 것이 아니라 거버넌스–지표–보고–개선의 순환 구조 속에서 통합되어야 한다.

- 거버넌스: 정보보호위원회, 리스크관리위원회, 감사위원회 간 연계 보고 체계
- KRI/KPI: 예방(패치율·교육이수율), 적발(MTTD, 평균탐지시간), 대응(MTTR, 평균대응□복구시간) 등 단계별 핵심지표 정의
- 3-Line Model: 현업(1선)–리스크·정보보호(2선)–내부감사(3선)의 명확한 역할 분담
- 지속적 개선 루프: 사고·점검 결과를 통제 개선·리스크 평가에 활용(Feedback Loop)

정보보호 인증체계 비교: ISMS-P vs ISO/IEC 27001 vs SOC 2

정보보호 인증은 기업의 통제 체계에 대한 외부 검증 수단이자, 고객·규제당국·투자자에게 신뢰를 전달하는 중요한 커뮤니케이션 도구이다. 그러나 인증별로 목적·적용 범위·테스트 방식이 상이하므로, 무엇을 언제 어떻게 취득할 것인지에 대한 전략적 접근이 필요하다.

1. 인증별 특성 비교표

구분	ISMS-P	ISO/IEC 27001	SOC 2
발급·기준	KISA/정보통신망법 기반 국내 법정 의무(일부 대상)	ISO/국제표준 자율 인증	AICPA SSAE 18 독립 감사인 발행
적용 범위	정보보호 + 개인정보보호 (통합)	정보보안경영시스템 전반	Trust Services Criteria(5): Security·Availability·Confidentiality· Processing Integrity·Privacy
테스트 방식	서면·현장 심사 (점검 + 인증심사, 시점)	적합성 심사 (시점 + 사후관리심사)	Type Ⅰ: 설계(시점) Type Ⅱ: 일정기간(통상 6~12개월) 운영효과성
산출물	인증서	인증서	감사보고서(Attestation Report)
주요 활용	국내 규제 대응·의무 준수	글로벌 B2B 신뢰 프로세스 성숙도 입증	B2B SaaS·공급망 실사 글로벌(미주) 고객 대응
갱신	3년 / 연 사후심사	3년 / 연 사후심사	연 1회 갱신 발행

2. 테스트 방식(Assessment Approach)의 차이

세 인증의 가장 본질적인 차이는 테스트 방식에 있다.

- ISMS-P: 법정 점검 및 인증심사를 결합한 형태로, 대체로 특정 시점의 적합성을 확인한다. 심사기관이 수행하며 공적 성격이 강하다.
- ISO 27001: ISMS의 설계 및 지속 운영의 적합성 심사로, 시점 인증 후 사후관리심사(Surveillance Audit)를 통해 지속성을 유지한다.
- SOC 2: AICPA의 감사기준(SSAE 18)에 따라 수행되는 독립감사로, Type Ⅰ은 특정 시점의 설계 적정성을, Type Ⅱ는 일정 기간(통상 6~12개월) 동안의 운영 효과성을 검증한다. 즉 SOC 2 Type Ⅱ는 ICFR 감사와 유사하게 '기간 중 통제가 효과적으로 작동했는가'를 증거 기반으로 입증한다.

3. 최근 동향

- SOC 2 Type Ⅱ 요구의 확산: 글로벌 B2B·SaaS 시장에서 공급망 실사의 표준 요구사항으로 자리잡는 추세이며 대기업 구매조건에 명시되는 사례 증가
- ISMS-P와 ISO 27001 연계 심사: 중복 심사 부담을 줄이기 위한 통합 심사·동시 취득 활성화
- ISO 27001:2022 개정 반영: 통제 항목이 114개에서 93개로 재편(4 Theme: Organizational/ People/Physical/Technological), Threat Intelligence·Cloud 보안 등 신규 통제 추가
- AI·클라우드·공급망 리스크 통제 강화: 세 인증 모두 AI 거버넌스, Cloud Shared Responsibility, Third-party Risk에 대한 요구 수준을 높이고 있음

정보보호목적 SOC 2 인증보고서의 발행 목적과 활용 방안

1. SOC 2 발행 목적

SOC 2는 AICPA가 정의한 Trust Services Criteria(TSC)에 대한 독립감사인의 감사보고서로서, 서비스 조직이 고객의 데이터·서비스를 어떻게 안전하게 관리하고 있는지를 외부에 입증하는 도구이다.

Trust Services Criteria(TSC)

- Security (공통 필수): 무단 접근 및 공격으로부터의 시스템 보호
- Availability: 합의된 수준의 가용성 확보
- Confidentiality: 기밀정보의 보호
- Processing Integrity: 처리의 완전성·정확성·적시성
- Privacy: 개인정보의 수집·이용·파기 적정성

기업은 자사 서비스의 성격에 따라 Security(필수)에 더해 Availability, Confidentiality, Processing Integrity, Privacy 원칙의 통제활동을 선택적으로 결합하여 범위를 설정한다.

2. 활용 방안

- B2B 영업 및 RFP 대응: 글로벌 고객, 특히 미국 소재 이용자기업의 보안 질의서(Security Questionnaire) 응대 부담을 획기적으로 감소시키는 Trust 증빙
- 공급망 실사 / Third-Party Risk Management(TPRM) 대응: 공급자 평가 절차에서 SOC 2 Type II 보고서 제출이 표준화되는 추세
- 내부통제 운영 효과성의 외부 검증: 외부 감사인의 감사의견을 통해 경영진·이사회·감사위원회가 내부통제의 성숙도를 객관적으로 점검
- 글로벌 규제 및 해외 진출 대응: 미국 상장 준비, 해외 파트너십, 클라우드 상위 고객사 대응의 공통 언어

3. 국내 기업의 Dual-Track 전략

국내 기업은 ISMS-P(법정 의무)와 SOC 2(선택적 전략)를 이중 트랙으로 운영하는 것이 합리적이다.

구분	Track 1 · ISMS-P	Track 2 · SOC 2 Type II
성격	법정 의무·Baseline	전략적·선택적
목적	국내 규제 준수	글로벌 고객·파트너 Trust
대상	국내 ISP·주요 정보통신서비스 제공자 등	B2B SaaS·해외 매출 비중 기업
활용	규제 이행 입증	공급망 실사·해외 영업·상장 준비

두 인증을 통합적으로 관리하면 공통되는 통제 영역(접근통제, 변경관리, 로그관리 등)의 증적을 공유할 수 있어 운영 효율도 제고된다.

정보보호공시와 내부통제 연계점에 대한 제언

1. 정보보호공시 제도 개요 및 한계

정보보호공시제도는 기업이 정보보호 투자·인력·인증 현황을 공시하도록 하여 이해관계자의 알 권리를 충족시키고 자율적 보안 투자를 유인하는 데 목적이 있다. 그러나 공시 수치의 산정 기준이 회사마다 상이하고, 작성 및 분류 절차와 관련 정보의 생성과정에 존재하는 내부통제 유무에 따라 신뢰성에 편차가 존재한다.

특히 공시의 핵심 항목인 '정보보호 투자액'은 정보기술(IT) 부문 지출과 정보보호 부문 지출을 구분하여 집계하는데, 두 부문 각각에서 서로 다른 방향의 리스크가 존재한다.

2. 투자액 산정의 이중 리스크

2.1 정보기술(IT) 부문 – 완전성(Completeness) 리스크/과소계상 위험

정보기술(IT) 성격의 지출임에도 불구하고 일반 운영비용·관리비용 등으로 분류되어 정보기술 투자액 집계에서 누락되는 경우이다. 예컨대 현업 부서가 자체 예산으로 직접 도입·운영하는 SaaS 구독료, 사업부 비용으로 처리되는 EUC(End User Computing) 도구 구입비, 일반 사무용 소프트웨어 라이선스 비용, 외주 용역비 내에 포함된 IT 개발·유지보수 비용 등이 IT 예산이 아닌 각 사업부의 일반 경비로 집계되어 정보기술 투자액에서 빠지는 상황이 이에 해당한다. 이러한 누락은 분모인 정보기술 투자액을 과소계상하게 만들어, 결과적으로 정보보호 투자액 비율(정보보호 투자액/정보기술 투자액)이 실제보다 높게 나타나는 왜곡을 초래할 수 있다.

2.2 정보보호 부문 – 실재성(Existence) 리스크/과대계상 위험

반대로, 정보보호와 직접적 관련이 없는 비용이 정보보호 투자액에 포함되어 부풀려지는 경우이다. 예컨대 일반 IT 인력의 인건비 일부를 보안 인력으로 계상하거나, 보안 기능이 부수적인 솔루션 전체를 보안 투자로 집계하는 사례이다. 이는 공시 수치를 과대계상하게 만드는 위험이다.

3. 리스크별 통제활동 제안 (Control Design Recommendation)

두 리스크를 감소시키기 위해 기업은 다음과 같이 이중의 통제를 설계·운영해야 한다.

3.1 IT 부문 과소계상(완전성) 리스크 대응 통제

#	통제활동	기대 효과
①	정보보호 지출 분류기준 정립 및 계정과목 매핑표 운영	보호성 지출의 정의·범위를 사전 확정하여 누락 방지
②	구매·품의 단계 체크리스트 운영 (보안성격 식별 항목)	지출 발생 시점에 보안성격 여부를 식별·Tag
③	CISO와 CFO 교차검토 통제 (공시 前 Reconciliation)	재무적 시각과 보안적 시각의 상호 검증
④	연 1회 전체 IT지출 대비 보호성 지출 재분류 점검	누락된 보호성 지출의 사후 식별·환류

3.2 정보보호 부문 과대계상(실재성) 리스크 대응 통제

#	통제활동	기대 효과
①	증빙 기반 실재성 검증 (계약서·산출물 매핑)	정보보호 활동의 실재 증명 자료 확보
②	정보보호 활동과의 직접 연관성 판정 기준 수립	경계비용(Borderline cost)에 대한 일관된 판단
③	2차 검토 (Second-line: 내부감사 / Compliance)	보안부서(1선)와 독립된 검토 라인 확보
④	공시 前 경영진 확인서(Management Representation) 및 외부 검증	공시 수치에 대한 경영진 책임·외부 객관성 확보

4. 거버넌스 차원의 제언

정보보호공시는 비재무적 공시로 분류되지만, 그 수치는 투자자·규제당국의 중요한 의사결정 근거가 된다는 점에서 재무보고에 준하는 통제 수준을 적용하는 것이 바람직하다.

- 공시 수치에 대해 내부회계관리제도에 준하는 '설계–운영–평가–보고'의 통제 프레임 적용
- 정보보호위원회와 내부회계관리위원회 간 연계 보고 체계 구축(중복 심의가 아닌 정보 공유·일관성 확보 목적)
- 감사위원회 차원의 정보보호공시 수치 검토 안건화
- 중장기적으로는 정보보호공시의 외부 검증(Assurance) 제도화 검토

맺는말

사이버 리스크 시대에 내부통제는 더 이상 재무보고만을 위한 장치가 아니다. 내부통제는 기업의 지속가능성과 신뢰의 기반이며, 사이버시큐리티는 그 핵심 축이다. 지금 3년의 준비가 향후 10년의 경쟁력을 결정한다는 인식 아래, 경영진·재무·IT·정보보호·감사가 하나의 통제 언어로 소통하고 협업하는 체계를 구축해야 한다. 본 보고서가 그 여정의 실무적 출발점이 되기를 기대한다.

04

전사 리스크 관리체계 정립: 규제 준수에서 '경쟁력'으로

- 전사 리스크 관리체계로의 전환의 시기
- 전사 리스크 관리체계(전사 내부통제)의 효익과 Insight
- 뉴 내부통제 거버넌스 하의 내부통제 운영모델
- 맺는말

최근 기업을 둘러싼 환경 변화와 다수의 사건사고의 결과는 단순한 규제 준수 차원을 넘어, 전사 리스크 관리 역량 자체가 기업의 지속가능성과 경쟁력을 좌우하는 국면으로 급격히 전환되고 있다. 상법 개정, 중대재해처벌법의 시행, 공정거래·개인정보·플랫폼 규제 강화 등은 개별 규정의 추가가 아니라, 기업과 경영진에게 요구되는 책임의 범위와 깊이가 근본적으로 달라졌음을 시사한다.

특히 상법 개정을 통해 이사의 충실의무가 "회사"에서 "회사 및 주주"로 확대되면서, 경영진과 이사회는 결과뿐만 아니라 그 의사결정 과정에서 리스크를 어떻게 인식하고 관리해 왔는지에 대해 설명 가능한 구조를 요구 받고 있다. 이제 내부통제는 형식적으로 '존재하는지 여부'를 넘어, 실제로 작동하고 있는지, 그리고 충분한 주의의무(Due Care)를 다하고 있는지를 입증해야 하는 핵심적인 경영 인프라가 되었다.

이러한 변화 속에서 과거와 같은 사후 대응 중심의 리스크 관리 방식은 명확한 한계를 노출하고 있다. 다수의 사례에서 확인되듯이, 단일 사고나 법규 위반은 재무적 손실을 넘어 평판 훼손, 규제당국 조사, 소송으로 연쇄 확산되며 기업 가치와 경영 안정성을 동시에 위협한다. 그럼에도 불구하고 많은 기업에서는 여전히 리스크 관리가 부서별·사안별로 분절되어 운영되고 있으며, 전사 관점에서 일관된 기준과 책임 구조를 갖추지 못한 경우가 적지 않다.

이러한 환경 변화는 전사 리스크 관리체계로의 전환을 더 이상 "잘하는 기업의 선택 사항"이 아니라, 모든 기업이 직면한 구조적 과제로 만들고 있다. 전사 리스크 관리체계(전사 내부통제)는 재무보고 목적에 한정되었던 기존 내부통제의 범위를 운영 및 법규준수 영역까지 확장하여, 전사 차원에서 리스크를 식별·평가·대응·모니터링하는 통합된 틀을 제공한다. 특히 내부회계관리제도를 통해 축적된 설계·운영·평가 경험은 이러한 전환을 위한 실질적인 기반이 되고 있으며, 이는 새로운 제도의 도입이 아니라 기존 역량의 전략적 확장이라는 점에서 그 의미가 크다.

중요한 점은 전사 리스크 관리체계가 단순히 "규제를 잘 지키기 위한 장치"에 머물지 않는다는 것이다. 실제 사례에서 확인되듯이, 리스크를 조기에 인식하고 관리할 수 있는 체계를 갖춘 기업은 경영 의사결정의 질이 높아지고, 불확실성에 대한 회복탄력성(Resilience)이 강화되며, 이해관계자 신뢰와 시장 평가 측면에서도 긍정적인 효과를 창출하고 있다.

이는 전사 리스크 관리체계가 비용이나 규제 대응 수단이 아니라, 중장기적으로 기업 경쟁력을 강화하는 전략적 자산임을 의미한다.

첫째, 왜 지금 전사 리스크 관리체계로의 전환이 필요한지,

둘째, 전사 리스크 관리체계 즉, 전사 내부통제체계가 실제 업무 현장에서 창출하는 실질적인 효익은 무엇인지,

셋째, 뉴 내부통제 거버넌스 하에서 내부통제가 어떻게 운영되어야 실효성을 가질 수 있는지

를 통해 전사 리스크 관리체계가 규제 준수의 도구를 넘어, 기업의 지속가능성과 경쟁우위를 뒷받침하는 핵심 경영 인프라임을 명확히 제시하고자 한다.

전사 리스크 관리체계로의 전환의 시기

최근 기업을 둘러싼 경영 환경은 과거 어느 때보다 복잡하고 불확실한 리스크 환경으로 변화하고 있다. 재무보고 리스크를 중심으로 설계되었던 기존 내부통제 체계만으로는 운영 리스크·법규준수 리스크·평판 리스크까지 포괄적으로 관리하는 데 구조적 한계가 분명해지고 있다.

특히 최근 상법 개정으로 이사의 충실의무가 "회사"에서 "회사 및 주주"로 확대되면서, 경영진과 이사회·감사위원회가 부담해야 할 책임의 범위가 실질적으로 커졌다. 이러한 변화는 단순히 규정을 준수하는 수준을 넘어, 회사가 리스크를 어떻게 인식하고 관리해 왔는지에 대한 '과정' 자체를 요구하는 방향으로 감독 기조가 이동하고 있음을 의미한다.

즉, 상법 개정의 요구 사항은 이사회 논의, 판단, 결의는 어떻게 이루어지는가, 무엇을 근거로 이루어지는가, 어떻게 확신하는가이고 이에 따라 회사에 이사회 판단 정당성 확보 인프라 구축과 전사적 리스크 관리체계 구축 및 운영을 요구하고 있는 것이다. 더불어 충분한 주의의무 (Due care) 입증 관점에서도 합리적인 근거와 충분한 소통을 통한 이사회 의사결정의 정당성 마련이 필요하다.

외부 환경 변화 및 다수의 사건사고로 인해 리스크 관리의 중요성이 강조되는 이제는 리스크 관리의 패러다임 전환이 절실하게 요구되는 시점이다.

1. 사후 대응 중심 리스크 관리의 한계

다수의 기업에서 여전히 리스크 관리는 사고 발생 이후의 사후 대응 중심으로 이루어지고 있다. 그러나 실제 사례를 살펴보면, 중대재해, 개인정보 유출, 공정거래 위반, 횡령 등 단일 사건이라 하더라도 그 영향은

- 매출 하락 등의 재무손실
- 평판 훼손 및 주가 하락
- 규제기관 조사 및 소송 등으로

연쇄 확산되는 구조를 보이고 있다.

감독당국 역시 개별 사고의 유무보다 사전에 어떤 내부통제 체계를 갖추고 있었는지, 그리고 그 체계가 실제로 작동하고 있었는지를 핵심 판단 기준으로 삼고 있다. 이로 인해, 기존과 같은 분절적·부서별 리스크 관리는 더 이상 효과적인 대응 수단이 되기 어렵다.

기존 일본의 유수 자동차 회사의 가속페달 설계 결함에 따른 인명사고 발생으로 인한 대규모 리콜 사태는 이러한 사후 대응 중심의 리스크 관리의 한계를 명확하게 보여 준다. 해당 회사는 결함을 초기부터 어느정도 인지했으나 예방 목적의 명확한 관련 리스크 관리 체계 정립과 운영, 사전 대응과 전사 공유 없이 사후 대응(리콜, 사과) 중심으로 처리하였으며 이로 인해 사상 최대 리콜, 브랜드 신뢰 급락, 규제·소송 비용 급증 등으로 회사에 치명적인 영향을 주었고 사후 대응 자체는 '늦은 방어'에 불과하며, 신뢰 손상은 회복까지 오랜 시간이 걸린다는 것을 보여 주는 대표적인 사례이다.

국내 기업의 대형 사고들(정보유출·기름 유출·안전사고·식품 이물질 등)의 주요 사유의 공통점은 다음과 같다.

- 잠재적 위험에 대한 사전 계획 부재
- 사고 발생 후에야 조직이 문제의 심각성을 인식
- 위기 대응이 임기응변적·부서 단위로 이뤄짐

결국 사후적으로 사과, 보상, 재발방지 대책을 발표하지만 대부분 근본 원인은 그대로 잔존하고 동일 유형 사고 반복 발생하는 경향이 있다. 사고 이후에야 리스크 관리의 필요성을 인식하는 구조 자체가 리스크임을 보여주고 있다. 또한, 문제는 '몰랐다'가 아니라, '알고도 움직이지 않았다'는 점이다.

표 1. **주요 항목별 사후 대응 중심 리스크 관리의 구조적 한계 요약**

구분	사후 대응 중심 관리의 한계
시점	이미 사고가 발생한 뒤
목적	피해 축소·책임 대응
초점	개별 사건, 특정 부서
의사결정	현장·실무 중심
한계	근본 원인 제거 불가, 반복 발생 가능, 거액의 사후 대응 비용, 평판 훼손

결국 사후 대응은 관리가 아니고 수습에 가까운 조치이므로 그 한계를 인식할 필요가 있다.

2. 전사 리스크 관리체계로의 전환 필요성

최근 다수의 사건사고와 관련된 리스크는 충분히 사전 인지 가능하였으나 경영진이 "설마 발생하겠어", "관리하고 있다고 생각함", "다음 분기에 보자" 등의 판단으로 실질 대응을 미룸으로 돌발적 위기 형태로 사건사고로 이어지고 있다.

최근 사고들은 개별 실패가 아니라 전사 리스크 관리 체계가 없는 조직의 구조적 한계를 보여주고 있으며 현업의 리스크 및 사고는 개별 부서만의 이슈가 아닌 경영 리스크이며 전사적 차원에서 관리가 되어야 함을 보여준다.

대부분의 사고는 사전 신호가 있었음에도 부서별·형식적 관리로 리스크가 조기에 관리되지 못했으며 규제와 법적 소송의 기준은 사고 발생 여부뿐만 아니라 전사적 리스크 관리체계가 실제로 작동했는지로 이동하고 있다.

특히 최근의 사례들은 법규미준수로 인한 과징금, 평판 훼손에 따른 매출 감소, 사후 보상, 소송 및 정부기관 대응 등을 위한 사후 대응 비용 등은 사전 예방 비용 대비 훨씬 크고 지속적으로 회사에 악영향을 미치고 있다는 점에서 전사 리스크 관리체계로의 전환은 이제는 필수적인 과제이다.

그리고 최근 상법 개정 및 법규 강화 등으로 회사와 경영진의 이러한 전사 리스크 관리에 대한 Due care에 대한 입증을 위해서 전사 리스크 관리체계로의 전환은 최적의 솔루션이 되고 있다.

이러한 변화 및 최근 다수의 사건사고의 결과 속에서 전사 리스크 관리체계(전사 내부통제)는

- 재무보고 목적 내부통제의 범위를
- 운영 목적 및 법규준수 목적까지 확장하여

전사 차원에서 리스크를 식별–평가–대응–모니터링하는 구조를 제공하여 예방중심의 전사 리스크 관리를 실효적으로 지원하는 최적의 솔루션이다.

특히 내부회계관리제도를 통해 축적된 리스크 식별·통제 설계·운영·평가 경험은, 전사 리스크 관리체계로의 확장을 위한 현실적인 기반이 되고 있다. 즉, "새로운 제도 도입"이 아니라, 기존 내부통제 경험의 전략적 확장이 전사 리스크 관리체계 전환의 시작이자 핵심이라 할 수 있다.

이제 전사 리스크 관리체계로의 전환은 현업 혹은 리스크 부서만의 활동이 아니라 기업 생존과 지속성을 지탱하는 전사적인 핵심 경영 인프라를 위한 필수적인 과제이다.

전사 리스크 관리체계(전사 내부통제)의 효익과 Insight

최근 급격한 환경변화에서 재무보고목적 뿐만 아니라 운영목적 및 법규준수 목적과 관련된 진화하는 다양한 리스크에 대한 사후약방문"式 대처의 극명한 한계 존재하고 있으며 기업내에 다양한 대응 방안이 운영되고 있지만 일관성 있고 체계적인 관리의 미흡, 실질적인 운영 및 모니터링의 부재 등으로 인해 리스크 관리의 실효성이 떨어지고 있는 시점에서 실질적인 전사 리스크 관리체계의 정립 및 운영은 소송 및 법적제제 등으로 회사, 경영진 및 사외이사의 책임이 가중되고 있는 상황을 고려할 때 기업의 전사적인 리스크 관리에 최적의 효익을 주는 솔루션이다.

1. 전사 리스크 관리체계(전사 내부통제)가 제대로 정착되지 않은 이유

전사 리스크 관리체계 정립(전사 내부통제)이 그 효익이 많음에도 불구하고 아직까지도 많은 회사들에 제대로 정착되지 않은 이유는 다음과 같다.

부족한 관심, 투자 형식적 운영

- 경영진의 관심과 투자가 부족
- 기업 전체 구성원들의 참여와 관심 부족
- 형식적 운영

통합내부통제 효과에 대한 불신

- 통합 내부통제체계 정립 및 운영이 주는 효과에 대한 여전한 불신이 존재

통합되고 일관된 운영 부재

- 준법, 운영, 재무보고 등 다양한 영역의 내부통제를 별도로 구분 운영하여 비효율적 (예: ESG, KSOX, ISO 등)
- 기업 내 리스크 관리 부서가 다양하게 존재

현업 피로도 증대 우려

- 내부통제업무 확대 시 현업의 업무 가중 등으로 현업 피로도 증대 예상을 우려

상기의 사유와 더불어서 실효적인 전사 리스크 관리를 위한 조직, 위원회 혹은 CRO(Chief Risk Officer) 등이 존재하지 않거나 실질적으로 운영되지 않고 있다는 점은 전사 리스크 관리 거버넌스 정립의 중요성을 보여 준다.

2. 실제 업무 사례를 통해 확인된 전사 내부통제의 효익

최근 전사 리스크 관리체계 정립(전사 내부통제) 프로젝트를 수행한 다수의 사례에서 공통적으로 확인된 효과는 다음과 같다.

(1) 예방 중심 리스크 관리로의 전환 및 전사 리스크 대응

첫 번째 효과는 현업부서를 포함한 전사적으로 리스크 관리가 사후 대응에서 사전 예방으로의 전환이 된 점이다.

중요 리스크를 전사 관점에서 식별하고 고위험 영역을 우선 관리함으로써, 사고 발생 가능성을 구조적으로 낮추는 효과가 확인되었으며 현업부서를 포함한 전사적인 리스크 관리의 중요성을 인지하게 되었다.

또한, 기존 현업부서에서의 리스크 대응 수준이 전사수준(경영진)으로 격상됨에 따라서 현업부서에서 비용 및 인력 등의 사유로 의사결정하기 힘든 과제들이 경영진의 관심과 지원 하에서 부서 문제가 아니라 경영진의 의사결정 사항이 되어 적시성 있게 개선이 되는 경우가 많아지게 되었다.

(2) 경영진·이사회 Due Care 입증 기반 마련

전사 내부통제 체계 하에서는 주요 리스크에 대해

- 식별 근거
- 평가 결과
- 대응 및 점검 이력

이 체계적으로 기록·관리된다. 이는 경영진과 이사회가 리스크를 인지하고 합리적인 판단을 했음을 입증할 수 있는 핵심 자료로 활용되며, 실제 소송·조사 대응 측면에서도 중요한 방어 수단으로 작동하고 있으며 결국 소송·조사 등에서 면책 혹은 경감의 주요 근거가 될 수 있다.

(3) 부서 간 사각지대 해소 및 중복 제거

기존에는 법무, 준법, 내부감사, 내부회계가 각자 리스크를 관리하면서 책임 공백이나 중복 통제가 발생하는 경우가 많았다. 전사 리스크 관리체계(전사 내부통제) 도입 이후에는 리스크와 통제를 하나의 기준으로 정렬함으로써, 관리의 사각지대를 감소시키고 전사적 관점의 의사결정을 가능하게 했다.

(4) 프로세스 및 통제의 고도화

리스크 관리가 실질적으로 운영되면서 부서의 업무상 오류나 부정 위험이 현저히 줄어들게 되어 사건사고 등에 대한 사후 대응 업무가 줄어들게 되고 업무에 대한 상호 신뢰성이 증대가 됨에 따라 결과적으로 업무 효율화에 기여하는 경우가 많아지게 되었다. 또한, 업무과정의 프로세스 및 통제 개선사항 파악을 통해 업무 자동화 및 효율화 추진도 기존에 비해서 보다 더 실질적으로 가능하게 되었다.

3. 전사 내부통제의 현업 부서 입장의 효익

전사 리스크 관리체계(전사 내부통제)는 경영진 및 리스크 관리조직뿐만 아니라 현업부서 입장에서도 하단의 실질적인 효익이 존재한다.

(1) "사고 나면 왜 몰랐냐"가 아니라, 사전에 경영 판단 근거 제공

리스크가 났을 때 책임 회피가 아니라, 미리 공유·보고·의사결정된 이력 제공으로 리스크 관리에 대한 충분한 주의의무(Due Care)를 입증하는 솔루션

(2) 현업 리스크가 개인 혹은 부서만의 판단이 아니라 '전사 리스크 및 과제'로 격상

현업부서에서 중요한 판단을 혼자 떠안지 않고, 회사의 공식 우선순위와 판단으로 처리 가능하여 개선과제가 보다 더 신속하고 실질적으로 개선될 가능성 증대

(3) 수습 업무가 줄고, 본업에 집중할 수 있고 업무 효율성 증대 효과

사고 수습·보고·감사 대응에 쓰이던 시간을 예방·계획·개선 활동으로 전환되어 현업 부서의 업무가 보다 더 효율적이고 체계적으로 개선되어 실질적인 리스크 관리뿐만 아니라 업무 효율성이 개선

(4) 현업부서의 리스크 이슈가 신속하게 경영진에게 공유

현업에서 느끼는 불안·이상징후를 포함한 리스크가 적시성 있게 경영진에 전달되는 통로 마련

결국 전사 리스크 관리체계(전사 내부통제)는 규제가 아니라, 현업 기준에서는 의사결정 속도·명확성·보호장치를 동시에 제공하는 도구다. 즉, 전사 리스크 관리체계는 현업을 통제하는 장치가 아니라, 현업을 보호하는 경영 인프라이다.

4. 전사 내부통제 산출물의 현업 포함 전사 활용 관점의 효익

추가적으로 통제기술서, 업무흐름도, 자가점검 체크리스트 등 내부통제 주요 산출물을 활용함으로써 현업부서를 포함해서 전사적으로 아래와 같은 효익을 얻을 수 있다.

구분	활용방안 및 효익
인수인계	신규 담당자에게 업무 인수인계 시 활용
담당자 업무 Guide	담당자가 스스로 업무할 때 업무 Checklist로 활용
현업부서 전반 업무이해	팀원들의 소속 부서 업무에 대한 전반적인 이해 증진 현업 부서내 리스크에 대한 전반적인 이해
프로세스 개선	프로세스상 개선이 필요한 항목에 대한 효율적이고 효과적인 확인

최근에는 현업부서의 프로세스 및 통제 내역 등을 보여주는 문서가 부족한 상황에서 이러한 전사 내부통제 산출물은 현업부서 포함 전사적으로 추가적인 효익을 제공할 수 있다.

5. 전사 리스크 관리체계(전사 내부통제)에 대한 핵심 Insight

실제 사례에서 도출된 전사 리스크 관리체계(전사 내부통제)의 가장 중요한 Insight는 '통제의 수'가 아니라, 리스크가 전사 차원에서 인식되고 실행되는 구조를 만드는 데 있다는 것이다. 통제 문서와 업무가 늘어나고 현업의 피로도를 증대시키는 것이 아니라,

- 리스크가 보이고
- 책임이 명확해지고
- 변화관리, 실행과 모니터링 및 점검이 반복되는 구조로 내재화

가 형성될 때 전사 리스크 관리체계(전사 내부통제)는 기업의 지속성장가능성 및 규제 대응을 위한 실질적인 전사 리스크 관리를 위한 경영 인프라 및 솔루션이 된다. 또한, 최근 소송의 증대 및 감독당국의 조사와 제재 증가, 법규 미준수에 대한 패널티가 증가하는 환경에서 경영진, 회사 및 임직원의 리스크 관리에 대한 충분한 주의의무(Due Care)를 입증하는 최적의 솔루션이다.

뉴 내부통제 거버넌스 하의 내부통제 운영모델

1. 전사 내부통제 운영의 기본 원칙

동적인 뉴 내부통제 거버넌스 하에서의 내부통제는 일회성 구축이나 진단으로는 충분하지 않으며, 지속적으로 순환하는 운영 모델을 전제로 한다. 효과적인 사례에서 공통적으로 확인된 운영 구조는 다음의 5단계이다.

다만, 재무보고 목적의 내부통제인 내부회계관리제도를 운영하는 경우에는 실무적으로 재무 리스크 평가, 변화관리, 통제 운영 및 통제 평가는 내부회계관리제도에서 별도로 수행하는 것이 더 효율적이고 효과적일 수 있다.

2. 실질적인 내부통제 운영을 위한 5단계 모델

① 변화관리 (Change Management)

- 법규·감독규정 개정, 신규 사업/서비스, 조직 개편, 시스템 변경, 사고·제재 등 리스크에 영향을 미치는 모든 변화 요인을 전사 차원에서 상시 관리
- 변화사항을 단순 공유에 그치지 않고, 리스크·통제 설계(RCM, 업무흐름도)에 공식 반영

✓ 내부통제의 출발점이자, 사후 대응 중심 관리에서 벗어나기 위한 핵심 단계

② 리스크 평가 (Risk Assessment)

실질적인 세부 리스크 평가를 통해 사건사고 최소화 및 예방 중심으로 전사 관점에서 무엇을 중점적으로 관리해야 하는지에 대한 전사적 위험 평가

- 변화관리 결과와 기존 리스크를 종합하여 재무·운영·법규준수 리스크를 공통 기준으로 평가
- 발생 가능성과 영향도를 기준으로 고위험 리스크를 선별하고 관리 우선순위 설정

✓ 경영진·이사회가 회사의 자원을 어디에 보다 더 집중해야 하는지 명확히 제시

③ 통제활동 (Control Activities)

리스크를 실제로 낮추는 '행동 가능한 통제' 설계 및 실행

- 정책, 절차, 승인, 검토, 시스템 통제 등 리스크 특성에 맞는 핵심 통제 중심 설계
- "통제가 있다"가 아니라 누가, 언제, 어떻게 수행하고 증빙은 무엇인지를 명확히 정의

✓ 불필요한 형식적 통제는 제거하고 실효성 중심으로 설계

④ 자가점검 (CSA_Control Self Assessment)

내부통제를 '감사 대응용 문서'가 아닌 '업무 수행 방식'으로 내재화

- 현업 부서가 정기적으로 통제 수행 여부를 직접 점검
- 자가점검 체크리스트를 업무 가이드 + 통제 점검 도구로 활용
- 미비점은 이슈 관리(Action Plan) 방식으로 추적·관리

✓ 통제의 지속성과 실효성을 결정하는 핵심 운영 단계

⑤ 제3자 독립적 평가 및 내부감사와의 연계

고위험 영역 등을 중심으로 제3자의 독립적인 통제활동에 대한 평가를 통해 객관성을 확보하고 전사 내부통제에 대한 실질적인 모니터링과 내재화를 지원

- 고위험 영역 중심의 제3자 운영평가
- 제3자는 회사내 독립 부서 혹은 외부 전문가를 포함하여 통제를 수행하는 현업부서가 아닌 객관적이고 독립적인 조직 혹은 인원을 의미
- 통제 설계 및 운영 평가의 객관성 확보
- 내부감사(3선)의 경영진 전사 내부통제 운영에 대한 점검과 연계하고 리스크 관리

✓ 경영진·이사회·감사(위원회)의 전사 리스크 관리에 대한 Due Care 입증 및 책임 리스크 완화 수단

3. 운영모델의 종합적 의미

상기 5단계가 단절되지 않고 순환 구조로 운영될 때, 내부통제는 규제가 아닌 실제 작동하는 전사 리스크 관리 시스템으로 기능한다. 그리고 내부통제위원회 운영, 성과평가와 연계, 내부통제매뉴얼, AI 및 Digital을 반영한 시스템 등을 통해 보다 더 효율적으로 내부통제를 운영하는 것이 전사 리스크 관리체계를 실효적으로 내재화하는 방안이다. 특히, 현업부서의 분절된 리스크 관리가 아닌 통합적인 전사 리스크 관리를 위해서는 전사 리스크를 관리하는 조직(예: Compliance팀, 내부통제팀, ESG팀 등), 내부통제위원회 혹은 CRO(Chief Risk Officer) 등의 구성 및 실질적인 운영이 기반이 되어야 한다.

맺는말

전사 리스크 관리체계로의 전환 즉, 전사 내부통제의 도입은 더 이상 선택의 문제가 아니다.

상법 개정과 규제 환경 변화, 이해관계자의 요구 수준을 고려할 때, 재무·운영·법규 준수 목적을 포함한 전사 내부통제는 기업의 지속성장가능성을 지탱하는 핵심 경영 인프라라 할 수 있다.

또한, 상법개정 등으로 소송의 증대 가능성, 법규 및 규정 강화 및 감독당국의 조사와 제재가 증가하는 환경에서 경영진, 회사 및 임직원의 리스크 관리에 대한 충분한 주의의무(Due Care)를 입증하는 최적의 솔루션이다.

전사 내부통제의 본질은 통제를 강화하는 것이 아니라, 리스크를 전사적으로 인식하고, 합리적으로 판단하며, 실행과 점검이 반복되는 구조를 만드는 것이다. 이 구조를 어떻게 설계하고 운영하느냐가 향후 기업 리스크 관리의 성패를 좌우하게 될 것이다.

05

AI, 그 혁신에 걸맞은 예측과 대응

- AI, 무엇을 바꾸고 있는가
- 현실화되는 AI 리스크
- 기술 리스크 vs. 경영 리스크
- 왜 많은 조직은 AI를 도입하고도 제대로 관리하지 못하는가
- 문서가 아니라 작동하는 구조가 신뢰를 만든다
- 미국 등 AI 선진국에서의 교훈
- 경영진과 감사위원회는 무엇을 물어야 하는가

AI를 둘러싼 기업의 관심은 이제 기술 그 자체에 머물지 않는다. 진짜 질문은 얼마나 빨리 도입하느냐가 아니라, 그 변화가 무엇을 바꾸고 어떤 비지니스 리스크를 만들어내는지를 얼마나 일찍 읽어내며, 이에 맞는 대응 구조를 얼마나 정교하게 갖추느냐에 있다.

AI는 이미 기업 활동 전반에 깊숙이 스며들고 있다. 문제는 활용 범위가 넓어질수록 위험의 양만 커지는 것이 아니라, 위험의 성격 자체가 달라진다는 데 있다. 이제 기업은 AI를 기술 혁신의 사례를 넘어서 경영의 문제, 곧 예측과 대응의 문제로 재정의해야 한다.

AI, 무엇을 바꾸고 있는가

과거의 자동화가 반복 업무를 줄이는 데 머물렀다면, 지금의 AI는 판단과 추천, 생성의 영역까지 들어오며 업무의 속도와 방식 자체를 바꾸고 있다. 이 변화가 중요한 이유는 효율이 커지기 때문만이 아니다. AI는 기존 통제의 전제까지 함께 흔든다. 전통적인 시스템은 규칙이 비교적 고정되어 있어 입력과 출력의 관계를 추적하기 쉬웠지만, AI는 확률적으로 답하고, 같은 질문에도 맥락에 따라 다른 결과를 낼 수 있으며, 외부 모델과 외부 데이터에 의존하는 경우도 많다. 따라서 기업은 시스템이 돌아가는지만 볼 것이 아니라, 어떤 변화가 나타날 것인가, 이 결과를 어디까지 신뢰할 수 있는가, 누가 책임지는가, 어디에서 사람의 판단이 개입해야 하는가를 함께 보아야 한다.

AI는 업무 구조 뿐만 아니라 인간의 역할을 함께 변화시키고 있다. 과거에는 담당자가 자료를 모으고, 맥락을 해석하고, 판단의 근거를 정리한 뒤 결론에 이르렀다. 그러나 이제는 AI가 먼저 초안과 가설, 추천안을 제시하고 사람은 이를 검토하고 수정하고 승인하는 방식이 빠르게 확산되고 있다. 겉으로는 같은 업무처럼 보이지만, 실제로는 업무의 무게중심이 직접 작성에서 검토와 선택으로 이동하는 것이다.

문제는 이 전환이 단순한 역할 조정에 그치지 않는다는 데 있다. 무엇을 질문해야 하는지, 어떤 결과를 의심해야 하는지, 어디까지를 사람이 책임져야 하는지에 대한 기준도 함께 다시 세워야 한다. 결과가 그럴듯해 보인다는 이유로 검토가 형식화될 수 있고, 설명이 어렵다는 이유로 잘못된 판단이 그대로 의사결정에 반영될 수도 있기 때문이다.

결국 AI 시대의 기업이 예측해야 하는 것은 기술 성능의 변화만이 아니다. 더 중요한 것은 AI가 업무 구조와 책임 구조를 어떻게 재편하는지, 그리고 그 변화 속에서 사람의 비판적 판단과 통제가 실제로 남아 있는지를 읽어내는 일이다. 그래서 AI 시대의 통제는 결과만 확인하는 수준에 머물 수 없다. 누가 어떤 질문을 했는지, 어떤 근거로 결과를 수용하거나 수정했는지, 사람의 판단이 어디에서 개입했는지를 함께 관리해야 한다.

현실화되는 AI 리스크

AI 리스크는 더 이상 먼 미래의 가능성이 아니다. 이미 여러 기업과 시장에서 편향된 결과, 부정확한 응답, 데이터 유출, 저작권 및 프라이버시 이슈, 외부 공급망 의존에 따른 장애와 같은 문제가 반복적으로 나타나고 있다. 중요한 점은 이런 사례가 특별한 실패가 아니라, AI 활용이 넓어질수록 더 자주 현실화될 수 있는 구조적 위험이라는 데 있다.

특히 최근에는 AI 활용의 확산 속도에 비해 관리 체계의 성숙 속도가 충분히 따라오지 못하는 모습이 분명하게 나타난다. 많은 기업이 이미 생성형 AI를 도입하고 실제 업무에 활용하고 있지만, 어떤 영역이 더 위험한지 구분하고, 누가 검토하고 책임지며, 어떤 상황에서 즉시 중단할 수 있는지를 명확히 정리한 곳은 아직 많지 않다. 활용은 빠르게 넓어지는데, 관리 및 통제는 그 속도를 따라가지 못하는 것이다.

이때 드러나는 리스크는 단순히 모델의 성능 문제에 그치지 않는다. 잘못된 답변은 잘못된 판단으로 이어질 수 있고, 민감한 정보의 입력이나 외부 모델 의존은 데이터와 프라이버시 문제를 키울 수 있다. 또 결과가 그럴듯해 보인다는 이유로 검토가 형식화되면, 오류는 더 늦게 발견되고 더 큰 의사결정으로 번질 수 있다. 결국 AI 리스크는 기술이 실패하는 순간만이 아니라, 사람이 이를 너무 쉽게 믿거나 조직이 충분한 통제 없이 확산시키는 순간 현실화된다.

따라서 기업이 주목해야 할 것은 "AI가 위험하다"는 추상적 선언이 아니다. 더 중요한 것은 어떤 리스크가 이미 현실에서 반복되고 있는지, 우리 조직은 그중 무엇에 가장 취약한지, 그리고 그 위험이 실제 업무와 의사결정 과정에서 어떤 형태로 나타날 수 있는지를 구체적으로 읽어내는 일이다. 그래야만 AI 리스크를 기술의 문제가 아니라 경영의 문제로 다룰 수 있다.

최근 Anthropic의 Claude Mythos 사례는 이런 위험이 얼마나 빠르게 현실화될 수 있는지를 상징적으로 보여준다. 공개된 자료에 따르면 Claude Mythos는 대규모 취약점 탐지 능력과 함께 통제·격리 실패 가능성까지 함께 논의되었고, 이는 고도화된 AI의 리스크가 더 이상 정확도 문제에만 머물지 않음을 보여준다. 중요한 것은 성능 자체보다, 이런 능력이 충분한 통제와 책임 구조 없이 확산될 경우 기업과 시장이 감당해야 할 위험의 크기이다.

기술 리스크 vs. 경영 리스크

AI가 촉발하는 불확실성과 위험을 IT 등 기술 부서의 문제로만 보면, 경영진은 가장 중요한 판단 시점을 놓치게 된다. 겉으로는 기술 이슈처럼 보여도, 실제 기업이 감당하는 결과는 대부분 경영 리스크이다.

예를 들어, 편향되거나 부적절한 결과는 곧바로 평판과 브랜드에 영향을 준다. 데이터 유출이나 프라이버시 침해는 법적 책임과 재무 손실로 이어진다. 거버넌스와 통제가 미비하면 사고가 났을 때 누가 책임져야 하는지도 불분명해진다. 또 모델 성능 저하나 외부 공급망의 문제는 운영 연속성과 핵심 의사결정의 신뢰를 흔들 수 있다.

즉, AI 리스크는 기술에서 시작될 수 있지만, 기업이 실제로 마주하는 것은 평판, 법적 책임, 재무 손실, 운영 차질과 같은 복합적인 리스크이다. 그래서 경영진에게 필요한 것은 기술을 세세히 이해하는 능력보다, 기술 리스크를 경영 리스크의 언어로 읽고 판단하는 능력이다.

왜 많은 조직은 AI를 도입하고도 제대로 관리하지 못하는가

문제는 많은 조직이 AI 리스크를 인식하지 못해서만은 아니다. 오히려 더 본질적인 한계는, 인식한 위험을 실제 운영과 의사결정의 구조 안에서 관리 가능한 형태로 전환하지 못한다는 데 있다. 즉, 리스크에 대한 우려는 존재하지만 그것이 책임, 권한, 통제 절차로 연결되지 못하는 것이다. 그 배경에는 대체로 세 가지 구조적 공백이 존재한다.

첫째, Ownership Gap이다. 승인자는 있지만 실질적으로 책임지는 사람은 없는 상태이다. 회의체와 위원회는 존재하지만 사고가 발생했을 때 누가 최종 책임을 지는지 모호하다면, 조직은 쉽게 책임 회피와 의사결정 지연에 빠질 뿐만 아니라 사후 대응 역시 방어적으로 흐르기 쉽다.

둘째, Alignment Gap이다. 개발, 현업, 준법, 보안 등 다양한 조직이 AI를 서로 다른 기준으로 이해하고 운영하는 상태이다. 기술 조직은 성능과 속도를, 현업은 활용성과 효율을, 준법과 보안은 규제와 통제를 우선시하기 때문에, 이를 하나의 리스크 언어로 정렬하지 못하면 중요한 위험은 조직 간 경계에서 누락되기 쉽다.

셋째, Authority Gap이다. 문제가 생겼을 때 누가 즉시 사용을 중단하고, 범위를 제한하며, 대응을 지시할 수 있는지가 불분명한 상태이다. AI 리스크는 확산 속도가 빠른 만큼, 중단 권한과 보고 체계가 사전에 명확하지 않으면 사고는 더 넓게 번지고 조직의 대응은 항상 한발 늦어질 수밖에 없다.

결국 많은 조직이 부족한 것은 위험에 대한 인식 자체보다, 그 위험을 실제로 작동하는 거버넌스 구조로 바꾸는 역량이다. 그래서 AI 관리의 핵심은 새로운 원칙을 추가로 선언하는 데 있지 않다. 누가 책임지고, 누가 정렬하며, 누가 멈출 수 있는지를 사전에 분명히 하는 운영 구조를 갖추는 데 있다.

문서가 아니라 작동하는 구조가 신뢰를 만든다

많은 기업이 이미 AI 정책과 가이드라인을 마련하고 있다. 그러나 문서가 존재한다고 해서 운영이 곧바로 안전해지는 것은 아니다. 원칙은 종이에 적혀 있을 수 있지만, 실제 사고는 언제나 운영의 빈틈에서 발생한다.

중요한 것은 누가 승인하는가, 누가 책임지는가, 누가 멈출 수 있는가, 누가 사후에 점검하고 설명하는가가 하나의 구조로 연결되어 있는지이다. AI 거버넌스는 선언이 아니라 작동 구조여야 한다. 문서보다 중요한 것은 권한과 책임, 중단과 보고, 점검과 검증이 실제로 연결된 운영 체계이다. 결국 신뢰는 원칙에서만 만들어지지 않는다. 신뢰는 작동하는 구조에서 만들어진다.

AI 거버넌스는 선언이 아니라 유효성 있는 운영체계여야 한다. 결국 신뢰는 원칙에서만 만들어지지 않는다. 신뢰는 작동하는 구조에서 만들어진다.

미국 등 AI 선진국에서의 교훈

미국, 유럽 등 AI 도입이 한국에 비해 앞서 있는 선도 시장은 이미 중요한 교훈을 보여주고 있다. 많은 기업들이 초기에는 (AI 리스크에 대한 충분한 인지 없이) AI를 생산성 향상 도구로 빠르게 수용했지만, 시간이 지나며 기술 자체의 도입이 아니라 AI 기술이 조직 전반에 가져올 변화의 폭(불확실성 및 리스크)을 미리 예측하고 준비하는 것이 AI 환경에서의 필수적인 요소임을 인지하기 시작했다. AI가 업무 수행 방식과 의사결정 구조를 바꾸고, 책임의 경계를 재정의하며, 외부 서비스와 제3자 기술 의존도를 높이는 순간, 이에 상응하는 통제와 거버넌스가 뒤따르지 않으면 리스크는 더 이상 기술 차원에 머물지 않고 경영과 운영의 문제로 확산된다.

한국 기업이 주목해야 할 지점은, 미국과 유럽이 이미 2~3년 앞서 이러한 흐름을 경험했다는 사실이다. 이는 한국 기업에게 불리한 출발점이라기보다 오히려 학습의 기회를 의미한다. 선도 시장에서 나타난 시행착오와 대응 사례를 참고할 수 있다는 점에서, 한국 기업은 동일한 문제를 처음부터 반복하기보다 더 짧은 시간 안에 보다 정교한 준비 체계를 갖출 수 있다. 따라서 규제와 통제를 단순한 부담으로 보기보다, AI 도입 과정에서 불확실성을 줄이고 조직의 수용력을 높이는 기반으로 인식할 필요가 있다.

경영진과 감사위원회는 무엇을 물어야 하는가

AI 거버넌스는 결국 경영진과 이사회 수준의 질문에서 시작된다. 지금 우리 회사는 어디에 AI를 쓰고 있는가. 그중 어떤 활용이 중요한 의사결정, 고객 영향, 재무보고, 법규 준수와 연결되는가. 책임자는 누구인가. 외부 모델과 데이터를 얼마나 의존하고 있는가. 사고가 발생하면 탐지하고 중단하고 보고할 수 있는가. 이 질문이 정리되지 않은 상태에서 AI 전략을 말하면 실행보다 불안이 앞서게 된다. 결국 이사회와 감사위원회가 던져야 할 질문은 복잡하지 않다. 우리 회사는 어떤 AI를 어디에 쓰고 있는가, 사고가 나면 누가 책임지는가, 외부 모델과 공급망은 어떻게 검증하는가, 문제가 생기면 누가 즉시 멈출 수 있는가. 이 질문에 선뜻 답하지 못한다면, 그 지점이 현재 조직의 가장 큰 리스크이다.

결국 AI 시대에 기업이 경계해야 할 오해는 두 가지이다. 하나는 AI를 기술 부서만의 과제로 보는 것이고, 다른 하나는 혁신의 속도만 따라가면 충분하다고 믿는 것이다. 실제로 기업에 더 중요한 것은 AI가 바꾸는 업무 방식과 책임 구조, 리스크의 성격을 얼마나 일찍 읽어내고 준비하느냐이다. 그리고 그 중심에는 컴플라이언스, 재무, 내부감사, 리스크 조직이 있다. 이들이 익숙한 내부통제의 언어로 변화를 해석하고, 기술 리스크를 경영 리스크로 번역하며, 문서가 아닌 작동하는 구조를 다시 설계할 때 비로소 기업은 AI를 더 넓고 더 오래 사용할 수 있다. 결국 AI, 그 혁신에 걸맞은 것은 더 많은 도입 그 자체가 아니라, 그 변화를 예측하고 흔들리지 않도록 대응하는 역량이다.

Contact

임성재 Partner
sung-jae.lim@pwc.com
02-709-6480

윤여현 Partner
yeo-hyun.yoon@pwc.com
02-3781-9988

김두삼 Partner
doo-sam.kim@pwc.com
02-709-8828

이정미 Partner
jeong-mi.lee@pwc.com
02-3781-9647

홍우식 Partner
woo-shik.hong@pwc.com
02-3781-3248

정수정 Partner
soo.jung.jeong@pwc.com
02-709-7038

임재욱 Partner
jae-wook.lim@pwc.com
02-709-8121

김진국 Partner
jin-kook.kim@pwc.com
02-709-3345

S/N: 2606A-RP-083

samil.com