ESG as Q

교보증권 리서치의
ESG 시리즈

발간일자: 2026. 06. 02

이사회 밖의 거버넌스(G)

[신재생에너지/ESG]
조혜빈 선임연구원
02-3771-9130
hevin.cho@iprovest.com

▪ 2025~2026년 자본시장에서 기업가치를 훼손한 거버넌스 리스크는 이사회 구성이나 주주환원 같은 구조 지표가 아니라, 구조 지표가 포착하지 못하는 내부통제의 실효성에서 나온 사례가 두드러짐. 데이터 유출과 마케팅 검수 실패가 과징금, 보상비, 매출 감소, 주가 하락으로 이어짐. 우발적 사고가 아니라 관리 시스템이 작동하지 않은 거버넌스 실패임

▪ 내부통제는 성격이 다른 두 층위로 나뉨. 하나는 개인정보 보안 같은 데이터 통제로, ESG 평가가 별도 항목으로 측정하는 영역. 다른 하나는 마케팅 검수나 내부 결재 같은 운영 컴플라이언스로, ESG 평가가 정면으로 측정하지 못하는 영역. 두 층위 모두 재무 손실로 이어지나, 평가가 신호를 주는 정도가 달라 투자 대응도 달라짐

▪ 내부통제 실패의 재무적 대가가 커지고 있음. 데이터 영역은 기업의 개인정보 보유량 증가로 유출 시 노출 규모가 확대되고, 징벌적 과징금 도입 등 제도 강화로 위반 비용도 상승. 운영 영역은 평판 훼손이 소비자 이탈과 매출 감소로 이어진 사례가 확인됨. 양 영역 모두 과거에는 경미했을 통제 실패가 대규모 손실로 이어지는 구조

▪ 데이터 통제 영역에서 ESG 평가는 노출도와 관리역량을 결합해 점수를 산출하므로, 데이터 통제 리스크에 노출된 기업을 사전에 식별하는 도구로 기능함. 다만 데이터 통제 실패의 손실은 사고 시점에 끝나지 않고 과징금, 보상비, 소송이 시차를 두고 누적됨. 투자자가 기대할 수 있는 우위는 위험조정성과의 방어에 가까우며, 리스크가 이벤트 발생 직후 다 반영됐다고 보지 않고 이후 누적될 비용을 반영하는 접근 필요

▪ 운영 컴플라이언스 영역에서는 ESG 평가가 신호 자체를 주지 못함. MSCI의 Business Ethics는 부패와 뇌물 감독, Accounting은 회계 투명성에 초점이 맞춰져 있어, 마케팅 검수나 결재 라인의 형식적 작동은 측정되지 않음. 그럼에도 재무 손실은 발생하므로, 이 영역의 대응은 등급에 의존하지 않고 통제 실효성을 독자적으로 점검하는 데서 나옴

▪ 규제와 평가 모두 감독 책임 쪽으로 초점이 옮겨가는 중. 국내에서는 CPO가 전사 개인정보 처리를 총괄하고 이사회에 정기 보고하도록 거버넌스 정비를 명령하는 시정조치가 나왔고, 이사 충실의무도 주주로 확대됨. 내부통제 실효성은 ESG 등급과 별도로 투자 판단에 반영해야 할 변수임

기업가치를 훼손한 것은 구조가 아니라 내부통제

거버넌스 논의는 통상 이사회 독립성, 지배구조, 주주환원에 집중된다. 그러나 2025~2026년 자본시장에서 기업가치를 직접 훼손한 사례 가운데 상당수는 이러한 구조 지표가 아니라, 구조 지표가 포착하지 못하는 내부통제의 실효성에서 나왔다. 내부통제란 회사가 사고를 막기 위해 갖춰둔 점검과 승인 절차, 즉 데이터 보안 체계나 마케팅 검수 라인 같은 관리 장치를 말한다. 데이터 유출, 퇴사자 접근권한 미회수, 마케팅 검수 실패는 모두 이 장치가 무너진 사례다. 사고처럼 보이지만, 본질은 통제 절차가 장부상 존재하되 실제로 작동하지 않은 거버넌스 실패다.

이 내부통제는 성격이 다른 두 층위로 나뉜다. 하나는 개인정보 보안 같은 데이터 통제로, ESG 평가가 별도 Key Issue로 측정하는 영역이다. 다른 하나는 마케팅 검수나 내부 결재 같은 운영 컴플라이언스로, ESG 평가가 정면으로 측정하지 못하는 영역이다. 두 층위 모두 사건이 터지면 과징금, 보상비, 매출 감소, 주가 하락으로 실적에 반영되지만, 평가가 신호를 주는 정도가 다르기 때문에 투자 대응도 달라진다.

데이터 통제 실패는 ESG 평가가 측정하는 영역에서 일어났다. 대표 사례는 쿠팡으로, 성명과 이메일 기준 3,367만여 건이 유출됐다. 과학기술정보통신부 민관합동조사단은 이용자 인증 시스템 개발자가 퇴사한 뒤에도 회사가 서명키를 갱신하지 않아, 공격자가 정상 로그인 없이 계정에 접속했다고 결론지었다. 외부의 정교한 해킹이 아니라 퇴사자 권한 관리라는 기본적 내부통제의 공백이 출발점이었다. 사고 인지 후 신고가 24시간을 넘겨 과태료 대상이 됐고, 자료 보전 명령 이후 접속기록이 삭제돼 조사가 제한되는 등, 통제 실패가 위기대응과 신고 통제의 문제로 연쇄됐다.

재무 영향은 이미 가시화됐다. 미국 상장 모회사 Coupang, Inc.는 이를 중대 사이버보안 이슈로 SEC에 공시하면서(2025년 12월 16일 8-K, 12월 29일 8-K/A), 규제당국의 제재, 소송, 추가 비용 등으로 인한 잠재적으로 중대한 재무 영향 가능성을 위험 요인으로 적시했다. 회사는 통지 대상 고객에게 약 1.685조원(약 12억 달러) 규모의 보상 바우처를 지급하기로 했으며, 이 바우처는 향후 거래의 판매가와 인식 매출을 차감하는 형태로 반영된다. 사고 영향으로 4Q25 연결 조정 EBITDA는 전년 동기 대비 약 36.6% 감소했다(전년 동기 약 4.2억 달러에서 약 2.67억 달러로). 한국 자회사 대표는 2025년 12월 사임했고, 미국에서는 공시 지연 등을 주장하는 투자자 집단소송이 제기됐다. 개인정보보호위원회의 제재 수위는 2026년 6월 중 결정될 전망이다.

[도표 1] 2025~2026 년 주요 내부통제 실패 사례

구분	기업명	이슈	재무 및 규제 영향
데이터	SK 텔레콤	가입자 약 2,300 만 명 USIM 정보 유출, 방화벽 설정 미흡, 서버 계정정보 관리 부실	- 과징금 1,347 억 9,100 만원('25.8.28, 역대 최대) - 과태료 960 만원, CPO 역할 보장 등 시정명령
	쿠팡	성명 및 이메일 3,367 만여 건 유출, 퇴사 개발자 서명키 미갱신, 전자 출입증 검증 미흡, 최초 4,500 계정 신고에서 3 천만 이상으로 확대, 신고 지연 및 자료보전명령 위반	- 보상 바우처 약 1.685 조원(약 12 억 달러, 매출 차감 반영) - 4Q25 연결 조정 EBITDA -36.6% YoY - 한국대표 사임, 미국 증권 집단소송, 제재 '26.6 월 결정 예정
운영 컴플라이언스	스타벅스 코리아	마케팅 논란, 리스크 관리 체계 결함, 승인 라인의 형식적 작동 비판 제기	- 이마트 주가 3 거래일간 약 13.7% 하락 - 스타벅스코리아 매출 감소, 선수금 약 4,276 억원(계약부채 약 4,543 억원) 환불 프로그램 시행 - 자회사 대표 및 기획 감독 임원 해임

주: 쿠팡 보상은 회사 발표 및 SEC 공시, 유출 규모는 과기정통부 조사 결과 기준
자료: 각 사, 언론종합, 교보증권 리서치센터

주가 흐름도 이 구조를 보여준다. Coupang, Inc. 주가는 사고 인지 직전부터 SEC 공시일까지 약 18% 하락했다. 주목할 점은 손실이 사건 시점에 한 번에 반영되고 끝나지 않았다는 것이다. 쿠팡의 경우 보상 바우처 결정, 4Q25 실적 훼손, 집단소송, 개인정보위 제재가 시차를 두고 순차적으로 현실화됐다. 이벤트 발생 시점에 손실이 주가에 모두 반영됐다고 보기 어려운 이유다.

관리 시스템 실패가 실적으로 이어진 사례는 과거에도 존재했다. SK텔레콤에서 가입자 약 2,300만 명의 USIM 정보가 유출돼, 개인정보보호위원회로부터 과징금 1,347억9,100만원이 부과됐다. 방화벽 설정 미흡, 암호화 미실시 등 기본적 안전조치 의무를 소홀히 한 결과였다. 여기서도 사건 인지에서 과징금 확정까지 수개월이 걸려, 데이터 통제 실패는 규제, 보상, 소송이 여러 갈래로 진행되며 재무 손실의 꼬리가 길다. 주목할 점은 시정명령의 방향이다. 규제 당국은 CPO 역할이 IT 영역에 한정돼 정작 유출이 발생한 인프라는 감독이 이뤄지지 않았다고 지적하고, CPO가 전사 개인정보 처리를 총괄하며 이사회에 정기 보고하도록 명령했다. 규제가 개별 보안 조치를 넘어 감독 체계 자체를 겨냥한 것이다.

운영 컴플라이언스 실패는 ESG 평가가 측정하지 않는 영역에서 일어났으나, 실적에는 분명하게 반영됐다. 내부통제 실패는 데이터 영역에만 국한되지 않는다. 스타벅스코리아의 마케팅이 사회적 논란을 일으킨 뒤, 그룹은 리스크 관리 체계의 결함을 인정하고 관련 임원을 해임했다. 사건의 사회적 쟁점과 별개로, 마케팅 검수와 승인이라는 절차적 통제가 실효성 있게 작동하지 못했다는 점이 핵심이다.

동사는 매출의 상당한 감소를 인정했고, 최대주주(지분 67.5%)인 이마트 주가는 사건 직후 3거래일간 약 14% 하락했다. 재무 임팩트는 매출 감소에 그치지 않는다. 동사는 소비자 이탈에 대응해 선불충전금을 사용 비율과 관계없이 환불하는 한시 프로그램을 도입했는데, 작년 말 기준 선수금 잔액은 약 4,276억원, 미사용 적립까지 합한 계약부채는 약 4,543억원에 달했다. 선수금은 고객이 충전금을 써야 매출로 인식되는 계약부채여서, 환불이 늘면 매출 인식 기반이 줄고 현금이 유출돼 매출과 유동성 양쪽에 부담이 된다. 통제 실패라는 근본 원인이 평판 훼손과 환불을 거쳐 계약부채의 현금화로 이어진 것이다.

[도표 2] 쿠팡(CPNG) 주가 추이

자료: Bloomberg, 교보증권 리서치센터

[도표 3] 이마트 주가 추이

자료: Quaniwise, 교보증권 리서치센터

위 사례는 같은 통제 실패이지만, ESG 평가가 이를 다루는 방식은 정반대다. 데이터 통제는 측정되고, 운영 컴플라이언스는 측정되지 않는다. 투자자의 대응 경로도 이에 따라 두 갈래로 갈린다.

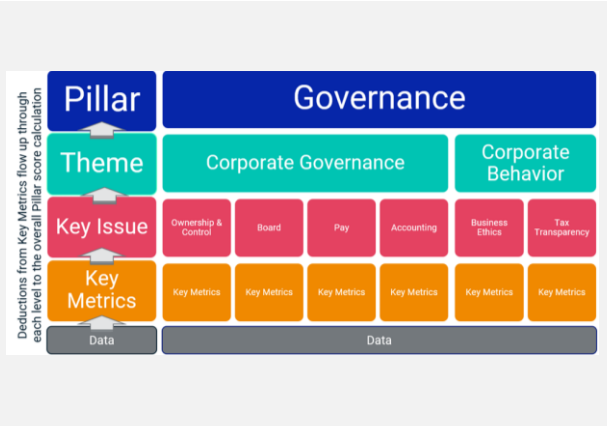
데이터 통제 영역은 ESG 평가가 측정하는 영역이다. MSCI는 데이터 유출 리스크를 Social Pillar의 Privacy & Data Security Key Issue로 측정하며, 노출도(수집 정보량, 규제 노출)와 관리역량을 결합해 점수를 산출한다. 이 설계상 데이터를 많이 보유하고 관리가 부실한 기업은 이 항목에서 구조적으로 낮게 평가된다. 따라서 이 점수는 개별 등급의 절대 수준과 무관하게, 데이터 통제 리스크에 노출된 기업을 사전에 식별하는 도구로 기능한다.

문제는 손실이 반영되는 방식이다. 데이터 통제 실패는 사건이 터진 시점에 손실이 한 번에 확정되지 않는다. 과징금, 보상비, 소송 비용이 규제와 사법 절차를 거치며 시차를 두고 현실화되고, MSCI 방법론상 데이터 유출이 구조적 문제로 판단되면 사건 이후 등급 하향까지 뒤따른다. 시장이 사건 당일 반영하는 것은 이 손실의 일부일 뿐이므로, 식별된 노출 기업에 대해 이후 누적될 비용을 앞질러 판단하는 사후 대응이 추가 손실을 줄인다. 손실 꼬리가 길다는 점이 그 근거다. 다만 이는 초과수익이 아니라 위험조정성과의 방어에 가깝다.

운영 컴플라이언스 영역에서는 ESG 평가가 신호 자체를 주지 못한다. 마케팅 검수나 내부 결재 시스템의 실효성은 ESG 평가의 측정 대상이 아니다. Governance Pillar의 Business Ethics는 뇌물과 반부패, Accounting은 회계 투명성에 초점을 둘 뿐, 승인 라인이 형식적으로만 작동하는 절차적 통제 실패를 포착하는 항목은 없다. 사건 전에는 등급에 드러나지 않지만, 스타벅스코리아 사례처럼 재무 손실은 분명히 발생한다. 이 영역에서 투자자의 대응은 등급에 의존하지 않고 통제 실효성을 직접 점검하는 데서 나온다.

결국 ESG 등급이 양호한 기업에서도 거버넌스 이벤트 리스크는 발생할 수 있다. 다만 한 영역(데이터 통제)에서는 그 리스크가 측정 가능한 신호로 존재하고, 다른 영역(운영 컴플라이언스)에서는 신호 자체가 부재하다는 점에서 투자 접근이 둘로 나뉜다.

[도표 4] MSCI 거버넌스(G) Pillar 모델 구조



자료: MSCI ESG Ratings Methodology, 교보증권 리서치센터

[도표 5] 내부통제 두 층위의 ESG 평가와 투자 접근

구분	ESG 평가 항목	신호 여부	투자 대응
데이터	MSCI Privacy & Data Security (S, 노출도+관리역량)	노출 기업 식별 가능, 단 사건 후 손실이 시차를 두고 누적	식별된 기업에 대해 사건 후 후속 비용을 앞질러 반영
운영 컴플라이언스	MSCI Business Ethics, Accounting (G, 부패 및 회계 중심)	사전 신호 부재 (사후 controversy로 일부 반영)	등급 너머 통제 실효성 독자적 점검

자료: MSCI ESG Ratings Methodology, 교보증권 리서치센터

[도표 6] MSCI ESG Ratings 33 개 Key Issue 계층 구조

3 Pillars	10 Themes	33 ESG Key Issues
Environment	Climate Change	Carbon Emissions
		Climate Change Vulnerability
		Financing Environmental Impact
		Product Carbon Footprint
	Natural Capital	Biodiversity & Land Use
		Raw Material Sourcing
		Water Stress
	Pollution & Waste	Electronic Waste
		Packaging Material & Waste
		Toxic Emissions & Waste
	Environmental Opportunities	Opportunities in Clean Tech
		Opportunities in Green Building
		Opportunities in Renewable Energy
Social	Human Capital	Health & Safety
		Human Capital Development
		Labor Management
		Supply Chain Labor Standards
	Product Liability	Chemical Safety
		Consumer Financial Protection
		Privacy & Data Security
		Product Safety & Quality
		Responsible Investment
	Stakeholder Opposition	Community Relations
		Controversial Sourcing
	Social Opportunities	Access to Finance
		Access to Health Care
		Opportunities in Nutrition & Health
Governance	Corporate Governance	Board
		Pay
		Ownership & Control
		Accounting
	Corporate Behavior	Business Ethics
		Tax Transparency

주: 데이터 유출 리스크는 Social Pillar의 Product Liability 테마 아래 Privacy & Data Security로 측정되는 반면, 결재 같은 운영 통제는 33개 Key Issue 별도 항목으로 존재하지 않음
자료: MSCI ESG Ratings Methodology, 교보증권 리서치센터

감독 책임 강화와 투자 함의

내부통제 실패에 대한 대응은 한국만의 현상이 아니다. 유럽에서도 GDPR 집행의 초점이 개별 보안 조치에서 조직적 책임, 거버넌스, 위탁업체 감독으로 옮겨가며, 감독 체계의 실효성을 규제가 점점 더 중시하고 있다.

국내 규제도 같은 방향이다. SK텔레콤 제재에서 규제 당국은 CPO가 전사 개인정보 처리를 총괄하고 이사회에 정기 보고하도록 거버넌스 정비를 명령했다. 데이터 유출 사고의 책임을 실무 부서가 아니라 이사회와 경영진의 감독 의제로 끌어올린 것이다. 규제와 평가의 관심이 점차 운영적 실효성으로 옮겨가고 있으며, 현재 신호가 부재한 운영 컴플라이언스 영역도 향후 측정 범위로 들어올 가능성이 있다.

내부통제는 더 이상 실무 부서의 컴플라이언스 항목이 아니라 이사회와 경영진이 직접 책임지는 거버넌스 의제로 격상되고 있다. 국내 이사 충실의무의 주주 확대, CPO 거버넌스 정비 명령, 유럽의 조직적 책임 및 감독 강조는 모두 개별 결과가 아니라 감독 체계를 겨냥한다.

따라서 투자 함의는 두 가지다. 첫째, 데이터 통제 영역에서는 평가 점수로 노출 기업을 식별하되, 대응의 초점은 사건 발생 자체보다 그 이후에 둬야 한다. 데이터 통제 실패의 손실은 사건 당일에 끝나지 않고 규제 제재, 보상, 소송이 시차를 두고 누적되므로, 사건 당일의 주가 반응만으로 리스크가 모두 반영됐다고 보면 추가 손실에 노출된다. 사건 이후 이어질 비용을 앞질러 판단하는 투자자가 사후 재가격의 충격을 줄여 위험조정성과를 지킨다. 다만 이 성과는 초과수익이 아니라 하방 리스크 회피로 나타난다. 데이터 집약도와 개인정보 보유 규모가 큰 업종일수록 손실 누적의 규모가 커, 동일 등급 안에서도 통제 수준의 차이를 별도로 점검해야 한다.

둘째, 운영 컴플라이언스처럼 평가가 사전 신호를 주지 못하는 영역에서는 등급을 넘어선 독자적 판단이 필요하다. 등급 자체를 불신할 이유는 없으나, 등급이 사전에 포착하지 못하는 운영적 실효성은 투자자가 직접 점검해야 할 몫이다. 마케팅 검수나 결재 시스템의 작동 여부, 위기대응 거버넌스, 공시 투명성은 사건 전 등급에 드러나지 않으므로, 정성적 점검 항목으로 보완한다. 규제와 평가가 모두 감독 책임으로 이동하는 만큼, 이사회와 경영진 차원의 리스크 관리 체계 유무가 향후 제재 강도와 등급 변동을 가른다. 이 영역의 관리 역량이 기업 간 차별화 요인이 되며, 내부통제 실효성은 ESG 등급과 별도로 투자 판단에 반영해야 한다.

■ Compliance Notice ■

이 자료에 게재된 내용들은 작성자의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 작성되었음을 확인합니다.

이 조사자료는 당사 리서치센터가 신뢰할 수 있는 자료 및 정보로부터 얻어진 것이나, 당사가 그 정확성이나 완전성을 보증하는 것이 아닙니다. 따라서 이 조사자료는 투자참고자료로만 활용하시기 바라며, 어떠한 경우에도 고객의 증권투자 결과에 대한 법적 책임소재의 증빙자료로 사용될 수 없습니다. 또한 이 조사자료의 지적재산권은 당사에 있으므로 당사의 허락 없이 무단 복제 및 배포할 수 없습니다.

당사 리서치센터 연구원은 고객에게 카카오톡 메신저 등으로 개별 접촉하지 않습니다. 당사 연구원 사칭 사기 등에 주의하시기 바랍니다.

- 동 자료는 제공시점 현재 기관투자가 또는 제3자에게 사전 제공한 사실이 없습니다.
- 전일기준 당사에서 1% 이상 보유하고 있지 않습니다.
- 추천종목은 전일기준 조사분석 담당자 및 그 배우자 등 관련자가 보유하고 있지 않습니다.

■ 투자의견 비율공시 및 투자등급관련사항 ■ 기준일자_2026.03.31

구분	Buy(매수)	Trading Buy(매수)	Hold(보유)	Sell(매도)
비율	95.9%	2.7%	1.4%	0.0%

[업종 투자의견]

Overweight(비중확대): 업종 펀더멘털의 개선과 함께 업종주가의 상승 기대
Underweight(비중축소): 업종 펀더멘털의 악화와 함께 업종주가의 하락 기대
Neutral(중립): 업종 펀더멘털상의 유의미한 변화가 예상되지 않음

[기업 투자기간 및 투자등급] 향후 6개월 기준, 2015.6.1(Strong Buy 등급 삭제)

Buy(매수): KOSPI 대비 기대수익률 10%이상
Hold(보유): KOSPI 대비 기대수익률 -10~10%
Trading Buy: KOSPI 대비 10%이상 초과수익 예상되나 불확실성 높은 경우
Sell(매도): KOSPI 대비 기대수익률 -10% 이하