석 사 학 위 논 문

ESG 경영을 위한 중소·중견 기업 보안·DR 거버넌스 방법론 연구

2026년

한성대학교지식서비스&컨설팅대학원

스마트융합컨설팅학과

ESG융합컨설팅전공

이 재 철

석 사 학 위 논 문
지도교수 원종혁

ESG 경영을 위한 중소·중견 기업 보안·DR 거버넌스 방법론 연구

A Governance Framework and Methodology for SME Security and Disaster Recovery Aligned with ESG Management

2025년 12월 일

한성대학교지식서비스&컨설팅대학원

스마트융합컨설팅학과

ESG융합컨설팅전공

이 재 철

석 사 학 위 논 문
지도교수 원종혁

ESG 경영을 위한 중소·중견 기업 보안·DR 거버넌스 방법론 연구

A Governance Framework and Methodology for SME Security and Disaster Recovery Aligned with ESG Management

위 논문을 컨설팅학 석사학위 논문으로 제출함

2025년 12월 일

한성대학교지식서비스&컨설팅대학원

스마트융합컨설팅학과

ESG융합컨설팅전공

이 재 철

이재철의 컨설팅학 석사학위 논문을 인준함

2025년 12월 일

심사위원장 주형근 (인)

심 사 위 원 정진택 (인)

심 사 위 원 원종혁 (인)

국 문 초 록

ESG 경영을 위한 중소·중견 기업 보안·DR 거버넌스 방법론 연구

한성대학교지식서비스&컨설팅대학원
스 마 트 융 합 컨 설 팅 학 과
E S G 융 합 컨 설 팅 전 공
이 재 철

ESG(Environmental, Social, Governance) 경영이 제도·시장 양 측면에서 빠르게 '정착 단계'로 변화하면서 정보보안과 재해복구(Disaster Recovery, DR)는 더 이상 IT 운영의 부수 영역이 아니라 지배구조(G) 영역의 통제·책임·증빙체계로 재정의되고 있다. 특히 EU의 CSRD는 지속가능성 보고의 범위와 엄격성을 확대하면서 향후 보증(assurance) 관행의 정교화를 예고하고 있으며 ISSB의 IFRS S1 또한 지속가능성 관련 리스크·기회에 대해 기업이 운용하는 거버넌스 프로세스 통제 절차를 명시적으로 공시하도록 요구하고 있다. 이러한 흐름 속에서 '보안'은 기술적 방어를 넘어 경영진의 책임 하에 리스크를 식별·관리하고 운영중단을 최소화하며 데이터 신뢰성을 유지하는 거버넌스 실천 과제로 자리 잡게 되었다(EU, 2022).

그러나 중소·중견 기업은 디지털 전환의 속도에 비해 보안과 DR을 경영 시스템으로 내재화하는 데 구조적 한계를 겪고 있다. ENISA(2021)는 중소·중견 기업이 공급망 기반 공격과 같은 외부 충격에 취약하며 인식 부족, 예산부족, 전문인력부족, 경영진 지원 부족 등이 대응·복구 역량의 약점으로 누적된다고 지적한다. 더 나아가 최근 덴마크 제조 중소·중견 기업을 대상으로 한 연구 보고에서도 '최근 몇 년 내 사이버 공격을 경험한 기업이 5개 중 1개' 수준이라는 결과가 제시되어 제조 기반 중소·중견 기업의 보안 취약성이 특정 국가의 예외가 아니라 국제적으로 반복되는 문제임을 시사한다. 국내 역시 스마트공장 보급 확산과 함께 데이터·설비·외주접속이 촘촘히 연결되고 있으나

현장에서는 자동화·데이터화 투자가 보안·DR의 부재 또는 형식적 운영과 병존하는 장면이 적지 않다. 이는 단순한 기술 격차라기보다 거버넌스 결손(책임·정책·통제·훈련·투자 우선순위)의 누적으로 해석될 여지가 크다(ENISA, 2021).

본 연구자는 스마트공장 및 ICT 인프라 구축·컨설팅 업무를 장기간 수행하며 중소·중견 기업이 보안을 '비용' 또는 '사고 이후의 보완책'으로 인식하는 경향이 전략·예산·조직 체계 전반에 어떤 형태로 반영되는지 지속적으로 관찰해 왔다. 또한 ESG 관련 감수·진단 업무 과정에서 경험한 바로는 보안·연속성 지표가 기업의 내부 통제와 연결되어 표준화되기보다 평가기관·고객사 요구에 따라 파편적으로 대응되는 한계가 뚜렷하게 관찰되었다. 반면 일정 규모 이상의 기업은 ISMS 기반의 관리체계, 사고 대응 프로세스, 백업·복구 체계, 공급망 요구사항 관리 등을 다층적으로 운영하며 결국 보안·DR 거버넌스 성숙도 격차가 협력사 평가와 거래 지속성에까지 영향을 미치는 구조가 강화되는 추세이다. 이러한 변화는 NIST CSF 2.0이 'GOVERN' 기능을 신설·강조하며 사이버 리스크를 전사 리스크관리와 연계하려는 흐름과도 맞물리며 중소·중견 기업 역시 거버넌스 관점에서 보안 및 DR체계를 재정립할 필요가 있음을 뒷받치한다(NIST, 2024).

이에 본 연구는 중소·중견 제조기업의 ESG 성숙도 향상을 위해 보안·DR을 거버넌스 관점에서 통합적으로 재구성하고 제한된 자원을 가진 기업이 현장에서 적용 가능한 방법론을 제안하는 것을 목적으로 한다. 첫째, ENISA의 SME 보안 권고, NIST CSF 2.0 및 ISO/IEC 27001의 관리체계 관점, NIST SP 800-34의 컨틴전시(Contingency) 계획 원리, 그리고 국내 K-ESG 가이드라인의 진단 항목을 종합하여 중소·중견 기업 보안·DR 취약요인을 '조직·정책·기술·운영·증빙' 구조로 모델링한다. 둘째, 계층분석법(AHP)을 적용해 보안·DR 구성요소의 상대적 중요도를 정량화함으로써 투자 우선순위와 단계적 이행 로드맵수립의 근거를 도출한다. 셋째, 분석 결과를 기반으로 ESG 공시·평가 맥락에서 활용 가능한 보안·DR 거버넌스 지표 모델을 제시한다. 넷째, 공급망 요구사항까지 확장 가능한 사이버 복원력(Cyber Resilience) 기반 실행 프레임워크를 설계하여 현장 적용성과 확장성을 높인다. 특히, 공급망 리

스크 관점에서는 CSF 2.0의 공급망 관련 범주(GV.SC)와 연계 가능한 접근을 검토함으로써 협력사 보안 요구사항이 '요청사항'에 그치지 않고 거버넌스 운영 프로세스로 정착될 수 있도록 프레임워크를 보완한다(ENISA, 2021).

본 연구의 의의는 중소·중견 기업이 대기업 수준의 보안·DR 대응체계를 단기간에 모방하는 방식에서 벗어나 거버넌스 성숙도에 기반한 단계적 구축을 통해 실효성을 확보할 수 있는 접근방법론을 제시한다는 것에 있다. 또한 보안·DR 거버넌스의 고도화는 생산·납기·품질에 직결되는 운영중단 위험을 낮추고 복구목표시간(RTO)·복구목표시점(RPO) 개선과 더불어 데이터 무결성 및 공시 신뢰성 제고 등 실질적 성과로 연결될 가능성이 높다. 나아가 협력사 보안 성숙도가 글로벌 밸류체인(GVC)에서 거래 지속성의 조건으로 강화되는 환경에서 본 연구가 제안하는 방법론은 공급망 전반의 ESG 리스크 완화와 국내 중소·중견 제조기업의 지속가능경영 역량 강화를 위한 실천적 기반을 제공할 것으로 기대된다(EU, 2022).

주요단어 : ESG 경영, 정보보안, 재해복구(DR), 운영연속성(BCP), 사이버 복원력(Cyber Resilience), AHP, 스마트공장, 보안 거버넌스

목 차

표 목 차

그 림 목 차

Ⅰ. 서론

1.1 연구배경

최근 ESG(Environmental, Social, Governance) 경영은 스마트공장 구축사업 및 공급망 관점에서 중요한 이슈로 확대되고 있으며 규제와 시장의 요구가 맞물리며 글로벌 표준으로 빠르게 자리 잡게 되었다(최유경 외, 2024). 이 과정에서 기업의 정보보안과 재해복구(Disaster Recovery, DR) 역량은 지배구조(G) 영역의 핵심 요건으로 다시 부각되고 있다(NIST, 2020). 특히 EU CSRD와 ISSB 공시 기준은 지속가능성 정보를 단순 서술이 아니라 리스크 관리와 내부통제의 결과로 다루는 방향을 강화하고 있다(European Union, 2022; IFRS Foundation/ISSB, 2023). 이러한 변화는 본 연구자가 수행한 스마트공장 구축 컨설팅 현장에서도 고객사 점검 항목의 변화로서 지속적으로 확인되고 있으며 보안 리스크는 더 이상 선택적 대응 사항으로 취급되지 않고 있다. 본 연구자는 NIST CSF 2.0에서 'Govern' 기능이 전면에 배치된 것은 보안과 DR을 단순한 기술 문제가 아니라 경영 통제 영역의 핵심 요소로 재정의하려는 국제 기준의 변화로 해석된다(NIST, 2024).

본 연구에서는 보안과 DR을 단순한 기술 운영 항목이 아니라 기업 내부의 책임 구조와 의사결정 체계 속에서 관리되어야 할 거버넌스 과제로 해석한다. 즉, 책임과 의사결정 구조 속에서 예산과 인력을 배분하고 성과를 측정하는 거버넌스 과제로 이동하고 있다는 점에 주목하고 있다(NIST, 2020).

그러나 국내 중소·중견 제조기업은 ESG 경영 및 보안과 DR에 대한 구조적 변화에 대한 변화 속도를 따라가기 어려운 제약을 안고 있다. 본 연구자가 스마트공장 구축에 대한 수준별 구축과 ICT 및 AI기술을 활용한 고도화 컨설팅을 수행하면서 현장에서 반복적으로 확인한 사실은 생산에 대한 설비투자와 제조 공정의 효율화에는 투자와 관심이 집중되는 반면 보안과 DR은 구축을 하지만 운영과 관리를 위한 기본적인 체계를 정착하지 못하는 경우가 많다는 것을 알게 되었다. 네트워크 분리, 권한관리, 로그기록, 백업, 복구 절

차 같은 항목은 문서로는 존재하지만 제조기업에서 실제로는 담당자 개인 경험에 의존하거나 유지보수 기업에 의존하고 사고 이후에 보강되는 방식으로 운영되기도 한다. 본 연구자가 관찰한 이러한 현장 경험의 문제점은 중소·중견 기업의 DR 문서화 부재와 침해대응 미흡과 예산·인력 제약을 지적한 NIST(2021), PMC(2024)의 문제의식과도 맞닿아 있다. Chen et al.(2023)의 선행연구 또한 보안 체계에 대한 역량의 부족이 제품 생산성 저하와 협력사 간 공급망의 신뢰성 약화로 직접 연결될 수 있음을 지적하고 있다.

한편, 국내 연구에서도 스마트공장 환경의 위협을 구조화하고 보안 요구사항을 도출하는 시도가 이어져 왔다는 것을 찾아볼 수 있다(박은주 외, 2017). 이러한 연구는 OT/IT 융합 환경에서 보안 이슈가 단순 시스템 구축 문제가 아니라 제품 생산과 품질저하 그리고 밴더사에 대한 납기와 연결된 운영에 대한 리스크임을 보여준다는 것을 알 수 있다(김일용 외, 2018).

또한 연구자가 “ESG 탄소중립 보고서 감수(2023)” 과정에서 다수 기업의 관리 현황을 검토했을 때 보안 지표의 표준화 필요성이 지속적으로 제기되었다. 중소·중견 제조기업의 보안 취약성은 단순한 내부 관리 이슈를 넘어 공급망 전반의 ESG 성과와 거래의 안정성에 영향을 미치는 핵심 요인으로 작용한다. 협력사의 보안 성숙도는 원청(벤더사) 기업의 ESG 평가에 직·간접적 영향을 미치며 글로벌 밸류체인(GVC) 환경에서는 이미 협력사 보안 수준 확인이 필수 요건으로 자리 잡고 있으며 미흡한 경우 협력사에서 제외되는 사례도 보고된다(ENISA, 2021). 국내에서도 중소·중견 기업 대상 사이버 위협과 거버넌스 대응을 다룬 연구는 이러한 현실을 제도와 정책 관점에서 해석하며 시사점을 제시한 바 있다(정제용·김용호·Victoria Wang, 2020). 다만 실무에서는 이 흐름이 더 빠르게 체감된다. 고객사 요구는 점검 항목을 늘리고 증빙자료를 요구하는 방향으로 강화되지만 정작 중소·중견 기업은 무엇부터 갖춰야 하는지 우선 순위를 세우기 어려운 실정이다(ENISA, 2021).

이처럼 ESG 경영이 강화되는 흐름 속에서 중소·중견 제조기업의 보안·DR 체계는 더 이상 선택이 아닌 필수 기반 역량으로 요구되고 있다. 본 연구는 이러한 문제의식을 바탕으로 실무 현장에서 관찰된 중소·중견 기업의 보안·DR 운영의 공백을 학술적 방법론으로 구조화하고자 한다. 나아가 ESG 지

배구조(G) 관점에서 이를 통합적으로 재해석함으로써 중소·중견 기업이 현실적으로 적용할 수 있는 보안·DR 거버넌스 방법론의 방향을 제시하고자 한다(European Union, 2022; IFRS Foundation/ISSB, 2023; NIST, 2024).

1.2 연구목적

본 연구는 연구자가 다년간 스마트공장 구축 및 ESG 컨설팅을 수행하는 과정에서 반복적으로 마주한 한계를 출발점으로 삼는다. 현장에서는 ESG 요구가 빠르게 고도화되고 있음에도 불구하고 중소·중견 제조기업이 정보보안과 재해복구를 체계적으로 통합·운영하지 못하는 사례가 지속적으로 확인되었다. 이러한 문제의식을 바탕으로 본 연구는 기술 항목의 추가가 아닌 책임 구조와 통제 운영에 대한 복구 역량을 하나의 거버넌스 흐름으로 재구성하는 방향에서 보안·DR 체계의 개선 가능성을 탐색하고자 한다. 본 연구가 강조하는 개선은 기술 목록을 늘리는 연구가 아니며 책임 체계와 통제 운영 그리고 복구 역량을 하나의 거버넌스 흐름으로 엮는 접근이라 할 수 있다. 이를 위해 다음과 같은 세부 목표를 설정해 볼 수 있다.

첫째, 기존 문헌(NIST, PMC, KPMG, Chen et al.)과 스마트공장 구축 및 ESG 컨설팅 현장에서 확인된 실무 사례를 바탕으로 중소·중견 기업의 보안·DR 취약요인과 ESG 요구사항 간 구조적 연계성을 분석한다. 이때 취약요인을 기술 미비로만 분류하지 않고 조직, 정책, 운영절차, 증빙 체계의 관점에서 재정리한다(정제용 외, 2020; ENISA, 2021).

둘째, AHP(Analytic Hierarchy Process) 기법을 적용하여 중소·중견 기업이 우선적으로 구축해야 할 보안·DR 구성요소의 상대적 중요도를 정량적으로 도출한다. 이를 통해 현장 실무자가 활용 가능한 객관적 의사결정 지표를 제공하고 투자 우선순위를 설명할 수 있는 근거를 제시한다. 국내에서도 스마트팩토리 보안관리 지표를 도출하고 가중치를 산정한 사례 연구가 보고된 바 있어 본 연구의 방법론 설계에 참고할 수 있다(김지태, 2023).

셋째, 도출된 우선순위와 글로벌 ESG 공시 기준(EU CSRD, ISSB, K-ESG)을 연계하여 중소·중견 기업이 활용 가능한 ESG 기반 보안·DR 지표

모델을 제안한다(European Union, 2022; IFRS Foundation/ISSB, 2023).

본 연구에서 제안하는 보안·DR 지표는 단순한 점검표나 형식적 공시 항목을 대체하기 위한 것이 아니다. 연구자는 EU CSRD와 ISSB 공시 기준이 지속가능성 정보를 리스크 관리와 내부통제의 결과로 다루고 있다는 점에 주목하였으며 이를 중소·중견 제조기업의 현실에 적용하기 위해서는 통제 운영의 실체가 남는 지표 설계가 필요하다고 보았다. 또한 DR은 계획 문서의 보유 여부가 아니라 반복적인 훈련과 점검 복구 성과의 검증을 통해 완성된다는 점에서 본 연구는 Cyber Resilience 프레임워크를 참고하여 현장 적용 가능성을 우선한 개선 방향을 정리하고자 하였다. DR은 계획서의 존재 여부로 완성되지 않는다. 훈련과 점검 그리고 복구 성과가 반복적으로 검증되어야 한다(NIST SP 800-34; ISO/IEC 27001:2022; NIST, 2024).

본 연구자가 현장에서 경험하였던 보안과 ESG 경영의 상관 관계에 대하여 위의 세가지 관점을 바탕으로 기업이 ESG 경영의 신뢰성을 확보하고 공급망에서의 경쟁력을 강화할 수 있도록 지원하고자 한다.

1.3 연구 기대효과

본 연구는 ESG-보안-DR의 통합적 관점에서 중소·중견 제조기업을 분석한 선행 연구가 충분하지 않은 상황에서 다음과 같은 이론적·실무적 기여를 제공한다.

첫째, 본 연구에서는 기존 K-ESG 평가체계가 원칙적으로 요구하고 있으나 구체적으로 설명하지 못한 보안·DR 운영 요소에 주목하고 이를 지배구조(G) 관점에서 해석 가능한 정량 지표로 구조화하고자 하였다. 이러한 접근은 보안과 DR을 공시 항목의 단순 확장이 아니라 거버넌스 운영의 결과로 이해할 수 있는 분석 관점을 제공한다(K-ESG 가이드라인, 2021; European Union, 2022; IFRS Foundation/ISSB, 2023). 특히 보안과 DR을 공시 항목의 추가가 아니라 거버넌스 운영의 결과로 설명하는 논리 체계를 제공한다는 점에서 의의가 있다.

둘째, 스마트공장 구축과 ESG 진단 실무를 수행하는 과정에서 연구자는

중소·중견 제조기업이 보안·DR의 필요성은 인식하고 있으나 이를 어떤 순서와 범위로 구축해야 하는지에 대한 기준을 갖지 못하고 있음을 반복적으로 확인하였다. 이에 본 연구에서는 OT/IT 환경의 현실을 고려하여 모든 통제를 일괄적으로 도입하기보다 핵심 통제부터 단계적으로 성숙도를 높이는 방향이 현실적이라는 판단 하에 개선 흐름을 정리하였다. OT/IT 환경에서는 완전한 통제를 한 번에 달성하기보다 핵심 통제부터 성숙도를 높이는 접근이 현실적이며 선행 연구에서도 이러한 단계화 필요성이 암묵적으로 전제된다(박은주 외, 2017; 김일용 외, 2018).

셋째, 협력사의 보안 취약성이 공급망 전체의 ESG 리스크로 전이되는 구조를 고려할 때 본 연구의 결과물은 공급망 전반의 리스크 완화와 ESG 대응력 제고에 기여할 수 있다(ENISA, 2021). 지적한 바와 같이 중소·중견 기업의 취약성은 공급망 공격의 관문이 될 수 있으며 이는 원청의 리스크로 전환된다. 국내 연구 역시 중소·중견 기업 사이버보안 거버넌스의 공백이 제도적 지원과 연계되어야 한다는 시사점을 제공한다(정제용 외, 2020).

마지막으로, 보안·DR 체계의 성숙은 생산 중단 상황에서의 대응 속도와 복구 안정성에 영향을 미칠 수 있으며 이는 RTO/RPO 관리 수준의 개선으로 이어질 여지가 있다. 이러한 변화는 운영 연속성과 공시 신뢰성에 대한 내부 인식을 강화하는 방향으로 작용할 수 있고 장기적으로는 ESG 지표 관리의 일관성을 높이는 기반으로 해석될 수 있다.

이러한 점에서 본 연구는 중소·중견 제조기업이 ESG–보안–DR을 하나의 통합된 거버넌스 체계로 설계할 수 있는 실질적 근거를 제공한다. 또한 연구자와 실무자에게 적용 가능한 의사결정 기준과 실행 프레임워크를 제시함으로써 학술성과 현장성을 동시에 확보하고자 한다.

Ⅱ. 이론적 배경

2.1 ESG 경영과 지배구조(G) 요소

선행연구에 따르면 ESG 경영이 기업의 지속가능성을 판단하는 기준으로 활용되는 과정에서 지배구조(G)는 단순한 조직 구조 평가를 넘어 투명한 의사결정과 리스크 관리가 실제로 작동하고 있는지를 가늠하는 기준으로 해석되고 있다(Clark et al., 2015; Eccles & Klimenko, 2019). 지배구조(G) 요소는 전통적으로 이사회 구조, 내부통제, 컴플라이언스 등을 중심으로 다뤄져 왔으나 최근 디지털 전환이 빠르게 진행되면서 기존의 이사회 구조나 컴플라이언스 중심 논의만으로는 기업의 관리 역량을 설명하기 어렵다는 지적이 제기되고 있다. 이에 따라 데이터가 어떻게 보호·관리되고 있는지 사이버 리스크에 대한 대응 체계와 운영연속성(BCP/DR)이 어떻게 설계되어 있는지가 지배구조(G) 평가에서 함께 고려되는 흐름이 나타나고 있다(ISSB, 2023; CSRD, 2024).

[그림 2-1]과 같이 ESG는 환경(Environment), 사회(Social), 지배구조(Governance)의 영문 첫 글자를 조합한 단어로서 기업 경영에서 지속가능성(Sustainability)을 달성하기 위한 3가지 핵심 요소입니다.

[그림 2-1] ESG 정보 공개 가이던스 (한국거래소, 2021)

한편, 스마트공장 고도화 프로젝트 현장에서는 동일한 생산 시스템이라도 데이터가 어떻게 생성되고 누가 승인하며 어떤 통제 흔적이 남는지에 따라 운영 안정성과 대외 신뢰도가 크게 달라진다. 이 차이는 곧 공시의 품질과도 연결된다. 국내 연구에서도 내부·외부 지배구조 요인이 ESG 공시품질에 유의미한 영향을 준다는 결과가 보고되었고 이는 G가 “형식적 구조”를 넘어 “정보의 신뢰성”을 좌우한다는 점을 시사한다(최미화, 2023).

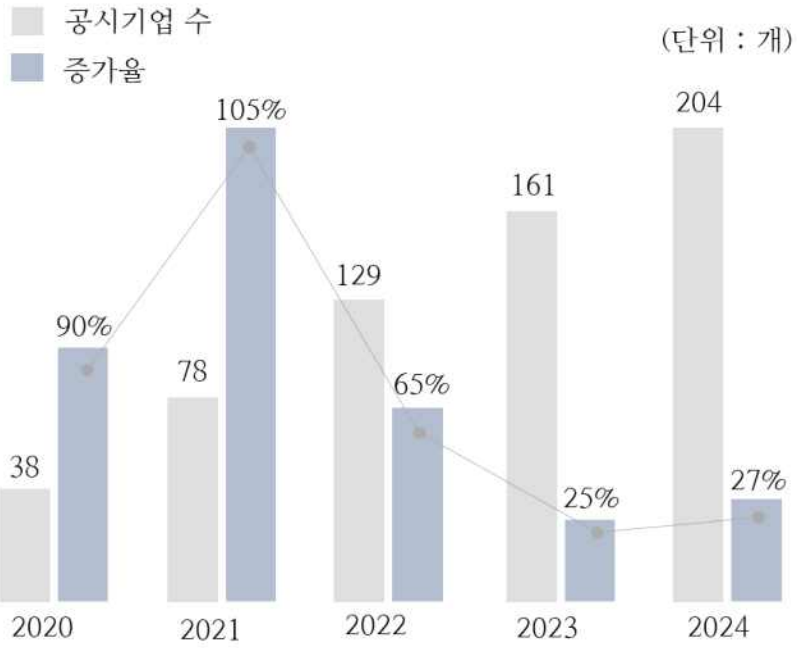
스마트공장과 데이터 기반 운영 환경이 확대되면서 사이버보안 이슈는 IT 부서 단위의 기술 관리로만 다루기에는 한계가 있다는 인식이 확산되고 있다. 국내 실증 연구에서도 이사회 차원의 전문성과 관여 수준이 사이버보안 관련 공시 여부에 영향을 미친다는 결과가 보고되었으며 이는 사이버보안이 전사적 리스크 관리 체계와 연결되어 논의되고 있음을 시사한다(송유정 외, 2024). 이러한 논의는 “산업자산 보호” 관점의 산업보안 거버넌스가 지속가능경영의 구성 요소로 다뤄져야 한다는 주장과도 접점을 가진다(최선영 외, 2022).

2.1.1 글로벌 ESG 경영 규제 동향

최근 ESG 경영이 기업의 지속가능성을 평가하는 기준으로 활용되면서 주요 국제 규제기관과 표준 제정 기구는 정보 관리와 리스크 대응 역량을 지배구조(G)의 운영 수준을 판단하는 중요한 요소로 해석하는 흐름을 보이고 있다(Tsang, 2023; Suttipun, 2025).

[그림2-2]는 연도별 지속가능경영보고서 공시 현황을 살펴보면 국내 기업의 자율 공시 참여가 점진적으로 확대되고 있음을 확인할 수 있다. 이러한 변화는 지속가능경영보고서 공시 의무화 논의와 맞물리면서 특히, 수출 비중이 높은 제조기업을 중심으로 대응 필요성이 인식된 결과로 해석된다(한국거래소, 2025). 국내 기업들의 지속가능경영보고서 공시 의무화가 추진되고 있는 가운데 ESG(환경·사회·지배구조) 경영 관련 글로벌 환경이 최근 변화를 맞이하고 있어 주목된다. 수출 산업 위주의 국내 기업들에게 적지 않은 영향이 있을 것으로 전망된다(김종아 외, 2023). 2025년 3월 한국거래소에 따르면 코

스피 상장법인 중 지난해 ESG 지속가능경영보고서를 자율 공시한 기업수는 204개로 전년 161개사 대비 27% 증가했다. 자산 2조원 이상 시가총액 10조원 이상 대규모법인들의 공시비율이 높았으며 제조업이 105개사로 가장 많이 공시했다. 뒤를 이어 금융·보험업이 44개였다고 거래소는 설명했다. 해마다 자율 공시 참여 법인이 늘어나는 추세로 지속가능경영보고서를 의무적으로 공시해야 하는 국내 제도 도입이 임박했기 때문으로 분석된다.



[그림 2-2] 연도별 지속가능경영보고서 공시기업 수 (한국거래소, 2025)

이러한 흐름은 특히 유럽연합의 CSRD 국제지속가능성기준위원회(ISSB)의 IFRS S1·S2, 국내 K-ESG 가이드라인을 중심으로 제도화되고 있다. 유럽연합의 CSRD(Corporate Sustainability Reporting Directive)는 기업이 재무 비재무 통합 공시를 수행하도록 의무화하면서 정보보안·사이버리스크·데이터 무결성을 지배구조(G) 공시항목에 명시하였다(EY, 2024; KPMG, 2024). 특히 CSRD는 기업의 “데이터 신뢰성 보장 메커니즘”을 요구하며 사이버 공격이나 시스템 장애에 대한 대응·복구 절차가 투명하게 관리되어야 한다고 강조한다.

최근 기업 실무 가이드에서는 CSRD 준수를 위해 ESG 데이터 소유권, 데

이터 품질관리, IT·보안 통제, 시스템 장애, 사이버 공격에 대비한 내부통제 설계가 필수라는 점을 반복적으로 강조하고 있으며 이를 통해 정보보안·DR이 “재무정보와 동일 수준의 신뢰성을 요구받는 공시 영역”으로 격상되고 있음을 알 수 있다(PwC, 2024; Deloitte, 2024).

[표2-1]과 같이 CSRD는 정보보안, 사이버 리스크, 재해복구 체계를 지배구조(G) 공시 항목에 명시적으로 포함하고 있으며 데이터 신뢰성 확보를 위한 내부통제와 대응·복구 절차의 관리 여부를 중점적으로 요구하고 있다(EY, 2024; KPMG, 2024). 이러한 특징으로 인해 CSRD는 다른 공시 기준과 비교할 때 기업의 보안·DR 운영 실태를 보다 직접적으로 점검할 수 있는 구조를 갖는 것으로 해석된다. 반면 ISSB는 재무적 영향 중심의 공시체계로서 정보보안·DR을 ‘기업가치 관련 리스크’ 범주 내에서 반영하고 있으며 산업별 기준(SASB)을 통해 보안 관련 공시 요구가 확장될 수 있다. 한편 K-ESG는 중소·중견 기업의 접근성을 고려한 자가진단 모델이지만 정보보안·데이터 거버넌스·DR 체계에 대한 정량적·구체적 지표가 부족하여 글로벌 규제 수준과의 간극이 존재한다(조찬희 외, 2023).

IFRS S1·S2 기준을 통해 기후위험뿐 아니라 정보보안·IT 운영 리스크를 기업 지속가능성에 영향을 미치는 핵심 요소로 분류한다. ISSB는 기업이 사이버 사고가 재무적 의사결정에 미치는 영향과 복구 능력을 명시적으로 공시하도록 요구함으로써 정보보안과 DR이 재무·비재무 모두에 영향을 미치는 요소임을 제도적으로 확인하였다(정준희 외, 2023).

국내에서는 K-ESG 가이드라인이 다양한 산업군의 ESG 평가 기준으로 활용되고 있으나 지배구조 부문에서 정보보안 및 DR 체계를 포괄하는 항목은 제한적이다. 예를 들어, K-ESG의 G-3(내부통제) 항목은 리스크 관리 체계를 검토 하도록 되어 있지만 사이버 리스크 대응, 백업 관리 체계, 재해복구 전략 등은 구체적으로 포함되지 않는다. 이로 인해 중소·중견 기업은 ESG 평가 과정에서 기술적 보안 요소보다 문서화된 통제 체계 중심의 평가에 편중되는 문제가 발생한다. 이처럼 글로벌 기준은 정보보안 및 DR 체계를 ESG 공시의 필수 요소로 확장하고 있으나 한국의 기존 평가체계는 이에 비해 구체성·정량성 측면에서 부족하여 보완이 필요한 상황이다(조찬희 외, 2023).

[표 2-1]은 글로벌 ESG 경영 규제 동향 비교로 사이트 코딧(CODIT) ESG경제 사이트 등을 활용하여 요약 정리한 내용으로 적용국적, 재정목적, 적용범위, 보안관련, 중요데이터 요구 수준등에 대하여 정리하였으며 중요내용은 지배구조에 대한 보안관점에서 내용을 정리하였다.

[표 2-1] 글로벌 ESG 경영규제 동향비교(CODIT, 2024; CODIT, 2025; 연구자 재구성, 2025)

구분	CSRD	ISSB	K-ESG
적용 국적	EU	IFRS S1·S2	대한민국
제정 목적	지속가능성 공시의 투명성·비교가능성 확보, 재무·비재무 통합보고	기업가치에 영향을 미치는 지속가능성 리스크·기회 공시의 국제 표준화	기업 ESG 수준 자가진단 및 국내 산업 특성 반영한 평가체계 제시
적용 범위	EU 역내·외 일정 규모 이상 기업(상장·비상장 포함)	전 세계 기업에 적용 가능한 글로벌 단일 기준	국내 중소·중견·대기업 모두 활용 가능 (법적 의무 아님)
지배구조(G) 요구수준	내부통제, 데이터 거버넌스, 정보 신뢰성 확보 체계 명시	지속가능성 정보에대한 지배구조(이사회·경영진 역할) 요구	전통적 지배구조 중심(이사회, 윤리경영, 내부통제)
사이버 보안 관련성	ESRS G1에서 사이버리스크·데이터 무결성·정보보안을 명확히 공시 항목으로 포함	산업별 SASB 기준에 따라 Data Security, Data Privacy 공시가능	CISO, 정보보호 체계 등 일부 항목만 존재(정량·세부 지표 부족)
DR/BCP 반영 여부	시스템 장애 대응·복구 절차, 데이터 신뢰성 보증 체계 요구	기업가치에 영향을 미치는 IT 운영 리스크 공시 가능(사고·복구 영향 포함)	DR/BCP 체계는 명시적 항목 부재 (간접적 평가 수준)
데이터 관리 요구 수준	ESG 데이터 품질관리, 내부통제(ICFR 수준)의 요구 강함	지속가능성 데이터 공시와 재무적 영향의 연결성 강조	데이터 거버넌스 관련 명시 수준은 상대적으로 낮음
공급망 평가 요구	공급망(supply chain) 사이버·ESG 리스크 공시 강화	산업별 리스크 기반 공급망 분석 요구	협력사 ESG 평가 항목 존재하나 보안·DR 요소는 미흡

2.1.2 ESG와 정보보안·DR의 연계성

최근 ESG 논의에서는 정보보안과 재해복구 체계가 기업의 지배구조(G)를 구성하는 운영 요소와 어떻게 연결되는지가 주요 쟁점으로 다뤄지고 있다. 이는 데이터 신뢰성 확보뿐 아니라 디지털 환경에서 기업 활동이 중단 없이 유지될 수 있는지를 판단하는 기준과도 연관된다. 지배구조(G)는 전통적으로 이

사회 구성, 내부통제, 윤리경영 등을 포함하는 영역이었지만 디지털 의존도가 높아진 최근 환경에서는 디지털 리스크 관리와 데이터 보호 체계를 포함하는 방향으로 확장되고 있다(오영균, 2022).

기업 환경에서 정보보안은 외부 침해 대응을 넘어 데이터 무결성과 접근 통제, 감사 가능성을 어떻게 유지하고 있는지와 밀접하게 연결된다. 한편 재해복구 체계는 사고 발생 이후 조직이 어느 수준까지 어떤 속도로 운영을 회복할 수 있는지를 판단하기 위한 관리 기준으로 활용되며 RTO와 RPO와 같은 지표는 이러한 회복 목표를 점검하는 수단으로 사용된다. 이러한 관리 체계는 ISSB가 요구하는 거버넌스 공시의 취지와도 맞물린다(ISSB, 2023).
ISSB와 CSRD 기준은 이러한 요소들이 기업의 지배구조 체계와 불가분의 관계에 있으며 공시의 신뢰성 확보를 위해 반드시 갖추어야 하는 요소로 강조한다. 또한 국내 연구에서도 ESG 맥락에서 정보보안이 기업 성과와 연결되거나 ESG 지배구조 요인이 정보보안 정책 준수 의도에 영향을 줄 수 있다는 논의가 제시된다(우재민 외, 2022; 이려화 외, 2023).

즉, ESG와 정보보안·DR 시스템은 분리된 개념이 아니라 상호 보완적 구조를 형성하며 기업의 지속가능성과 위험관리 수준을 판단하는 데 핵심적인 역할을 담당한다. 이러한 논의를 종합하면 ESG와 정보보안·DR 체계를 개별 관리 항목으로 분리해 이해하기보다는 공시의 신뢰성과 운영연속성을 함께 뒷받침하는 관리 구조로 해석할 여지가 크다. 이에 본 연구는 보안·DR을 ESG 맥락에서 통합적으로 검토함으로써 중소·중견 기업의 경영 안정성과 리스크 관리 수준을 설명할 수 있는 틀을 설정하고자 한다. 즉, 공시 신뢰성과 운영연속성의 기반을 구성하는 통합 거버넌스 구조로 설정하는 것이 합리적이다. 이러한 배경에서 ESG 기반의 보안·DR 체계 구축은 중소·중견 기업의 경영 안정성을 강화하는 전략적 요소로 대두되고 있다(오영균, 2022).

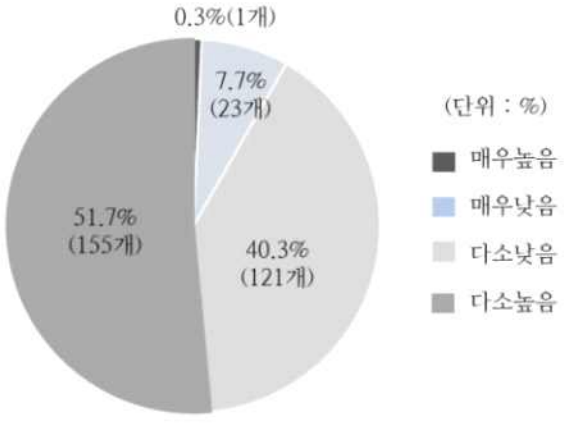
2.1.3 공급망 ESG 리스크와 중소·중견 기업의 역할

최근 글로벌 공급망 환경에서는 협력기업의 보안 성숙도가 ESG 평가 과정에서 어떻게 반영되고 있는지가 주요 논점으로 다뤄지고 있다. 이는 개별

기업의 내부 통제 수준을 넘어 공급망 전반의 리스크 관리 역량을 함께 점검하려는 흐름과 연결된다. UNGC(United Nations Global Compact)는 공급망에서 발생하는 사이버 사고가 원청 기업의 ESG 등급에 직접적인 악영향을 준다고 분석한 바 있다. 예를 들어, SolarWinds 해킹 사건은 공급망 내 특정 협력사의 보안 취약점이 연쇄적인 보안 사고로 확산될 수 있음을 드러낸 사례로 자주 인용된다. 이 사건 이후 다수의 글로벌 기업이 협력사 보안 점검과 인증 절차를 강화한 점은 공급망 차원의 보안 관리가 실질적인 경영 이슈로 인식되기 시작했음을 시사한다(손영우 외, 2024).

중소·중견 기업이 공급망 내 ESG 리스크의 주요 기원이 된다는 분석은 ENISA(2021)에서도 반복적으로 확인된다. ENISA는 중소·중견 기업의 보안과 DR 역량 부족이 공급망 전체의 취약점을 구성하여 원청 기업의 운영 중단 또는 데이터 유출로 이어질 수 있음을 경고하였다(손영우 외, 2024).

[그림2-3]은 중소벤처기업진흥공단의 국내 300개 수출기업 대상으로 '중소·중견 기업 ESG 자가진단 시스템 분석결과'에 따르면 '수출기업의 공급망 ESG 실사 대응현황과 과제' 조사에 따르면 응답기업의 51.7% 가 향후 공급망 내 ESG 경영 수준 미흡으로 고객사(원청기업)로부터 계약·수주가 파기될 가능성이 높다고 느끼는 것으로 나타났으며 다소낮음(40.3%), 매우낮음(7.6%), 매우높음(0.3%)으로 ESG 경영 미흡이 향후 계약 수주 파기될 가능성으로 나타났다.



[그림 2-3] ESG 미흡에 따른 계약 파기 예측(대한상공회의소, 2022)

국내 제조업 환경에서 다수의 중소·중견 기업이 공급망을 구성하고 있다는 점을 고려하면 이들의 보안·DR 역량은 개별 기업 차원을 넘어 산업 전반의 안정성과 연계되어 해석될 수 있다. 이러한 관점에서 중소·중견 기업의 보안 체계 고도화는 공급망 ESG 리스크를 완화하는 하나의 접근 방향으로 논의될 여지가 있다(나진성, 2022).

2.2 정보보안 및 DR체계 이론

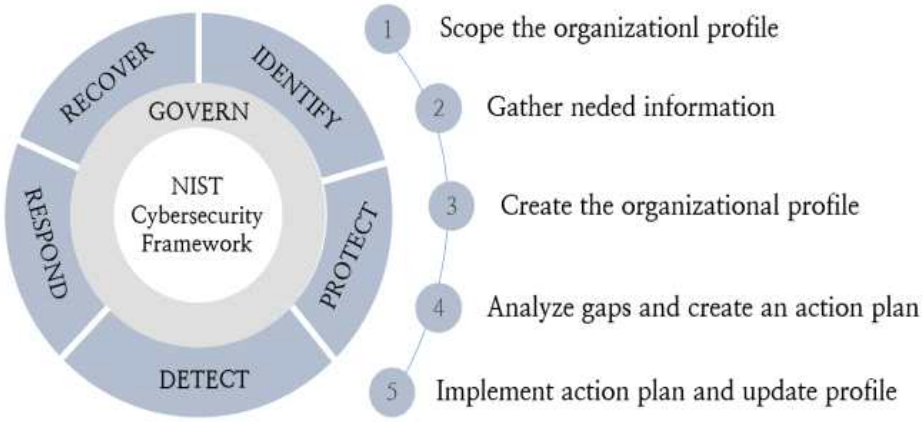
디지털 전환이 일상화된 제조 환경에서 정보보안과 재해복구(DR)는 더 이상 분리된 기술 영역으로 구분하지 않고 있다(김현주 외, 2013; 박유림 외, 2017; 강현선, 2018). 특히 스마트공장 환경은 OT(운영기술)와 IT가 결합되면서 장애나 침해사고가 곧바로 생산중단과 품질 리스크로 이어진다(권영국 외, 2021). 이런 맥락에서 보안은 “침해를 막는 체계”에 머물지 않고 사고를 전제로 업무연속성(BCP) 과 복원력(resilience) 을 포함하는 관리체계로 확장되는 흐름이 뚜렷하다(이수종 외, 2013; 박유림 외, 2017; 최재혁 외, 2019; 김종원 외, 2023).

2.2.1 정보보안 프레임워크

조직의 정보보안 체계는 정보자산 보호를 위한 핵심 관리 기반으로서 기밀성·무결성·가용성이라는 보안 원칙을 지속적으로 유지하는 데 목적이 있다. 이를 달성하기 위해 관리 정책, 내부 절차, 기술적 보호 장치, 물리적 보안 환경이 상호 연계된 형태로 운영된다. 이러한 보안 관리 접근을 체계화한 국제적 기준으로는 NIST가 제시한 사이버보안 프레임워크와 ISO가 제정한 ISO/IEC 27001 정보보안 관리체계 표준이 널리 활용되고 있다.

[그림 2-4]는 NIST CSF 2.0을 토대로 사이버보안 위험 관리를 조직의 전반적인 위험관리 체계와 연계할 수 있는 보안 프레임워크를 나타낸다. 이 프레임워크는 사이버 위협을 독립적인 기술 문제로 다루는 방식에서 벗어나 조직의 기존 위험관리 프로세스 내에 통합함으로써 관리의 일관성과 효율성

을 강화하는 데 목적이 있다. 더 나아가서 클라우드, 데이터 기반 운영, 지능형 ICT 환경 등 변화하는 기술 조건에서도 적용 가능하도록 설계되어 지속적인 보안 관리와 위험 대응을 지원하는 구조적 기준을 제시한다.



[그림 2-4] NIST CSF 조직(KISA, 2024)

NIST CSF는 Identify – Protect – Detect – Respond – Recover의 5단계 구조로 구성되며, 특히 “Recover” 단계는 재해복구(DR) 및 업무연속성계획(BCP)과 직접적으로 연계된다. 중소·중견 기업 대상 연구에서는 NIST CSF가 단계적 실행 구조를 제공함으로써 실무 적용성이 높고 보안 체계의 성숙도 진단에 효과적인 프레임워크로 평가되고 있다.

ISO/IEC 27001은 정보보안 관리체계(ISMS)를 구축하기 위한 국제 표준으로, 리스크 평가, 대응, 정책 수립, 운영 관리 등 전사적 통제 체계를 요구한다. 인증 기반 체계라는 특성상 대기업에는 널리 확산되어 있으나 중소·중견 기업의 경우 비용과 전문 인력 부족으로 전면 도입에 현실적 제약이 존재한다.

두 프레임워크는 모두 데이터의 기밀성·무결성·가용성 확보를 핵심 관리 대상으로 규정하며 이는 ESG 지배구조(G) 영역에서 요구되는 공시 신뢰성과 내부통제와 직결된다. 특히 사이버 사고로 인한 운영 중단과 데이터 훼손은 ESG 평가와 투자 신뢰에 영향을 미치는 거버넌스 리스크로 확장되고 있다.

이러한 점에서 NIST CSF는 운영 실행 중심의 프레임워크로 ISO/IEC 27001은 거버넌스·통제 중심의 표준으로 상호보완적 성격을 가지며 중소·중견 기업 환경에서는 두 체계를 결합한 통합적 접근이 보다 현실적인 대안이 될 수 있다. 이 특성은 본 연구가 ESG 지배구조 관점에서 보안·DR 요소를 구조화하고 우선순위 모델을 도출하고자 하는 연구 설계의 이론적 기반을 제공한다.

2.2.2 DR/BCP 프레임워크

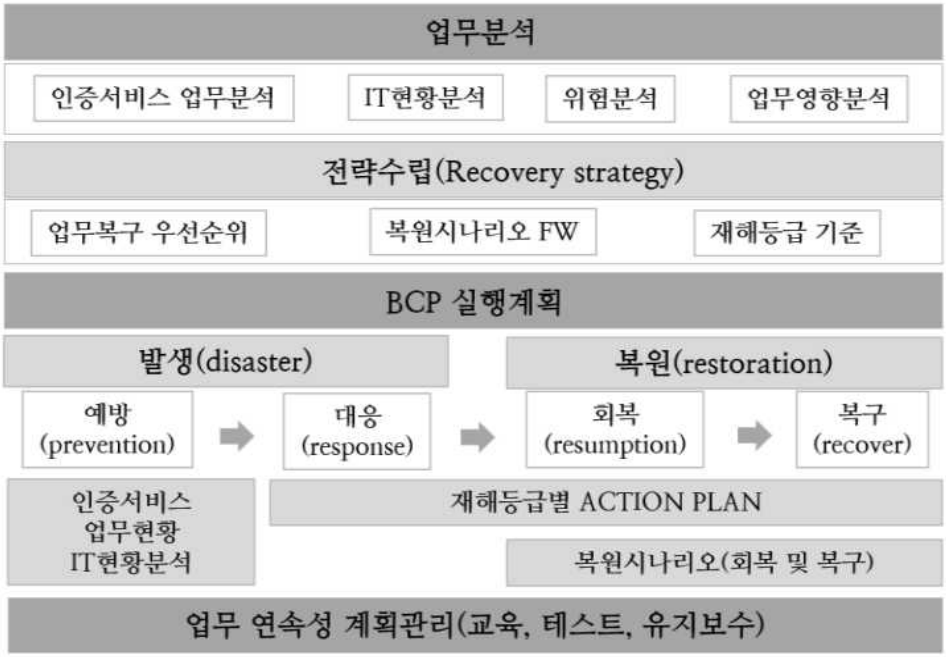
DR(Disaster Recovery)과 BCP(Business Continuity Planning)은 조직이 장애·재난 등으로부터 핵심 업무와 서비스를 복구하고 운영 중단을 최소화할 수 있는 역량을 의미한다.

첫째, NIST SP 800-34 Rev.1은 DR 및 BCP 수립을 위한 국제적 기준으로, 비즈니스 영향 분석(BIA), 복구 전략 수립, 재난 대응 절차, 테스트 및 검증 단계로 구성된다. 이 문서는 특히 중소·중견 기업이 체계적인 복구 계획을 설계하기 위한 표준화된 참조 프레임워크로 활용될 수 있다.

둘째, 아시아개발은행(ADB)과 PDRF가 제시한 MSME DR 프레임워크는 인력과 예산 제약을 고려하여 최소 요건 중심의 복구 전략을 제안한다. 선행 연구에 따르면 기업은 선진 DR 모델을 그대로 적용하기보다 업종 특성과 조직 여건을 반영한 최소 필수 DR 전략을 구축하는 것이 실효성이 높다고 보고되고 있다.

셋째, Cyber Resilience는 보안 사고 이후에도 기업이 운영을 유지·복원할 수 있는 능력을 의미하며 특히, White Paper(2025)는 복원력이 ESG 전 영역(E·S·G)의 기반 역량이며 복구 체계 부재는 공시 신뢰성과 기업가치에 부정적 영향을 미친다고 지적하였다.

[그림 2-5]는 ISO 22301 표준을 기반으로 재난 발생 이전의 예방·대응 단계부터 복구·재개·유지관리 단계까지를 포함하는 비즈니스 연속성 관리 체계를 제시한 것이다. 이 체계는 업무 영향 분석, 복원 시나리오, 대응 조직, 지속적 교육·훈련을 통합함으로써 DR과 BCP를 단순한 기술 계획이 아닌 전사적 운영·거버넌스 체계로 확장한다.



[그림 2-5] BCP-DR 연계 프레임워크(KISA, 2025; 연구자 재구성, 2025)

2.2.3 Cyber Resilience 개념과 최신 연구 동향

최근 연구와 정책 문서는 사이버보안과 DR을 별개로 다루기보다 사이버 복원력(Cyber Resilience) 이라는 상위 개념으로 통합하는 경향이 강하다. 복원력은 단순히 침해를 차단하는 능력만을 뜻하지 않는다. 사고가 발생하더라도 핵심 기능을 유지하고 피해를 제한하며 빠르게 복구하고 이후 더 강해지도록 학습하는 능력을 포함한다(WHITE PAPER, 2024).

최근 연구들은 사이버 보안과 DR을 분리된 체계로 보지 않고 복원력 기반 통합 모델로 이해하며 주요 동향은 다음과 같다.

첫 번째로 사고 대응 체계는 사고 이전(Prevent)-사고 동안(Withstand)-사고 이후(Recover)의 3단계 구조로 설명될 수 있으며, 이러한 틀 위에서 AI 기반 이상 탐지 및 자동 복구 전략의 도입, 공급망 단위의 복원력 평가 모델 제시, 그리고 중소·중견 기업의 복원력 성숙도 수준을 측정하기 위한 간소화된 체크리스트 개발이 주요 구성요소로 논의된다. 나아가 ESG 공시 기준에서 요구하는 '지

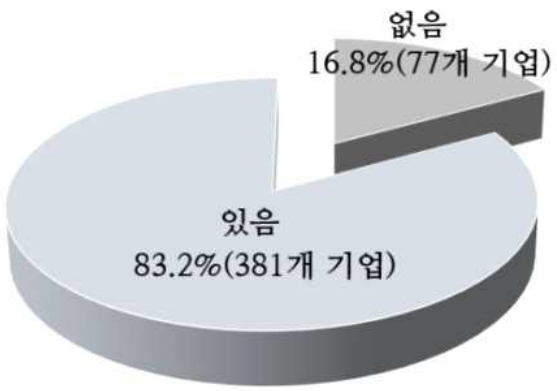
배구조의 신뢰성 확보'는 복원력 개념과 직접적으로 연결되며, 이는 본 연구가 지향하는 AHP 기반 보안·DR 우선순위 모델의 이론적 기반을 이룬다(최재혁, 2019).

2.3 중소·중견 보안·DR 취약요인 분석

2.3.1 인력·예산·기술적 한계

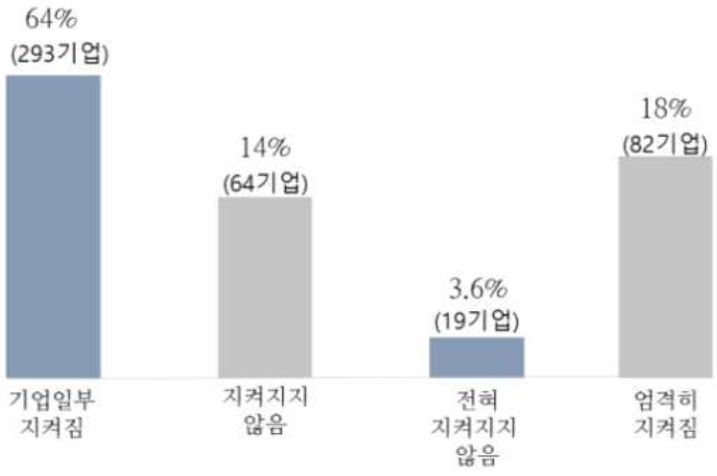
중소·중견 기업의 보안·DR 취약성은 "기술이 없어서"라기보다 인력과 예산이 구조적으로 얇은 상태에서 의사결정과 운영이 굴러가는 방식에서 반복적으로 나타난다. 현장 컨설팅에서 가장 자주 확인되는 패턴은 보안이 전담 기능으로 분리되지 못하고 IT 운영의 한 업무로 흡수되는 구조다. 이 경우 보안은 상시 관리 체계라기보다 장애나 사고가 발생했을 때만 뒤늦게 점검하는 "사후 보완" 성격으로 굳어지기 쉽다.

[그림 2-6]과 같이 중소·중견 기업 제조기업중 자동차분야, 가전분야, 조선, 뿌리기업 등 458개 기업을 대상으로 설문조사를 한 결과 응답기업 중 83.2%가 자체 보안 규정을 보유하고 있으며 자체 보안 규정을 엄격히 지키고 있지 않은 기업은 16.8%에 불과하다고 조사 되었다.



[그림 2-6] 자체 보안규정 보안유무(지란지교소프트, 2025)

[그림 2-7]과 같이 응답기업 64%가 정보보안을 전담하는 책임자를 배치하지 않은 등 체계적인 관리를 하지 못하고 있었으며 3.6%가 기업이 USB 등 이동식 저장매체나 메일 및 메신저 등 인터넷을 통한 정보 유출에 대해 기술적 조치 방안이 마련돼 있지 않은 것으로 나타났다.

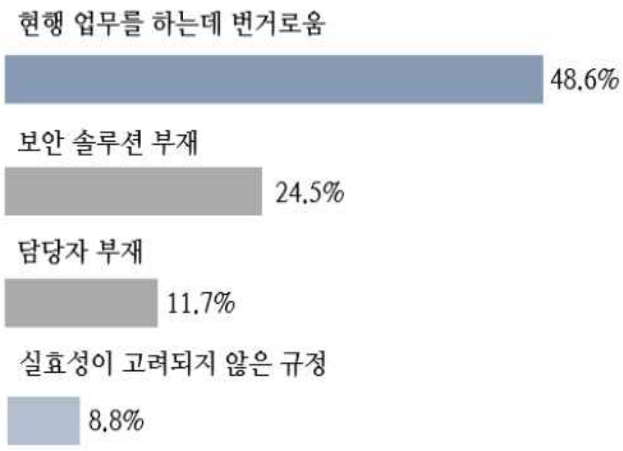


[그림 2-7] 보안규정 준수유무(지란지교소프트, 2025)

[그림 2-8]은 기업이 보안 규정을 준수하지 못하는 주요 원인을 제시한다. '현업 업무 수행에 번거롭다'는 응답이 48.6%로 가장 높게 나타났는데 이는 보안 규정이 실제 업무 흐름과 충분히 연계되지 못하고 현장 운영에 부담 요소로 인식되고 있음을 시사한다. 즉, 보안 통제가 업무 효율성과 충돌할 경우 규정 준수 수준이 저하되는 경향이 확인된다.

'보안 솔루션의 부재'(24.5%)는 규정 이행을 지원할 기술적 기반이 부족함을 의미하며 중소·중견 기업 환경에서 문서 중심 보안체계의 한계를 보여준다. '전담 담당자 부재'(11.7%) 역시 책임 주체와 운영 거버넌스의 미비를 반영하는 결과로 해석된다. 또한 '실효성이 고려되지 않은 규정'(8.8%)은 상위 기준을 그대로 도입한 규정이 현장 환경과 괴리될 경우 형식화될 가능성이 높음을 시사한다.

종합하면, 본 결과는 보안 미준수의 원인이 개인 인식보다 업무 친화성 부족, 기술 지원 미흡, 거버넌스 구조 부재, 현장 부적합 규정 등 구조적 요인에 기인함을 보여주며, 보안·DR 체계를 ESG 지배구조 관점에서 재설계할 필요성을 뒷받침한다.



[그림 2-8] 보안규정이 지켜지지 않는 이유(지란지교소프트, 2025)

첫 번째, NIST(2021)의 소규모 기업 실태 조사에서도 70% 이상이 문서화된 DR 계획을 갖추지 못한 것으로 보고되었으며 이는 전문 인력 부재가 복구 체계 부실로 직결됨을 시사한다. 한편 정보보호 산업 조사에서도 숙련 중급인력의 이탈이 지속적으로 발생해 “확보·유지” 자체가 어려우며 인력 이동이 생기면 업무 인수인계에도 영향을 미치게 되어 결국 업무 공백이 발생하는 리스크를 겪게 된다. 그리고 업무 공백을 메우기 위한 재교육이나 직무 전환을 해야하기에 이에 대한 문제가 커지고 있다(KISA, 2024).

두 번째, 보안 예산의 일회성·비정기성으로 대기업과 달리 중소·중견 기업의 보안 투자는 연간 계획이 아닌 사고 발생 후 단기 보완 형태로 이뤄지는 경향이 강하다. 이러한 이유로는 예산이 “고정비”가 아닌 “변동비”로 분류하고 있으며 ESG 대응 예산에서도 보안은 우선순위에서 낮고 DR센터·백업 인프라 구축 비용을 부담하기 어려움 등이 있다. 이와 같은 예산 구조는 DR/BCP 체계 구축의 지속성을 저해하고 사고 후 복구 실패 가능성을 증가시키는 주요 요인으로 작용한다.

세 번째, 최신 보안 기술 도입의 어려움으로는 AI 기반 탐지·자동화 백업·제로트러스트 등 최신 보안 기술은 중소·중견 기업에게 비용·운영 난이도 측면에서 진입장벽이 높고, 구축 비용 대비 효과 측정 어려움, 기술 운영을 위한 전문성 부족, 외부 공급업체 의존도 증가로 인하여 장기적 비용 부담

증가로 이어지고 있는 실정이다.

Chen et al.(2023)는 백업 및 DR 시스템 구성요소를 분석한 결과를 보면 중소·중견 기업의 기술적 취약성보다 거버넌스 부재가 복구 실패의 더 큰 원인임을 강조하였다. 즉, 기술 도입 부족은 단일 문제가 아니라 조직적 미비와 결합해 리스크를 키운다.

2.3.2 스마트공장 도입 환경에서의 위험요인

제조업의 디지털 전환이 가속화되면서 보안 리스크는 새로운 양상으로 확장되고 있다. 스마트공장 시스템은 생산성 향상을 가능하게 하지만 정보보안과 DR 측면에서는 기존 IT 환경보다 훨씬 복잡한 위험 요인을 내포하고 있다.

첫 번째, 스마트공장 환경에서는 IT(정보기술)와 OT(운영기술)가 긴밀하게 연결되며 기존 OT(운영기술) 설비에 없던 네트워크 연결이 보안 취약점을 만든다. OT(운영기술) 장비는 보안 패치가 어렵고 PLC·HMI 등 제어장비는 기본적으로 방어 기능이 약하며 OT(운영기술) 침해는 생산설비 중단으로 직결됨으로 ESG ‘운영연속성’에 직접 영향을 준다.

두 번째, 수많은 IoT 센서가 실시간 데이터를 수집하면서, 데이터 무결성·접근권한·통신 암호화 등 보안 요구사항이 급격히 증가하고 있는 실정이며 센서·게이트웨이 장비의 인증 체계 미비, 원격 유지보수 채널이 공격 통로로 악용, 데이터 조작 시 품질 불량 및 안전사고로 이어질 가능성이 높게 나타나고 있다.

세 번째, 스마트공장 설비는 대체로 수명이 길고 패치 주기가 불규칙하여 새로운 취약점 대응이 지연되는 경우가 많다. 이는 국외 설비의 경우 패치 배포 지연 제조사가 보안 지원을 중단하는 장치 존재와 패치 적용 시 생산 중단으로 이어지게 됨으로 기피 현상이 발생한다. PMC(2024)는 이러한 구조적 문제로 인해 스마트공장 보안 취약성이 생산 차질·납기 지연·품질 문제를 유발하여 ESG 평가의 운영연속성 지표에 부정적 영향을 미친다고 분석하였다.

KISA의 스마트공장 보안위협 가이드 [그림2-9]의 8가지 중소·중견 제조기반의 스마트공장 보안위협 내용은 다음과 같다.

첫째, 의도적인 공격 행위에 기인한 위협은 내부자 또는 외부 공격자가 시

스템의 정상적인 운영을 방해하거나 정보를 탈취하기 위해 수행하는 행위를 의미한다. 여기에는 서비스 이용을 마비시키는 공격, 악성코드 유포, 설비 및 소프트웨어의 무단 변경, 생산·운영 데이터의 변조, 특정 기업이나 공정을 겨냥한 표적 침해, 개인정보의 부적절한 활용, 반복적인 인증 시도를 통한 침입 시도 등이 포함된다. 이러한 위협은 생산 연속성과 데이터 신뢰성에 직접적인 영향을 미친다.

둘째, 통신 도청 및 정보 노출과 관련된 위협은 스마트공장 내 다양한 시스템과 IoT 장치 간 통신 과정에서 발생한다. 통신 경로에 제3자가 개입하는 중간자 공격은 IoT 통신 프로토콜의 탈취 또는 변조와 네트워크 트래픽 분석을 통한 시스템 구조 노출 등이 대표적이며 이는 제어 명령이나 생산 정보의 외부 유출로 이어질 수 있다.

셋째, 물리적 침해로 인한 위협은 공장 설비나 기반 인프라에 대한 직접적 또는 간접적 물리 공격을 포함한다. 생산 설비, 제어 장치, 통신 장비 등이 훼손되거나 파괴될 경우 단순한 보안 문제를 넘어 안전사고 및 장기적인 생산 중단으로 확산될 가능성이 있다.

넷째, 비의도적 사고로 인한 보안위험은 악의적 목적이 아닌 운영 과정에서의 실수나 관리 부재로 발생한다. 예를 들면, 의도하지 않은 데이터 삭제 또는 설정 변경, 장비나 시스템의 부적절한 사용, 외주 인력이나 협력업체로 인한 정보 손실 등이 이에 해당하며 관리 체계 미흡 시 반복적으로 발생할 수 있다.

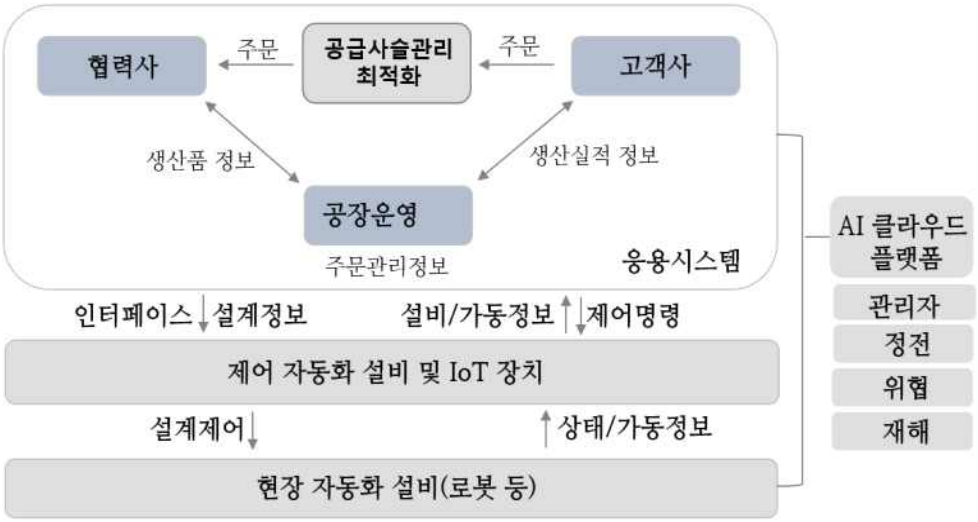
다섯째, 설비 및 시스템의 고장 또는 오작동에 따른 위협은 기술적 결함과 운영상의 문제에서 비롯된다. 센서나 액추에이터의 오류, 제어 시스템의 장애, 소프트웨어 취약점의 악용, 서비스 제공 업체의 실수 또는 서비스 중단 등이 포함되며 이는 공정 품질 저하와 운영 불안정성을 초래한다.

여섯째, 전력 및 기반 서비스 중단으로 인한 위협은 스마트공장의 연속 운영을 저해하는 주요 요인이다. 전원 공급 장애, 통신 네트워크 중단, 보안 관제, 데이터 백업과 같은 지원 서비스의 상실은 생산 차질뿐 아니라 데이터 손실 위험을 동반한다.

일곱째, 법·제도적 측면의 위협은 관련 법규나 계약 조건을 충족하지 못할

경우 발생한다. 개인정보 보호 규정 위반이나 계약상 보안 의무 불이행은 기업의 신뢰도 저하뿐 아니라 법적·재무적 리스크로 이어질 수 있다.

마지막으로, 자연적·환경적 요인에 따른 위협은 기업이 통제하기 어려운 외부 요인에서 기인한다. 지진, 홍수, 태풍과 같은 자연재해나 화재, 환경 오염 사고 등은 스마트공장 인프라와 정보 자산 전반에 광범위한 피해를 유발할 수 있다.



[그림 2-9] 스마트공장 보안위협 가이드(KISA, 2019)

2.3.3 중소·중견 기업의 ESG 정보보안 거버넌스 특징

디지털 전환이 일상화된 제조 현장에서 중소·중견 기업의 보안·DR 취약성은 종종 “기술 부재”보다 조직 운영과 거버넌스의 구조적 미비에서 반복적으로 드러난다. 실제 국내 실태 조사에서도 중소·중견·벤처기업은 전담인력·예산·조직 기반이 약한 상태가 확인되었으며 이 조건 자체가 상시적인 보안관리 체계 정착을 어렵게 만든다(KISA, 2018; KISA, 2023). 또한 중소·중견 기업에서는 보안이 전담 기능으로 분리되기보다 IT 운영업무에 흡수되어 사고 직후에만 관심과 자원이 집중되는 “사후 보완” 패턴이 나타난다는 지적도 꾸준히 제기되어 왔다(여상수 외, 2009). 현장에서 컨설팅을 수행하다 보면 자주

나타나는 문제는 다음과 같이 네가지로 분류해 볼 수 있다.

첫 번째, 책임 주체의 부재가 가장 큰 문제로 부각되고 있다. CISO가 없고 정책 수립·이행·점검의 흐름이 약하면 역할·책임(R&R)이 불명확해지면서 사고 대응 체계와 투자 의사결정도 비정형적으로 굴러가기 쉽다(여상수 외, 2009; 박유림 외, 2017).

두 번째, 기본 통제의 누락이다. 공용계정 사용, 퇴사자 계정 미삭제, 접근권한 최소화 미흡 같은 계정·권한관리의 빈틈은 랜섬웨어 확산이나 내부자 위협, 데이터 유출의 출발점이 되기 쉬운데 이는 국내 ISMS-P 기준에서도 핵심 통제 항목으로 반복적으로 요구되는 부분이다(KISA, 2025).

세 번째, 로그·관제 기반 부족이다. 로그가 충분히 남지 않거나 장기 보관·위변조 방지가 미흡하면 사고 원인 분석이 어려워지고 결과적으로 재발방지와 감사·규제 대응과 같은 대외 설명시 신뢰성이 저하되기도 한다(KISA, 2025).

네 번째, DR 운영의 문서화·훈련 부재다. 백업을 하고 있어도 주기·보관 방식·복구 절차가 문서화되어 있지 않거나 복구 테스트가 없으면 실제 사고에서 복구 성공률이 급감한다는 점은 국내에서도 BCP 관점의 DR 설계 필요성과 ISMS 관점의 통합관리 논의로 이어져 왔다(김현주 외, 2013; 박유림 외, 2017). 국외 연구에서는 DR 구성요소보다 거버넌스 부재가 복구 실패를 좌우할 수 있다고 하였다(Chen, 2023)

2.4 계층분석법(AHP) 정의

2.4.1 AHP 개요

계층분석법(AHP: Analytic Hierarchy Process)은 Saaty가 제안한 대표적 다기준 의사결정(MCDM) 기법으로 복잡한 의사결정 문제를 논리적 계층 구조로 분해한 뒤 쌍대비교(pairwise comparison)를 통해 요소 간 상대적 중요도를 정량화하는 방법이다(Saaty, 1980; Saaty, 1987). 이러한 접근은 평가기준이 다층적이고 정성적 판단이 불가피한 영역에서 의사결정 근거를 구조화할 수 있다는 점에서 정책·경영 분야에 폭넓게 적용되어 왔다(고길곤 외,

2008). AHP는 “정답이 하나로 고정되기 어려운” 현실 문제에서 전문가의 판단을 구조화해 우선순위(weight/priority)로 제시한다는 점에서 정책·경영·리스크 분야에서 폭넓게 활용되어 왔다(고길곤 외, 2008).

현장에서 중소·중견 기업의 보안·DR 수준을 진단하다 보면 “무엇이 더 급한가”를 두고 이해관계자가 서로 다른 언어로 이야기하는 장면을 자주 마주한다. 이때 AHP는 정성적 판단을 명시적으로 구조화하고, 전문가 판단의 논리성을 일관성 검증으로 확인할 수 있어 보안·DR·ESG처럼 요소가 많고 상호 연동되는 평가 문제에 실무적으로 잘 맞는다(남정민 외, 2022).

본 연구는 보안과 DR 그리고 ESG는 서로 따로 움직이는 영역이 아니라는 데에 중점을 두고 있다. 접근 통제가 약하면 사고 가능성이 커지게 되고 로그/백업이 약하면 사고 후 복구 성패가 갈리는 구조와 같이 동일한 운영 현장에서 상호 제약과 연쇄 효과를 만들며 평가 과정에는 필연적으로 정성적 판단이 개입된다. 이런 상황에서 AHP는 “누가 봐도 납득 가능한 절차”로 판단을 수치화하고 합의 가능한 우선순위를 도출하는 데 유용하다(Saaty, 1980; 고길곤 외, 2008).

AHP의 주요 특징은 다음과 같이 정리할 수 있다.

첫 번째, 계층화(Hierarchical structuring) 기능을 통해 문제를 ①목표 ②평가기준 ③세부요소 ④대안 순의 형태로 구조화함으로써 복잡한 의사결정의 범위를 관리 가능한 단위로 줄일 수 있다(Saaty, 1980).

두 번째, 정성·정량 정보를 함께 수용할 수 있다. 즉 “어느 요소가 더 중요한가”와 같은 질적 판단을 1~9 척도 기반의 비교 판단으로 변환해 가중치를 산출한다(Saaty, 1980; Saaty, 1987).

세 번째, 보안 전문가, ESG 평가자, 스마트공장 구축 실무자 등과 같이 다양한 이해관계자들의 의견을 일관된 계산 틀 안에서 통합할 수 있다. 국내에서도 AHP를 활용해 학계·실무 전문가 집단의 인식 차이를 비교하고 우선순위를 도출하는 방식이 정책·위험관리 연구에서 반복적으로 적용되어 왔다(이홍재 외, 2017; 고길곤 외, 2008).

네 번째, 일관성 검증(Consistency Ratio; CR) 절차를 통해 전문가 판단의 논리적 타당성을 점검할 수 있어 연구 설계 단계에서 “판단의 질”을 통제

할 수 있다(Saaty, 1980).

다섯 번째, 이 모든 과정이 단계적으로 기록되기 때문에 결과 가중치가 “어떻게 도출되었는지”를 설명하기 쉬워 의사결정의 투명성을 높인다. 이는 평가 기준이 다층적인 ESG 지표나 통제 항목이 많은 보안/관리체계 평가에서 특히 강점으로 작동한다(이중정 외, 2014; 남정민 외, 2022).

국내 연구에서의 AHP는 ESG 요소의 중요도를 도출하거나(남정민 외, 2022), 정보보호 투자·위협요인·관리체계 항목의 우선순위를 정리하는 데 활용되어 왔다(성기훈 외, 2010; 이중정 외, 2014). 그리고 AHP의 측정·평가 관점에서 기본 개념과 해석의 틀을 비교적 체계적으로 정리해 왔다(민재형, 1996). 또한, AHP는 정책·행정 분야에서 폭넓게 활용되어 왔으며 적용 과정에서 발생하는 설계·표본·강건성(robustness) 이슈까지 점검한 메타 분석이 축적되어 있다(고길곤 외, 2008). 이는 곧, AHP가 “보안·DR·ESG처럼 정량만으로 설명하기 어려운 분야”에서 실무적 설득력을 갖춘 분석 도구로 자리 잡아 왔음을 보여준다.

따라서 본 연구의 문제의식인 “중소·중견 기업 보안·DR 구성요소의 우선순위 도출”은 ①평가요소의 다층성과 복잡성, ②요소 간 상호작용, ③전문가 정성 판단의 정량화 필요성이 동시에 존재한다. 이러한 조건을 고려할 때 AHP는 현장 전문가의 판단을 체계적으로 수렴하면서도(이홍재 외, 2017), 결과의 일관성과 설명 가능성을 확보할 수 있는 방법론으로 판단된다(Saaty, 1980; 고길곤 외, 2008).

2.4.2 AHP 의사결정 적용 방식

AHP(Analytic Hierarchy Process) 활용시 적용 절차의 첫 단계는 문제 정의와 목표 설정이다. 무엇을 결정할 것인지에 대한 평가의 목적을 명확히 규정한 후 ①목표 ②기준 ③세부요소 ④대안 순의 형태로 문제를 계층화(hierarchy)하여 비교 가능한 구조로 정리한다(Saaty, 1980). 이 과정에서 기준 간 중복이나 정의의 불명확성은 비교 판단의 왜곡으로 이어질 수 있으므로 항목의 개념과 범위를 사전에 정교하게 합의하는 것이 중요하다(고길곤 외, 2008).

다음으로 계층의 각 수준에서 요소 간 쌍대비교 행렬을 구성한다. 비교는

“A가 B보다 얼마나 중요한가”를 묻는 방식으로 수행되며 일반적으로 1~9의 Saaty 척도를 활용해 판단 강도를 수치화한다(Saaty, 1980; Saaty, 1987). 다수 전문가가 참여하는 경우에는 개별 판단을 집단 판단으로 통합하기 위해 기하평균과 같은 대표값으로 행렬을 결합하는 방식이 널리 사용된다(Saaty, 1980; 고길곤 외, 2008). 이후 쌍대비교 행렬로부터 각 요소의 가중치(weight)를 산정하고, 상위–하위 가중치를 종합하여 최종 우선순위를 도출한다(Saaty, 1980). 이때 AHP는 판단의 신뢰도를 확보하기 위해 일관성 검증(consistency check)을 포함하며 일관성지수(CI)와 일관성비율(CR)을 통해 비교 판단이 논리적으로 수용 가능한지 점검한다(Saaty, 1980).

일반적으로 CR이 기준값(예: 0.1) 이하일 때 일관성이 확보된 것으로 해석하며 기준을 초과하면 비교 판단을 재검토하거나 기준 정의를 보완하는 방식으로 응답 품질을 개선한다(Saaty, 1980; 고길곤 외, 2008). 따라서, 집단 의사결정이 필요한 경우(보안 전문가, 스마트공장 구축 PM, ESG/내부통제 담당 등)에는 개인 판단을 통합하는 방식이 연구의 품질을 좌우한다. 국내에서는 다수 전문가 의견 종합(우선순위 결합)의 방법론이 비교적 일찍부터 논의되어 왔다(김성철 외, 1994). 더불어 다수 전문가의 이상치나 불일치 판단을 다루기 위한 절차도 제안되어 왔다(조성훈 외, 1998).

가중치 산정과 집단판단 통합을 위한 쌍대비교는 Saaty의 1–9 척도를 사용해 전문가가 두 요소의 상대적 중요도를 판단하도록 구성하였다. 실제 국내 AHP 적용 연구에서도 9점 척도를 기반으로 쌍대비교 행렬을 구성하고 각 행의 기하평균(geometric mean) 등을 활용해 집단 응답을 통합한 뒤 가중치를 산정하는 절차가 흔히 사용된다(김규범 외, 2025). 또한 쌍대비교 행렬로부터 고유벡터 기반의 가중치를 도출하고 응답의 논리적 모순 정도를 CI/CR로 확인하는 방식은 국내 디지털 성숙도 지표 가중치 연구에서도 동일하게 기술된다(김성훈, 2023).

최근 국내에서도 ESG 실행요인의 우선순위를 도출하거나 산업별 진단항목 가중치를 산정하는 데 AHP가 폭넓게 활용되고 있는데 예컨대 중소·중견 물류기업의 ESG 이행 진단항목 가중치를 AHP로 도출한 연구(박원배 외, 2024). 뿌리산업(중소·중견 기업 비중이 큰 산업군)에서 ESG 활동 요인의 중

요도·우선순위를 AHP로 분석한 연구는 현장형 이슈를 '가중치'로 변환하는 방법으로서 AHP의 유용성을 보여준다(송우창, 2024).

해외 연구에서는 집단 통합을 AIJ(개별 판단행렬의 통합)와 AIP(개별 우선순위의 통합)로 구분해 설명하며 집단이 "하나의 행위자처럼" 판단하는지 또는 "개인의 집합"인지에 따라 적절한 결합 방식이 달라질 수 있음을 정리한다(Forman & Peniwati, 1998). AHP 방법론 전개를 정리한 국제적 리뷰는 모델링, 판단척도, 일관성, 불완전 행렬, 민감도, 집단 의사결정 등 확장 주제를 폭넓게 다루며 연구 설계 시 참고할 실무적 체크포인트를 제공한다(Ishizaka & Labib, 2011). 정리하면 AHP는 ①계층화 → ②쌍대비교 → ③가중치 산정 → ④일관성 검증 → ⑤종합 우선순위 도출의 흐름으로 운영되며 결과가 "왜 그렇게 도출되었는지"를 절차적으로 설명할 수 있어 의사결정의 투명성을 높인다(고길곤 외, 2008).

본 연구는 이 절차를 활용하여 중소·중견 기업 보안·DR 구성요소의 상대적 중요도를 도출하고 제한된 자원 환경에서 단계적 개선 우선순위를 설정하는 근거로 활용하고자 한다(Saaty, 1980; 고길곤 외, 2008).

2.4.3 AHP 계층구조 설계 및 일관성 검증

계층구조 설계는 AHP 결과의 설득력을 좌우한다. 제가 현장에서 체크리스트를 만들 때도 늘 같은 결론에 도달하는데 "요소를 많이 넣는 것"이 정답이 아니라 상위 기준은 적고 명확하게 하위 요소는 중복을 줄이고 현장 언어로 정의하는 편이 응답 품질을 훨씬 올린다. 실제로 국내 정책 연구에서 AHP 적용 과정의 문제점(설문 스크리닝, 표본 선별, 결과 도출의 강건성 등)을 분석한 연구는 계층 설계와 데이터 정제가 실무적으로 얼마나 중요한지 반복적으로 강조한다(고길곤 외, 2008). 그리고 쌍대비교 척도 자체가 응답 일관성에 영향을 줄 수 있다는 점도 간과하기 쉽다. 국내 연구에서는 기존 9점 척도(양방향 17점 표현)가 오히려 응답자의 일관성을 저하시킬 수 있다는 문제의식에서 더 단순하면서도 일관성을 높이는 척도 재구성을 제안한 바 있다(송근원 외, 2013).

일관성 검증은 AHP의 핵심 절차로 일반적으로 일관성비율(CR)을 통해 판단의 논리적 타당성을 확인한다(Saaty, 1987). 국내 실증연구에서는 CR 기준을 0.1 이하로 두는 사례도 많고(서윤정 외, 2013). 현실적 제약을 고려하여 0.2 이하까지 허용하는 사례도 확인된다(정우수, 2008). 즉, 연구 주제·표본 특성·의사결정 난이도에 따라 허용 기준을 어떻게 운영할지에 대한 "연구자 판단"이 필요하다. 한편, 일관성 지수/비율을 단순 임계값으로만 처리하기보다 차원별 분포 특성과 통계적 검정 관점에서 접근한 국내 연구도 존재한다. 이는 설문 데이터를 "버릴지/재조사할지"를 기계적으로 결정하기보다 일관성의 의미를 더 엄밀히 다루려는 시도로 이해할 수 있다(이종찬 외, 2014).

최근 국내 연구들도 이 기준을 실무 운영 규칙으로 활용한다. 예를 들어 스마트항만 기술 도입 우선순위를 다룬 연구는 CI/CR이 0.1 이상이면 재설문을 실시해 0.1 미만이 되도록 조정했다고 명시했고(한승훈, 2024). 자망 어구 보증금제 표식 방안 연구 역시 CR 0.1 이상 응답은 재설문 요청 또는 제외하는 방식으로 표본을 정제했다(차은, 2025). 또한 특구 제도 문제점에 대한 인식 차이를 비교한 연구에서는 CR을 기준으로 응답 품질을 관리하며 복잡한 의사결정 환경에서 0.1~0.2 기준의 해석 틀을 함께 제시한다(서정흔 외, 2025).

현장에서는 비교 항목이 많거나 개념 경계가 겹칠수록 응답자가 순간적으로 판단을 흔들리는 경우가 생기는데 이때 일관성 검증을 '제외'로만 처리하면 오히려 좋은 표본을 잃는 느낌이 있었다. 그래서 최근에는 비일관성의 원인을 줄이기 위한 보정(재점검) 접근이 강조되는 흐름이 보인다. 실제로 AHP 설문 자체를 개선해 CR을 낮추고 무효 응답을 줄이는 방법을 제안·검증한 연구도 발표되었다(박진선 외, 2024). 한편 공공부분의 다기준분석 지침 연구에서는 비일관성 비율이 일정 수준(예: 0.2 이상)이면 재조사가 필요하다는 운영 원칙을 제시한다(KDI, 2011).

따라서, AHP 결과 해석에서 종종 언급되는 순위반전(rank reversal) 문제는 연구 설계 단계에서부터 인지하고 있어야 한다. 국내에서도 집단 의사결정 과정에서 순위반전의 발생과 해결방안을 다룬 논의가 축적되어 있어 결과를 정책·컨설팅 의사결정에 반영할 때 해석의 안전성을 높이는 근거로 활용할 수 있다(강문식, 2003).

AHP 분석을 수행하기 위해서는 문제를 계층 구조(Hierarchy)로 분해하는 과정이 필요하다. 본 연구에서는 ESG 기반 보안·DR 우선순위 도출을 연구 목표로 설정하고 다음과 같은 구조로 계층 모델을 설계하였다.

AHP 분석을 수행하기 위해서는 문제를 계층 구조(Hierarchy)로 분해하는 과정이 필요하다. 본 연구에서는 ESG 기반 보안·DR 우선순위 도출을 연구 목표로 설정하고 다음과 같은 구조로 계층 모델을 설계하였다. 상위 기준은 ESG 지배구조 관점에서 의미가 명확하고 상호 중복 가능성이 낮은 영역으로 제한하였으며 하위 요소는 중소·중견 제조기업 현장에서 실제 관리·통제가 이루어지는 실행 단위 중심으로 구성하였다. 특히 선행연구 검토와 전문가 사전 인터뷰를 병행하여 각 요소의 정의와 범위를 구체화함으로써 응답자가 개념 혼동 없이 비교 판단을 수행할 수 있도록 설계를 보완하였다. 이를 통해 계층 구조의 이론적 타당성과 함께 현장 적용 가능성을 동시에 확보하고자 하였다.

첫 번째로 AHP 계층 구조의 기본형으로 [표2-2]과 같이 레벨 계층 수준이 4단계로 이루어져 있다.

[표 2-2] AHP 계층 구조별 결정요인(Sub-criteria, NIST, (2021); Criteria, IFRS Foundation (2023); GOAL, KPMG (2023)

계층 수준	내용
Level 1: Goal	• ESG 기반 중소·중견 기업 보안·DR 우선순위 결정
Level 2: Criteria	• ESG 요구와 보안 거버넌스 기반의 주요 평가 기준
Level 3: Sub-criteria	• 각 기준을 세분화한 보안·DR 구성요소
Level 4: Alternatives	• 평가 결과로 도출되는 실행 전략 또는 개선 방향

두 번째로 본 연구에서 설계한 AHP 구조 세부 요소로는 ①Goal(목표)로 “중소·중견 기업의 ESG 기반 보안·DR 체계 우선순위 도출” 이는 ESG 경영의 지배구조(G) 요구사항과 기업의 실질적 보안·복구 역량을 연결하여 중소·중견 기업이 제한된 자원으로 가장 효과적인 보안·DR 체계를 구축할 수 있도록 하는 데 목적이 있다. Criteria(평가 기준)의 5대 요소는 [표2-3]과 같이 평가 기준으로 구분된다.

[표 2-3] ESG거버넌스 5대 평가기준 (KISA, 2022; LPMG, 2023; NIST, 2025; 연구자 재구성, 2025)

기준	세부 항목(예시)
보안 거버넌스 (Security Governance)	• 정책·규정·조직 체계 및 관리 프로세스 성숙도 – R&R 정의, 보안책임자 유무, 보안조직 운영
재해복구 (Disaster Recovery, DR)	• 백업체계·복구절차·RTO/RPO 등 원력(Resilience) 요소 – 백업주기, 복구절차 문서화, DR 테스트
기술적 보호조치 (Technical Controls)	• 암호화, 접근통제, 네트워크 보안, OT/IT 보안 등 기술 체계 – 패치관리, 네트워크 분리, 접근제어, OT 보안
보안 인식 및 교육 (Security Awareness)	• 종업원 교육, 보안문화, 내부자 위협 관리 – 정기 교육, 피싱 훈련, 내부자 통제
정책 및 문서화 수준 (Policy & Documentation)	• DR 매뉴얼, 사고보고체계, 로그관리 등 문서기반 통제 – 로그관리, 보안규정, 사고 대응 매뉴얼

세 번째로 Alternatives (대안)은 AHP 결과를 통해 다음과 같은 실행 대안을 비교·결정할 수 있다. 실행 대안 내용으로는 ①DR 우선 구축 전략, ②보안 거버넌스 강화 전략, ③기술적 통제 중심 전략, ④보안 교육·내부통제 중심 전략을 중심으로 중소·중견 기업은 자원과 인력의 문제를 해결하고 이를 위한 AHP 산출 내용은 실행 전략 선택에 매우 중요한 역할을 한다.

따라서 AHP 신뢰도를 평가하는 기준으로서 일관성 검증과 보정은 매우 중요하다. Saaty는 무작위 행렬 대비 일관성비율(CR)이 충분히 작을 때(경험칙으로 약 10% 이하) 판단을 수용할 수 있다고 설명한다(Saaty, 1990).

[표 2-4] 일관성 검증 및 관리 Flow (연구자 재구성, 2025)

단계	주제	내용	비고
1	1차 검증	• 응답자별 CR을 산출하고, 기준(원칙: CR ≤ 0.10)을 넘는 응답은 비교쌍을 다시 확인하도록 안내	Saaty(1990), 한승훈(2024)
2	보정(재응답)	• 동일 기준 초과 구간이 반복되는 항목은 질문 문구/정의(용어)를 다시 설명하고 재응답을 받음	박진선 외(2024)
3	정제	• 재응답 이후에도 기준을 지속적으로 초과하는 응답은 분석에서 제외하고, 최종적으로 기준 충족 표본만으로 가중치를 확정	KDI(2011), 차은(2025)

결국 이 과정은 “CR 수치 맞추기”가 목적이 아니라 전문가 판단이 흔들리는 지점을 찾아 계층 정의와 설문을 정돈해가는 품질관리 과정에 가깝다(박진선 외, 2024; 서정흔 외, 2025).

2.4.4 민감도 분석 및 한계

AHP로 산출된 우선순위가 실제 컨설팅 의사결정(예산·인력·규제 압력 변화)에 “버틸 수 있는 결과”인지 확인하기 위해 본 연구에서는 민감도 분석(sensitivity analysis)을 필수 검증 절차로 둔다(Ishizaka & Labib, 2011).

국내에서도 AHP를 적용한 뒤 결과의 신뢰성을 설명할 때 민감도 분석을 함께 수행하는 흐름이 점점 일반화되고 있는데 예컨대 AHP 기반 우선순위를 도출한 뒤 민감도 분석으로 결과 변동 가능성을 점검한 연구(유근환, 2023), AHP-TOPSIS 기반 의사결정 결과를 일관성 검증과 민감도 분석으로 함께 검증한 연구(주현철 외, 2025), 산출 가중치의 변동 영향을 민감도 분석으로 확인하고 다른 전문가 집단으로 적합성까지 재검증한 연구(엄진욱 외, 2023), 그리고 ‘민감도 분석+다기준 의사결정’ 결합으로 대안 선택의 안정성을 보여준 연구(김준섭 외, 2024) 등에서 공통적으로 확인된다.

본 연구의 민감도 분석은 실무에서 가장 해석이 명료한 방식으로 설계한다. 즉, 상위 기준(예: 거버넌스/운영통제/기술통제/복구·연속성)의 가중치를 ±10%, ±20%, ±30% 범위에서 단계적으로 변화시키고(나머지 기준은 합이 1이 되도록 재정규화), 변화 시나리오별로 최종 우선순위(특히 상위 Top-k)가 유지되는지와 순위 역전이 발생하는 임계 구간이 어디인지 확인한다(김준섭 외, 2024; 주현철 외, 2025).

또한 최근 MCDA 분야의 체계적 문헌고찰에서도 민감도 분석이 결과의 신뢰도를 높이는 핵심 장치로 정리되므로 본 연구에서도 “순위가 바뀌지 않는다”는 선언에 그치지 않고 어떤 기준의 변동이 결과를 가장 크게 흔드는지(민감 요인)까지 함께 제시해 해석 가능성을 확보한다(Więckowski & Sałabun, 2023).

다만 한계도 분명하다. 첫째, 민감도 분석은 어디까지나 “가중치 변화”라

는 한 축의 불확실성을 다루는 절차이므로 계층 구조(기준 정의·경계 설정) 자체가 달라질 때의 구조적 불확실성까지 완전히 흡수하진 못한다(Ishizaka & Labib, 2011). 둘째, AHP는 쌍대비교의 일관성을 CR로 점검하는데 실무 연구에서는 통상 CR≤0.1을 수용 기준으로 운영하는 경우가 많다(Saaty, 1990). 하지만 CR을 낮추는 과정이 곧바로 “현실적으로 더 옳은 판단”을 보장하는 것은 아니며 최근에는 판단 일관성을 개선하면서도 순위를 보존하려는 보정 접근(Ishizaka & Siraj, 2020)이나 전문가 판단의 논리적 응집도를 높이기 위한 도구·절차 제안(Frish, 2025)도 제시되고 있어 본 연구 역시 일관성 기준을 ‘기계적으로 통과’시키기보다 비일관성이 발생한 비교쌍을 재확인하는 방식으로 데이터 품질을 관리했다. 셋째, 보안·DR·ESG의 구성요소는 상호 의존성이 강한데(예: 접근통제 미흡이 로그 신뢰성·사고분석·복구절차 전반에 연쇄 영향) AHP의 기본 합성 방식은 기준 간 독립성을 전제로 해 결과 해석에서 이 점을 주의해야 하며 불확실성이 큰 판단을 다루기 위해 퍼지 AHP 등 변형 기법에서 안정성(민감도)을 별도로 비교하는 연구도 참고할 필요가 있다(Vinogradova-Zinkevič, 2023).

본 연구의 “민감도 분석 및 한계”는 AHP 결과를 단순 산출물로 끝내지 않고 현장 변동성에 대한 강건성(robustness) 점검까지 포함해 설명력을 높이는 한편 동시에 계층 구조·판단 불확실성·기준 간 상호의존성이라는 방법론적 한계가 존재한다.

2.5 선행연구 분석

2.5.1 선행연구 분석

국내외에서는 ESG 경영과 정보보안, 재해복구(Disaster Recovery, DR), 그리고 의사결정 기법을 연계한 다양한 선행연구가 축적되어 왔다. 특히 최근 연구들은 전통적인 지배구조 평가나 공시 중심 접근을 넘어 디지털 전환 환경에서 정보보안과 운영연속성(BCP·DR)을 기업 지속가능성을 구성하는 핵심 관리 요소로 다루는 경향을 보이고 있다. 이들 연구는 공통적으로 ①ESG 공

시의 신뢰성 확보를 위한 보안·DR 체계의 구조화, ②사이버 리스크 및 운영 중단 리스크를 ESG 거버넌스 영역에 편입, ③제한된 자원 환경에서의 투자·구축 우선순위 도출 방법론 적용, ④중소·중견 기업에 적합한 실행 중심 모델 제시라는 네 가지 방향으로 전개되고 있다.

지배구조(G) 관점의 연구들은 ESG와 정보보안의 구조적 연계를 실증적으로 제시하고 있다. 최미화(2023)는 국내 기업을 대상으로 한 실증 분석을 통해 이사회 구조, 내부통제 수준, 감사기구 특성이 ESG 공시 품질에 유의미한 영향을 미친다는 점을 입증하였으며 이를 통해 지배구조(G)가 단순한 제도 항목이 아니라 정보의 신뢰성과 관리 성숙도를 결정하는 핵심 변수임을 밝혔다. 송유정 외(2024)는 이사회 차원의 사이버보안 전문성, 전담 위원회 존재 여부, 보안 관련 의사결정 활동성이 보안 공시 가능성과 수준에 긍정적 영향을 미친다는 결과를 제시하며 사이버보안을 IT 부서 차원이 아닌 최고 의사결정 구조의 통제 과제로 확장해야 할 필요성을 강조하였다. 이러한 연구들은 정보보안이 ESG 거버넌스(G)의 핵심 구성요소로 편입되고 있음을 보여준다.

중소·중견 기업을 대상으로 한 연구들은 보안 및 DR 취약성이 기술 자체의 부족보다 거버넌스와 운영 체계 미비에서 비롯된다는 점을 반복적으로 확인한다. 여상수 외(2009)는 중소기업 정보시스템 운영 실태 분석을 통해 보안 전담 인력과 책임 주체 부재와 비정형적 운영 구조가 사고 대응 실패와 서비스 중단 장기화로 이어질 수 있음을 지적하였다. KISA(2023)는 국내 중소·중견 기업 다수가 문서화된 DR 계획, 복구 목표(RTO/RPO), 정기 모의훈련 체계를 갖추지 못하고 있음을 실태조사를 통해 보고하며 중소기업의 DR 역량이 관리체계 결핍 단계에 머물러 있음을 보여주었다. Chen et al.(2023)은 IS 백업 및 DR 시스템 도입 요인을 분석한 결과 하드웨어·소프트웨어보다도 경영진 지원, 역할 정의, 프로세스 표준화 등 거버넌스 요소가 복구 성과에 더 큰 영향을 미친다고 분석하였다. 이는 중소기업 환경에서 보안·DR이 기술 구축 문제가 아니라 조직·의사결정·관리 구조의 문제임을 명확히 시사한다.

한편 정보보안과 DR을 통합적으로 설명하는 개념으로서 사이버 복원력(Cyber Resilience)에 대한 연구도 확대되고 있다. Carias et al.(2020)은 사고 이전(Prevent), 사고 중(Withstand), 사고 이후(Recover)의 3단계 구조를 통해

복원력을 개념화하며, 보안과 복구를 단일 체계로 통합할 필요성을 제시하였다. 이후 연구들은 여기에 AI 기반 이상 탐지, 자동 복구 메커니즘, 공급망 단위 복원력 평가, 중소기업 대상 성숙도 모델과 체크리스트 개발 등을 결합하면서 복원력을 '기술 기능'이 아닌 '거버넌스 기반 운영역량'으로 확장하고 있다. 이러한 접근은 ESG 공시에서 요구하는 운영 안정성, 리스크 관리 체계, 지배구조의 책임성 요구와 직접적으로 연결된다.

의사결정 방법론 측면에서는 AHP(Analytic Hierarchy Process)가 ESG, 정보보안, DR과 같이 다기준·정성적 판단이 요구되는 영역에서 대표적인 분석 도구로 활용되어 왔다. Saaty(1980)는 AHP를 통해 복잡한 의사결정 문제를 계층 구조로 분해하고 전문가 판단을 쌍대비교 방식으로 정량화할 수 있음을 제시하였다. 국내에서도 고길곤 외 (2008), 이홍재 외 (2017)은 정책 및 위험관리 영역에서 AHP가 이해관계자 판단을 구조화하고 논리적 일관성을 검증하며 자원 배분 우선순위를 도출하는 데 효과적임을 입증하였다. 최근 연구들은 ESG 실행요인 도출, 정보보호 투자 항목 선정, DR 전략 대안 평가 등에 AHP를 적용함으로써 보안·DR 영역에서도 전략적 의사결정 도구로서의 활용 가능성을 확장하고 있다.

종합하면, [표 2-5] ESG 경영 관련 선행 연구들은 ESG 지배구조(G) 영역에서 정보보안과 DR이 핵심 관리 요소로 부상하고 있음을 공통적으로 보여주며 특히 중소·중견 기업 환경에서는 기술 도입 이전에 거버넌스 기반의 구조화와 우선순위 설정이 중요함을 시사한다.

그러나 기존 연구들은 개별 요소 분석이나 제도·개념 논의에 머무는 경우가 많아 중소기업이 제한된 자원 하에서 무엇부터 구축해야 하는지에 대한 통합적 우선순위 모델은 충분히 제시되지 못하였다.

이러한 연구 흐름은 본 연구가 AHP를 활용하여 중소·중견 기업의 보안·DR 구성요소 우선순위를 도출하고 이를 ESG 공시 및 거버넌스 체계와 연계 가능한 실행 프레임워크로 제시하고자 하는 연구 목적과 이론적·실증적 측면에서 긴밀히 연결된다.

[표 2-5] ESG 경영 관련 선행연구 (연구자 재구성, 2025)

연구자 (연도)	연구주제	연구방법	연구결과	주제어
Clark et al. (2015)	지속가능성 공시와 기업 전략	문헌·정책 분석	ESG가 투자·경영 전략 핵심 요소로 이동	ESG
Eccles & Klimenko (2019)	The Investor Revolution	문헌고찰 (SLR)	ESG가 투자·경영 전략의 핵심 프레임으로 이동	ESG, Governance
송지현 (2020)	정보보안과 지속가능성	문헌연구	ESG와 보안의 구조적 연계성 제시	ESG
ENISA (2021)	Cybersecurity for SMEs	정책·보고서 분석	ESG 맥락에서 SME 사이버리스크 관리 중요성	ESG, Cybersecurity
신유진 (2021)	ESG 공시체계 변화와 정보보호 요소	문헌·제도 분석	ESG 공시에서 정보보안·거버넌스 요소 확대	ESG
박지훈 외 (2022)	ESG 공시 확대와 지배구조 리스크	문헌·정책 분석	ESG 공시 강화 → 내부통제·리스크관리 중요	ESG, Governance
김상훈 외 (2022)	중소기업 ESG 대응전략	사례·정책 분석	중소기업 ESG는 거버넌스 체계가 핵심	ESG
오영균 (2022)	K-ESG 거버넌스 한계	제도 분석	국내 ESG는 거버넌스·리스크 정량성 부족	ESG
Li & Wu (2022)	Cyber risk와 ESG 성과	실증분석	사이버리스크가 ESG 성과에 유의미	ESG, Risk
문상일 (2023)	ESG 공시제도 개선	법·제도 분석	ESG 공시에서 리스크·통제 체계 강화 필요	ESG
최미화 (2023)	지배구조 특성과 ESG 공시 품질	실증분석	지배구조 수준이 ESG 공시 품질에 유의미	ESG, Governance
Tsang et al. (2023)	ESG disclosure review	문헌고찰	ESG 공시가 리스크·지배구조 중심으로 진화	ESG, Governance
Deloitte (2024)	CSRD assurance-ready	실무 리포트	ESG 공시는 내부통제·데이터 거버넌스 필수	ESG, CSRD
Suttipun et al. (2025)	ESG disclosures & market	실증분석	ESG 공시가 기업가치·시장반응과 연계	ESG

ESG 경영에 관한 선행연구는 지속가능성 담론을 넘어, 최근에는 공시·내부통제·리스크 관리 중심의 거버넌스 기반 경영 체계로 확장되는 흐름을 보이고 있다. 글로벌 규제(CSRD, ISSB) 강화와 투자자 정보 요구의 증대에 따라

ESG는 자율적 사회책임 차원을 넘어 기업가치와 위험 노출 구조를 좌우하는 전략 영역으로 전환되고 있다.

Clark et al.(2015)과 Eccles & Klimenko(2019)는 ESG가 기업 전략과 투자 판단의 핵심 프레임으로 이동하고 있음을 제시하며, ESG 공시가 경영 관리체계 전반을 규정하는 요소로 변화하고 있음을 강조하였다. 이는 이후 ESG 연구가 환경·사회 성과 중심에서 지배구조와 통제 체계 중심으로 확장되는 이론적 기반이 되었다.

국내에서는 ESG와 정보보안·거버넌스의 연계를 다룬 연구가 나타나며, ESG 공시가 운영 신뢰성과 위험관리 영역으로 확장되고 있음을 보여준다(송지현, 2020; 신유진, 2021). ENISA(2021)는 중소기업 환경에서 사이버 리스크 관리가 지속가능성의 핵심 요소임을 강조하며, ESG 의제에 디지털 리스크가 편입되는 흐름을 제시하였다.

2022년 이후 연구들은 ESG 공시 확대가 내부통제 및 거버넌스 체계 강화를 요구하고 있음을 공통적으로 지적한다(박지훈 외, 2022; 김상훈 외, 2022). 오영균(2022)은 K-ESG 체계의 정량성·통제 구조 한계를 지적하며, 국내 ESG 거버넌스의 구조적 보완 필요성을 제기하였다. Li & Wu(2022)는 사이버 리스크가 ESG 성과에 유의미한 영향을 미침을 실증하여, 정보보안이 ESG의 핵심 리스크 요인임을 제시하였다.

최근 연구들은 ESG 공시 품질과 지배구조의 관계를 검증하며, 공시의 핵심이 '공개'가 아니라 통제 체계와 데이터 신뢰성에 있음을 강조한다(문상일, 2023; 최미화, 2023; Tsang et al., 2023). Deloitte(2024)는 CSRD 대응에서 ESG 내부통제와 데이터 거버넌스 구축 필요성을 제시하였으며, Suttipun et al.(2025)은 ESG 공시가 시장 반응과 연결됨을 실증하였다.

종합하면, [표 2-6] 정보보안 관련 선행연구는 ESG 경영 연구가 ESG의 전략 프레임으로 이동하고 거버넌스·통제 중심 구조로 진화하며 정보보안·사이버 리스크가 핵심 요소로 편입되는 흐름을 보여준다. 그러나 국내에서는 제조기업 관점의 실행 가능한 거버넌스 모델 연구가 제한적이다. 본 연구는 이러한 공백을 전제로 ESG 지배구조 관점에서 정보보안 및 DR 요소를 구조화하고 AHP 기반 중요도 분석을 통해 실질적 우선순위를 도출하고자 한다.

[표 2-6] 정보보안 관련 선행연구 (연구자 재구성, 2025)

연구자 (연도)	연구주제	연구방법	연구결과	주제어
여상수 외 (2009)	중소기업 정보시스템 안정성	사례분석	운영 관리가 보안 성숙도 좌우	Security
김현주 외 (2013)	BCP 기반 재해복구시스템	프레임워크 설계	보안·연속성 통합 필요	Security
박은주 외 (2017)	STRIDE 기반 스마트팩토리 보안	위협모델링	제조환경 특화 보안 요구 도출	Security, Smart Factory
김일용 외 (2018)	산업제어시스템 보안 모델	구조 분석	OT 환경 보안 통합 필요	ICS, Security
김윤경 (2021)	중소기업 보안 거버넌스	문헌·사례	중소기업 보안은 거버넌스 부재	Security, Governance
이정민 외 (2021)	공급망 보안 관리	문헌·사례	협력사 보안이 핵심 리스크	Security
Calder (2021)	Cybersecurity governance	실무 프레임	보안은 이사회 통제 영역	Security, Governance
안재훈 외 (2023)	스마트공장 OT 보안	문헌·정책 분석	제조보안은 운영·거버넌스 문제	OT Security
Gartner (2023)	Cybersecurity as sustainability	리포트	보안은 ESG 기반 인프라	Cybersecurity
손영우 외 (2024)	공급망 보안 위협	사례·정책	협력사 보안이 핵심 리스크	Supply Chain, Security

정보보안 연구는 전통적으로 네트워크·시스템 보호 중심에서 발전해 왔으나 최근에는 거버넌스·운영 관리·공급망·지속가능성 영역으로 빠르게 확장되고 있다. 여상수 외 (2009)은 중소기업 보안 수준이 기술보다 운영 관리 구조에 의해 좌우됨을 지적하였으며 이후 제조·스마트공장 환경으로 연구 범위가 확대되었다(박은주 외, 2017; 김일용 외, 2018).

2020년 이후 연구들은 보안을 명확히 '경영 통제 문제'로 재정의한다. 김윤경(2021)과 Calder(2021)는 보안 실패 원인을 기술 부족이 아닌 책임 구조·의사결정·조직 거버넌스 부재로 분석하였다. 또한 공급망 환경이 복잡해지면서 보안은 개별 기업 문제가 아니라 ESG·공급망 리스크의 핵심 요소로 인식되고 있다(이정민 외, 2021; 손영우 외, 2024).

특히 스마트공장·OT 보안 연구는 보안 사고가 곧 생산 중단, 안전 문제, ESG 리스크로 직결됨을 강조한다(안재훈 외, 2023). Gartner(2023)는 사이버 보안을 지속가능 경영의 필수 인프라로 규정한다.

이는 정보보안이 IT 하위 기능을 넘어 ESG 거버넌스 하의 핵심 통제 요소로 재배치되어야 함을 시사하며 본 연구의 통합 프레임 필요성을 뒷받침한다.

[표 2-7] 재해복구(DR)·BCP 관련 선행연구 (연구자 재구성, 2025)

연구자 (연도)	연구주제	연구방법	연구결과	주제어
김현주 외 (2013)	BCP 기반 DR 설계	시스템 설계	DR·연속성 통합 필요	DR, BCP
박유림 외 (2017)	ISMS-DR 통합	프레임 비교	DR은 보안 거버넌스 요소	DR, ISMS
NIST (2016)	Cyber recovery	가이드라인	복구는 경영 통제 프로세스	DR
ISO22301 (2019)	Business continuity	국제표준	연속성은 조직 관리체계	BCP
Xu & Zhang (2021)	DR 역량과 성과	실증분석	복구역량이 성과에 영향	DR
김태훈 (2022)	DR 역량과 경영성과	실증분석	DR 성숙도가 경쟁력 변수	DR

[표 2-7] 재해복구(DR)·BCP 관련 선행연구는 초기에는 시스템 백업·복구 중심이었으나 최근에는 기업 성과, 거버넌스, 복원력(resilience) 개념과 직접 연결되고 있다. 김현주 외(2013)와 박유림 외(2017)는 재해복구가 개별 기술 체계가 아니라 ISMS·운영관리·거버넌스의 하위 구조로 통합되어야 함을 제시하였다.

NIST(2016)와 ISO 22301은 복구와 연속성을 공통적으로 경영진 책임 하의 관리 체계로 규정하며 훈련·검증·의사결정 구조까지 포함하는 프레임을 제시한다. Xu & Zhang(2021), 김태훈(2022)은 DR 역량이 기업 성과에 실증적 영향을 미친다는 점을 검증함으로써 DR을 경영 역량 변수로 전환시켰다.

이러한 연구 흐름은 재해복구가 IT 복구 차원을 넘어 기업의 회복탄력성과 ESG 신뢰성을 좌우하는 핵심 요소임을 보여준다. 이는 본 연구가 DR을 ESG 지배구조 하위 지표로 통합하려는 시도의 핵심 이론 근거가 된다.

[표 2-8] AHP 관련 선행연구 (연구자 재구성, 2025)

연구자 (연도)	연구주제	연구방법	연구결과	주제어
Saaty (1980)	AHP 이론	AHP 개발	다기준 의사결정 체계화	AHP
김성철·어하준 (1994)	전문가 종합	AHP	다수 전문가 통합 가능	AHP
민재형 (1996)	AHP 평가	AHP	정책·경영 평가 적합	AHP
고길곤·하혜영 (2008)	정책 AHP 활용	AHP	복합 의사결정 구조화	AHP
성기훈 외 (2010)	보안 위협 중요도	AHP	보안 요소 우선순위 도출	AHP, Security
엄진욱 외 (2023)	AHP 민감도 분석	AHP	결과 신뢰성 검증	AHP
Vinogradova-Zinkevič(2023)	Fuzzy AHP	Fuzzy-AHP	불확실성 반영 가능	AHP
박진선 외 (2024)	일관성 개선	AHP	결과 신뢰도 향상	AHP

[표 2-8] AHP 관련 선행연구는 복합적·비정형적 의사결정 문제에서 전문가 판단을 구조화하고 우선순위를 정량화하는 대표적 방법론으로 자리 잡아 왔다(Saaty, 1980). 국내에서는 김성철 외, (1994), 민재형 (1996) 이후 정책·경영·기술 분야 전반에 확산되었다.

보안·리스크 영역에서는 성기훈 외(2010)가 AHP를 활용하여 위협요인 중요도를 정량화함으로써 보안 분야에서의 적용 가능성을 입증하였다. 최근 연구들은 일관성 관리, 민감도 분석, Fuzzy-AHP 등으로 확장되며 전문가 판단 기반 평가의 신뢰성 강화에 초점을 두고 있다(엄진욱 외, 2023; Vinogradova-Zinkevič, 2023; 박진선 외, 2024).

이는 ESG, 보안, DR처럼 지표 간 상호의존성이 강하고 정량화가 어려운 영역에서 AHP가 가장 적합한 방법론임을 시사하며 본 연구의 방법론적 정당성을 뒷받침한다.

2.5.2 기존 연구 종합 및 문제점 도출

선행 연구들을 종합적으로 검토한 결과, ESG 경영, 정보보안·재해복구(DR), 그리고 의사결정 방법론은 각각의 연구 영역에서 일정 수준의 이론적·실무적으로 이루어졌으나 이들 선행 연구 요소들에 대하여 중소·중견 기업 관점에서 종합적으로 연결한 연구는 여전히 제한적임을 확인할 수 있었다.

첫번째로, ESG 지배구조(G) 영역의 확장에 대한 연구 축적은 충분하나 정보보안·DR과의 구조적 연결은 부분적 수준에 머물러 있음을 확인하였으며 특히, Clark et al.(2015), Eccles & Klimenko(2019). ESG가 투자와 경영전략의 핵심 기준으로 전환되고 있음을 제시하였고 최미화(2023). 송유정 외(2024)는 지배구조 요인이 ESG 공시 품질과 사이버보안 공시에 유의미한 영향을 미친다는 점을 실증적으로 제시하고 있다. 또한 ISSB(2023), CSRD/ESRS(2024)는 정보보안, 데이터 신뢰성, 내부통제를 지배구조 공시의 필수 요소로 제도화 하였다.

그러나 이러한 연구와 제도는 보안·DR이 '중요하다'고 규정하는 수준에 머무를 뿐 실제 중소·중견 기업이 어떤 보안과 DR 요소부터 우선적으로 구축해야 하는지에 대한 구체적 우선순위 체계나 실행할 수 있는 기준에 대해서는 제시하지 못하고 있다.

둘째, 중소·중견 기업의 보안과 DR 취약성에 대한 실태 분석은 풍부하지만 개선 전략은 선언적 수준에 머물러 있다.

여상수 외(2009), KISA(2018, 2023, 2024)는 중소·중견 기업이 전담 인력 부족과 예산의 비효율적 편성과 문서화 및 직원의 훈련 부재로 인해 구조적 취약성을 가진다는 점을 반복적으로 지적하였다. ENISA(2021)와 UNGC 역시 중소·중견 기업의 낮은 보안과 복원력 수준이 공급망 전체의 ESG 리스크로 연결될 수 있음을 경고하였다. Chen et al.(2023)은 백업·복구 실패의 핵심 원인이 기술보다 거버넌스와 관리 프로세스 부재와 무관심에 있음을 정량적으로 입증하였다. 그럼에도 불구하고 대부분의 연구는 '중소·중견 기업은 취약하다'는 진단에 머물며 제한된 정보보안 자원을 가진 중소·중견 기업이 무엇을 먼저 준비해야 하는지에 대한 내용을 선택하여야 하는지에 대한 의사결

정 지원 도구는 제시하지 못하고 있다.

셋째, 정보보안·DR 프레임워크는 고도화 되어 있으나 중소·중견 기업 적용성에는 한계가 존재한다. NIST CSF, NIST SP 800-34, ISO/IEC 27001, ISO 22301 등은 보안·DR·업무연속성을 체계적으로 설명하는 표준을 제공하고 있으며 특히 Recover 단계와 BIA 기반 DR 절차는 ESG 공시의 지속운영 연속성 요구와 직접적으로 연결된다고 볼 수 있다. 그러나 이들 프레임워크는 대기업 또는 공공기관 중심으로 설계되어 중소·중견 기업이 전면 도입하기에는 비용과 인력부족 운영비용 부담이 크다. PDRF & MSME(2023)가 최소요건 중심의 가이드를 제시했음에도 구성요소 간 상대적 중요도를 판단할 수 있는 체계는 여전히 부족하다고 분석하고 있다.

넷째, 사이버 복원력(Cyber Resilience)은 ESG와 보안·DR을 연결하는 유의미한 개념이나 실증적 우선순위 모델은 제한적이다. Carias et al.(2020)가 제시한 Prevent－Withstand－Recover 3단계 구조는 사고 전반, 중반, 후반부를 포괄하는 통합적 관점을 제공하며 최근 연구들은 AI 기반 이상 탐지, 자동 복구, 공급망 단위 평가, 중소·중견 기업 성숙도 체크 리스트로 확장되고 있다.

그러나 복원력 연구 역시 개념적 프레임이나 사례 중심 논의가 주를 이루며 ESG 공시와 연계된 정량적 우선순위 도출 모델은 충분히 제시되지 못하고 있다.

다섯째, AHP 방법론은 보안과 DR체계와 ESG 평가에 적합함에도 이 세 영역을 통합 적용한 연구는 드물다. Saaty(1980, 1987, 1990). AHP 이론은 다양한 기준과 정성적 판단을 매뉴얼화 하는데 적합하며, 고길곤 외(2008), Ishizaka & Labib(2011). AHP 설계와 일관성 및 민감도 분석의 중요성을 체계적으로 정리하였다Chen et al.(2023). AHP를 활용해 중소·중견 기업(SME) 백업 요소의 중요도를 도출함으로써 실무적 가능성을 보여주었다. 그럼에도 기존 연구들은 보안과 DR 및 ESG를 각각의 평가 대상으로 다루는 경우가 대부분이며 ESG 공시 요구를 반영한 보안과 DR을 통합하여 연구한 우선순위 모델로 확장한 연구는 제한적이다.

이상의 선행연구를 종합하면 다음과 같은 연구 공백이 도출된다. ESG 지

배구조(G)에서 정보보안과 DR의 중요성은 제도적으로 강조되나 실행 우선순위를 제시하는 정량적 모델이 부재하며 중소·중견 기업 보안과 DR 취약성은 충분히 진단되었으나 중소·중견 기업의 제한된 자원 환경에서의 선택 기준이 제시되지 않았다고 볼 수 있다. 기존 보안과 DR 표준은 포괄적이나 중소·중견 기업 맞춤형 우선순위 설계 도구로 활용하기 어렵고 사이버 복원력 개념은 확산되고 있으나 ESG 공시와 직접 연계된 실증적 의사결정 모델이 부족하다고 볼 수 있다. AHP는 적합한 방법론임에도 ESG과점, 보안관점, DR관점을 종합한 적용 연구가 미흡하다.

따라서 본 연구는 이러한 한계를 보완하고자 ESG 지배구조 요구를 반영한 보안과 DR 구성요소를 체계화하고 AHP를 활용하여 중소·중견 기업 환경에 적합한 우선순위 모델을 제시한다는 점에서 기존 연구와 차별성을 가진다. 이는 ESG 공시 신뢰성 확보와 실제 업무에 적용하기 위한 실행 가능성을 동시에 충족하는 분석 틀을 제공한다는 점에서 학술적·실무적 의의를 갖는다.

Ⅲ. 연구방법 및 연구설계

3.1 연구모형 및 연구절차

본 연구는 제조 현장에서 디지털 전환(DX)이 일상화되면서 정보보안과 재해복구(DR)/업무연속성(BCP)이 더 이상 분리된 기술 과제가 아니라, 거버넌스 기반의 운영관리 체계로 결합되고 있다는 문제의식에서 출발하였다. 특히 ESG 공시·평가가 “정책 보유 여부”를 넘어 “리스크를 어떻게 관리하고 사고 시 어떻게 복원하는가”를 묻는 방향으로 이동하면서 중소·중견 ·중견 제조기업에는 보안과 복구를 함께 설계·운영할 수 있는 실행 가능한 모델이 요구된다. 이러한 흐름은 ENISA가 중소·중견 기업 대상 사이버보안 권고를 실행 가능한 단계로 제시한 점에서 확인되며(ENISA, 2021), NIST 또한 CSF 2.0에서 Govern 기능을 명시적으로 추가하고 Recover를 포함해 사이버리스크 관리의 생애주기를 구조화한 데서 뚜렷하게 드러난다(NIST, 2024).

[표 3-1] 연구절차 및 단계 (연구자 재구성, 2025)

단계	주요 내용	산출물
연구기반 정립	• 국제 보안·연속성 표준·가이드 및 국내 ESG 지표 분석, 중소·중견 기업 보안·DR 취약성 선행연구 검토, 스마트공장/ESG 컨설팅 현장 사례 정리	• 문헌·기준 비교표, 취약 패턴 목록, ESG－보안－DR 연계 개념도, 평가요소 후보 Pool
평가요소 도출·정제	• 평가요소 후보를 기준(Criteria)·세부지표(Sub-criteria)로 분류, 중복·누락·용어 정의 정리, 측정 가능성/현장 적용성 검토	• 평가요소 목록(초안/확정안), 지표 정의서(운영적 정의), 분류체계 표
AHP 모형 설계	• 연구목표(Goal) 확정, Goal－Criteria－Sub-criteria 계층구조 설계, 설문 문항(쌍대비교) 구성	• AHP 계층도(도 3-1), AHP 설문지(예비/본), 기준·세부지표 설명서
표본·데이터 수집	• 전문가 패널 구성(분야 균형), 예비설문을 통한 문항 정제, 본 설문(온라인/오프라인) 수행	• 표본 구성표(표 3-3), 설문 데이터셋, 예비설문 수정 로그
AHP 분석·검증 및 모델화	• 쌍대비교 행렬 구축, 고유벡터 기반 가중치 산출, 일관성(CR) 검증 및 데이터 정제, (필요 시) 민감도 점검, 결과의 로드맵/지표화	• 기준·세부지표 가중치표, CR 검증 결과, 우선순위 도출 결과, 실행 로드맵(안), ESG 연계 지표(KPI) 모델(안)

본 연구의 [표 3-1] 연구절차 및 단계는 (1)국제 표준·가이드 및 국내 ESG 지표를 기반으로 평가 요소 후보군을 도출, (2)스마트공장 구축·운영 및 취약성 점검 현장에서 반복 관찰되는 취약 패턴을 반영해 요소를 정제, (3)AHP 계층구조(Goal – Criteria – Sub-criteria)를 설계, (4)전문가 설문을 통해 가중치(우선순위)를 산출하며 일관성(CR) 검증으로 신뢰도를 확보, (5)최종적으로 우선순위를 실행 로드맵과 ESG 연계 지표(안)로 변환하는 단계로 구성하였다. DR/BCP의 설계·운영 관점은 NIST SP 800-34(Rev.1)의 컨틴전시 계획 구조와 프로세스를 참고하였고(NIST, 2010), 정보보호 관리체계의 기본 틀은 ISO/IEC 27001:2022의 위험기반 접근을 준용하였다(ISO, 2022).

3.2 평가요소 도출 및 분류체계 확정

3.2.1 연구대상 및 자료수집

연구대상은 제조업 기반 중소·중견 기업의 운영 현실을 이해하는 이해관계자 집단으로 구성하였다. 구체적으로는 ①제조기업 IT/보안 담당자, ② DR/BCP 운영 경험자, ③스마트공장 구축 컨설턴트(OT/설비 네트워크 포함), ④ESG 평가·보고 실무자(지배구조 지표 이해)를 포함한다.
자료수집은 ①문헌자료(국제 표준·가이드, 국내 정책·가이드, 학술연구), ②현장자료(스마트공장 구축/운영, 취약성 진단/개선, 장애·복구 대응 과정에서 축적된 산출물), ③전문가 의견(AHP 설문 및 보완 인터뷰)로 구성하였다.

중소·중견 기업 보안·DR 취약성은 종종 “기술의 부재”로 설명되지만 실제로는 전담 인력과 예산 그리고 책임 체계의 결여 등 운영·거버넌스의 구조적 제약이 리스크를 증폭시키는 양상으로 반복된다. 예컨대 KISA의 지역 중소·중견 ·벤처기업 실태조사에서는 정보보호 전담인력 보유 비율이 낮고(전담인력 부재/불명확 응답이 다수) 최근 수년간 랜섬웨어 등 침해사고 경험도 확인되어 운영 역량 격차가 구조적 문제로 제시된다(KISA, 2023). 또한 국회입법조사처 보고서는 기업 규모별 정보보호 정책·조직 보유율 격차와 지원정책 과제를 정리하며 중소·중견 기업 보안 역량 강화가 “투자 유인·제도·지원체계”

차원에서 다뤄져야 함을 강조한다(국회입법조사처, 2023; 2025).

3.2.2 분류체계 정의

본 연구는 전통적인 독립·종속변수의 인과모형을 직접 추정하기보다 ESG 지배구조(G)의 관리 요구를 보안·DR 운영요소로 연결하는 매핑(mapping) 방식으로 분류체계를 구성하였다. 이는 AHP가 통계적 인과추정보다 복합 의사결정 상황에서 상대적 중요도(우선순위)를 합의적으로 도출하는 데 강점을 갖기 때문이다(Saaty, 1980; 2008). 그리고 ESG경영의 거버넌스(G) 관점에서는 K-ESG 가이드라인에서 제공되는 내부통제·리스크관리·투명성·공급망 관리 등은 K-ESG 가이드라인의 진단항목 구조를 참고하여 구성하였다(산업통상자원부, 2021). 보안·DR 측면에서는 정보보호 관리체계(ISO/IEC 27001:2022)의 위험기반 관리 접근과(ISO, 2022) 업무연속성 관리체계(ISO 22301:2019)의 계획-운영-점검-개선 프레임을 실무형 지표로 번역하는 방식으로 분류체계를 정교화하였다(ISO, 2019).

본 연구는 보안 거버넌스(역할·책임, 정책, 의사결정), 기술적 통제(접근권한, 패치, 로그/모니터링), DR/복구역량(백업, 복구절차, 테스트), 교육·인식(정기 교육, 훈련), 문서화·운영관리(표준절차, 변경관리)를 기본 축으로 설정하였다. [표 3-2] 연구변수 정의는 ESG 구성요소 및 보안·DR 성숙도로 구분된다.

[표 3-2] 연구변수 정의 (IFRS Foundation, 2023; NIST Cybersecurity framework (CSF) 2.0, 2024; 연구자 재구성, 2025)

변수 구분	요소	세부 지표
ESG 구성요소	내부통제	역할·책임 구분, 정책 문서화
	리스크 관리	개인정보·시스템 보호, 사고대응 절차
	공급망 관리	협력사 보안 점검, 파일공유 관리
보안·DR 성숙도	보안 거버넌스	CISO 역할, 조직 내 책임체계
	DR 체계	복구절차, 백업주기, DR 테스트
	기술적 통제	접근권한, 패치관리, 로그관리
	교육 및 인식	정기 교육 여부, 실습 기반 교육

3.2.3 설문지 작성 및 예비설문

본 연구의 설문지는 AHP의 쌍대비교(pairwise comparison) 절차에 따라 기준(Criteria)과 세부지표(Sub-criteria) 간 상대적 중요도를 평가할 수 있도록 설계하였다(Saaty, 1980, 2008). 설문 설계의 핵심은 “현장 적용 가능한 우선순위 도출”에 있었기 때문에 문항의 명확성(clarity), 비편향성(non-bias), 응답 부담(response burden)을 동시에 고려하였다. [표 3-3] AHP 설문 구성은 10가지 항목으로 구성되고 내용은 다음 [표 3-3]과 같다.

[표 3-3] AHP 설문 구성 요약 (연구자 재구성, 2025)

구분	항목	주요 내용	비고
1	설문 목적	• ESG 관점에서 중소·중견 기업 보안·DR 구성요소의 상대적 중요도(우선순위) 도출	• 결과는 4장 실행모델(로드맵·지표) 설계의 입력값으로 활용
2	기준(Criteria) 수	• 5개(C1~C5): 보안 거버넌스 / 기술 통제 / DR·복구역량 / 정책·문서화·운영관리 / 교육·인식·훈련	• 기준 정의서(운영적 정의)와 함께 제시하여 해석 편차 최소화
3	세부지표(Sub-criteria) 수	• 15개 내외(기준별 3개 수준): 예) 접근권한, 패치관리, 로그관리, 백업주기, DR 테스트 등	• 기준별 3개 내외로 설계해 문항 수와 피로도 관리(필요 시 부록 확장)
4	비교 블록 구성	• 블록 A: Criteria 간 쌍대비교 / 블록 B: 각 기준(Ci) 내 Sub-criteria 간 쌍대비교	• 동일 상위 기준 내 비교 원칙 준수(계층별 비교)
5	총 문항수(쌍대비교)	• 기준 비교 10문항(5×4/2) + 세부지표 비교 15문항(기준별 3문항×5) = 총 25문항	• 문항 수 산정식 n(n−1)/2 적용, 설문지에 문항 수·소요시간 안내
6	척도(Scale)	• Saaty 1~9 척도(2·4·6·8 중간값 포함), 숫자 의미(동일~절대적 중요) 안내	• 응답자 간 척도 해석 차이를 줄이기 위해 앵커(예시 문구) 제공
7	예상 소요시간	• 15~25분(온라인 기준, 모바일 응답 시 다소 증가 가능)	• 응답 중단 방지를 위해 진행률 표시/저장/재개 옵션 권장
8	예비설문(Pre-test)	• 분야별 전문가 3~5인 대상: 용어 오해, 중복 문항, 비교 가능성, 설문 길이(피로도) 점검	• 예비설문 결과로 문항/정의 수정 → 최종본 확정(수정 로그 관리)
9	예비설문 수정내역(요약)	• ① 용어 명확화(OT/IT 병기, 운영적 정의 추가) ② 중복 항목 통합 ③ 비교 난이도 조정(상위/하위 재배치) ④ 설문 길이 최적화(기준별 3개 내외 유지)	• 변경 이력(Change log): 삭제/통합/재정의 항목 기록(재현성 확보)
10	응답 품질 관리 및 산출물	• CR 검증 기반 정제: CR 기준 초과 응답 재확인 또는 제외 → 최종 가중치 산출	• 산출물: 설문 데이터셋, CR 결과표, 기준·세부지표 가중치표, 종합 우선순위 결과

기준(Criteria)은 5개로 고정하고 세부지표(Sub-criteria)는 기준별 3개 내외로 제한하여 총 문항 수가 과도해지지 않도록 조정하였다. 이는 AHP 응답 품질이 설문 피로도와 직결된다는 경험적 관찰을 반영한 것이다. 다음으로 각 항목에는 운영적 정의(operational definition)를 부여하여 IT/OT, 보안/ESG 등 응답자 배경이 달라도 동일한 개념을 떠올릴 수 있도록 정리하였다. 마지막으로 예비설문(pre-test)은 분야별 전문가 3~5인을 대상으로 수행하여 용어 오해 가능성, 중복 항목, 비교 난이도가 높은 항목, 설문 길이로 인한 응답 부담을 점검한 뒤 최종안을 확정하였다. 이 과정에서 삭제·통합·재정의된 항목은 변경이력(change log)으로 남겨 연구 재현성을 확보하였다.`

3.3 AHP 계층구조 설계

본 연구의 분석 설계는 AHP 기반 의사결정 실험의 절차로 구성하였다. 즉 (1)계층 구조 설정, (2)쌍대비교 행렬 작성, (3)고유벡터(Eigenvector) 기반 가중치 산출, (4)일관성비율(CR) 검증, (5)가중치 확정 및 우선순위 도출의 순서로 수행하였다(Saaty, 2008). 또한 AHP 결과를 실행모델로 연결하기 위해 우선순위 결과가 실제로는 어떤 실행 과제로 번역되는지(예: 단기/중기/장기 로드맵, ESG 연계 KPI 항목)에 대하여 후속 장에서 제시할 수 있도록 산출물 구조를 함께 설계하였다.

본 연구의 실험설계는 AHP(Analytic Hierarchy Process)의 의사결정 실험 절차를 분석 프로토콜로 정의한 것으로 전문가의 상대적 판단을 쌍대비교 행렬(pairwise comparison matrix)로 구조화하고 이를 우선순위 벡터(priority vector)로 변환하는 일련의 계산 흐름으로 구성된다. 계층구조는 목표(Goal) – 기준(Criteria) – 세부지표(Sub-criteria) 3단으로 고정하며 각 계층에서 동일 수준 요소 간 비교만 수행하는 수준별 비교(level-wise comparison) 원칙을 적용하였다.

먼저 기준 계층에서 기준 수를 $nC = 5$ 라 할 때, 기준 쌍대비교 문항 수는 조합식은 다음과 같다.

$$m_C = \binom{n_C}{2} = \frac{n_C(n_C-1)}{2} = \frac{5 \cdot 4}{2} = 10$$

세부지표 계층은 각 기준 Ci 하위에 세부지표 수 nSi = 3 설계하므로 기준별 세부지표 비교 문항 수는 다음과 같다.

$$m_{S_i} = \binom{n_{S_i}}{2} = \frac{3 \cdot 2}{2} = 3$$

그리고 전체 세부지표 문항수는 다음과 같다.

$$m_S = \sum_{i=1}^{n_C} m_{S_i} = 5 \times 3 = 15$$

따라서 총 쌍대비교 문항 수는 다음과 같이 문항수가 산정된다.

$$m_{\text{total}} = m_C + m_S = 10 + 15 = 25$$

각 응답자는 문항별로 Saaty 1~9 척도에 따라 상대 중요도를 입력하도록 한며 이를 바탕으로 쌍대비교 행렬을 구성한다.

기준 비교행렬을 $A^{(C)} = [a_{ij}] \in \mathbb{R}^{n_C \times n_C}$라 하면

$a_{ii} = 1, \quad a_{ij} > 0, \quad a_{ji} = \frac{1}{a_{ij}}$ 의 역수성을 만족하도록 정의한다.

마찬가지로 기준 Ci 하위 세부지표 비교행렬을

$A^{(S_i)} = [s_{jk}^{(i)}] \in \mathbb{R}^{ns_i \times ns_i}$ 로 두고 동일한 역수성 조건을 적용한다.

또한 본 연구는 “현장 적용이 가능한 우선순위” 도출을 위해 각 비교 판단이 단순히 기술적 완성도만 반영되지 않도록 응답 지침에서 운영 지속성(operability), 사고 영향도(impact), 구축 난이도(feasibility), 규제·ESG 설명가능성(explainability)을 함께 고려하도록 설계하였다. 이는 후속 장에서 전역

가중치(global weight)를 실행 로드맵 및 ESG 연계 지표로 변환하는 모델 번역(model translation)의 정합성을 높이기 위한 방법이다.

마지막으로 데이터 품질 관리는 일관성 검증 규칙을 사전에 설정하여 수행한다. 각 응답의 비교행렬에 대해 λmax 를 추정하고 일관성지수(CI)와 일관성비율(CR)을 산출하여 기준을 초과하는 응답은 재확인 또는 제외하는 방식으로 정제한다.

[표 3-4] 산정식 표기 및 행렬 정의 요약 (연구자 재구성, 2025)

연번	기호	내용	정의
1	n_C	• 기준(Criteria) 개수	본 연구 nC = 5
2	n_{S_i}	• 기준 Ci 의 세부지표 개수	본 연구 nSi = 3
3	$A^{(C)} = [a_{ij}]$	• 기준 비교행렬	$\mathbb{R}^{n_C \times n_C}$, $a_{ji} = 1/$
4	$A^{(S_i)} = [s_{jk}^{(i)}]$	• 기준 Ci 하위 세부지표 비교행렬	$\mathbb{R}^{n_{S_i} \times n_{S_i}}$
5	$w^{(C)}$	• 기준 가중치 벡터	$\sum_i w_i^{(C)} = 1$
6	$w^{(S_i)}$	• 기준 Ci 하위 세부지표 지역가중치 벡터	$\sum_j w_j^{(S_i)} = 1$
7	$GW(S_{ij})$	• 세부지표 Sij 전역가중치	$GW = w_i^{(C)} \cdot w_j^{(S_i)}$

3.3.1 연구분석 방법

본 연구의 분석은 (1)응답으로부터 비교행렬을 구성, (2)우선순위 벡터를 산출, (3)일관성 검증으로 응답을 정제, (4)다수 전문가 판단을 집계, (5)전역가중치로 종합 우선순위를 도출하는 절차로 수행하였다.

3.3.1.1 우선순위 벡터 산출(고유값 해법 : Eigenvalue Method)

기준 비교행렬 $A(C)$에 대해 우선순위 벡터 $w(C)$는 다음의 고유방정식에서 주고유벡터(principal eigenvector)로 산출하면 다음과 같다.

$$A^{(C)}\, w^{(C)} = \lambda_{\max}^{(C)}\, w^{(C)}$$

여기서 $\lambda_{\max}^{(C)}$ 는 최대 고유값이며 $w^{(C)}$ 는 정규화하여 아래 수식을 만족하도록 한다.

$$w^{(C)} \leftarrow \frac{w^{(C)}}{\sum_{i=1}^{n_C} w_i^{(C)}}$$

각 기준 Ci 하위 세부지표 비교행렬 $A^{(S_i)}$에 대해

$$A^{(S_i)}\, w^{(S_i)} = \lambda_{\max}^{(S_i)}\, w^{(S_i)}, \qquad w^{(S_i)} \leftarrow \frac{w^{(S_i)}}{\sum_{j=1}^{n_{S_i}} w_j^{(S_i)}}$$

로 지역가중치(local weight)를 산출한다.

실제 측정시 고유값 해법 외에 기하평균 기반 근사도 사용 가능하지만 본 연구에서는 기본 해법으로 정합성 확보를 위해 고유값 해법을 사용하였다. 응답 집계 단계에서는 비율척도 특성을 고려해 기하평균을 함께 활용하였다.

3.3.1.2 일관성 검증 (CI, CR 산출)

각 비교 행렬의 논리적 일관성은 일관성 지수(CI)와 일관성 비율(CR)로 평가한다. 차원이 n인 행렬 A에 대해

$$CI = \frac{\lambda_{\max} - n}{n - 1}$$

이며, 무작위 일관성지수(Random Index) $RI(n)$를 사용하여

$$CR = \frac{CI}{RI(n)}$$

로 계산한다. 본 연구는 기본 기준으로 $CR < 0.10$ 을 적용하고, 기준 초과 응답은 (i) 비교 쌍 재확인(recheck) 또는 (ii) 제외(exclusion)의 규칙에 따라 데이터 정제를 수행하였다.

3.3.1.3 다수 전문가 판단의 집계 (AIJ, AIP)

전문가가 K명일 때, 개인 k의 비교행렬을 $A_k = [a_{ij}^{(k)}]$라 하자. 집계 방

식은 두 가지가 대표적이다.

우선 판단의 집계 방식(AIJ : Aggregation of Individual Judgments)은 비율척도에서 곱셈적 구조를 유지하기 위해 비교행렬 요소를 기하평균으로 집계한다.

$$\bar{a}_{ij} = \left(\prod_{k=1}^{K} a_{ij}^{(k)} \right)^{1/K}$$

이로부터 집계행렬 $\bar{A} = [\bar{a}_{ij}]$을 구성하고 동일하게 고유값 해법으로 $\bar{w}$를 산출한다.

$$\bar{A}\,\bar{w} = \bar{\lambda}_{\max}\,\bar{w}$$

본 연구는 비율척도·역수성 보존 측면에서 AIJ(기하평균 기반)을 기본으로 적용하고 AIP 결과와 비교하여 집계 방식에 따른 결과 변동을 점검한다.

3.3.1.4 전역 가중치(Global Weight) 및 종합 우선순위

기준 Ci 의 가중치를 $w_i^{(C)}$, 기준 Ci 하위 세부지표 Sij 의 지역가중치를 $w_j^{(S_i)}$라 하면 세부지표의 전역가중치는 계층적 곱으로 산출된다.

$$GW(S_{ij}) = w_i^{(C)} \times w_j^{(S_i)}$$

전역가중치 벡터 GW를 내림차순으로 정렬하면 보안·DR 구성요소에 대한 종합 우선순위를 얻을 수 있다.

$$\text{Priority Rank} = \text{sort\_desc}\,(\mathbf{GW})$$

3.3.1.5 데이터 정제 규칙(분석 재현성 확보)

응답자 k의 행렬이 $CRk \geq \tau$ (임계값 τ = 0.10)를 만족하면 다음 규칙을 적용한다.

$$CR_k \geq \tau \Rightarrow \begin{cases} \text{recheck}(k) \\ \text{exclude}(k) \end{cases}$$ (재확인/재응답 가능 시)
(재확인 불가 또는 반복 초과 시)

정제 후 최종 표본을 $\tilde{K}$로 두고, $\tilde{K}$에 대해서만 집계 및 최종 가중치를 확정한다.

[표 3-5] AHP 분석 산출물 및 수식 매핑(연구자 재구성, 2025)

단계	입력	내용	산출물
행렬 구성	쌍대비교 응답	$a_{ji} = 1/a_{ij},\ a_{ii} = 1$	$A^{(C)}, A^{(S_i)}$
가중치 산출	비교행렬	$Aw = \lambda_{\max} w$, 정규화	$w^{(C)}, w^{(S_i)}$
일관성 검증	λ max	$CI = \frac{\lambda_{\max} - n}{n-1},\ CR = CI/RI$	CR 결과표
집계(AIJ)	A_k	$\bar{a}_{ij} = \left(\prod a_{ij}^{(k)}\right)^{1/K}$	$\bar{A}, \bar{w}$
전역가중치	$w^{(C)}, w^{(S_i)}$	$GW = w_i^{(C)} \cdot w_j^{(S_i)}$	종합 우선순위

본 연구는 기준 비교행렬 $A^{(C)}$및 기준별 세부지표 비교행렬 $A^{(S_i)}$을 구성한 후 주고유벡터 w를 통해 가중치를 산출하고 CR 검증을 통과한 응답만을 집계(AIJ)하여 전역가중치 $GW(Sij)$를 도출하였다.

[표 3-6] Random Index $RI(n)$ (연구자 재구성, 2025)

n	1	2	3	4	5	6	7	8	9	10	비고
$RI(n)$	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	

3.4 표본 선정 및 데이터 수집

본 절에서는 본 연구에서 활용된 표본의 구성 방식과 설문 데이터를 확보하기 위한 절차를 상세히 설명한다. AHP 기반 분석은 응답자의 전문성에 따라 결과의 신뢰성이 크게 달라지므로 표본 선정 과정에서 분야별 균형성과

실무경험을 동시에 고려하였다.

본 연구는 제조 중소·중견 ·중견기업의 ESG－보안－DR 연계 이슈를 현실적으로 반영하기 위해 판단표집(judgmental purposive sampling)과 할당 기반 이질적 패널 구성(quota-based heterogeneous panel)을 병행하여 표본을 설계하였다.

3.4.1 표본 선정기준

본 연구는 보안·DR 체계가 실제 제조기업 운영에서 어떠한 방식으로 작동하는지 그리고 ESG 지배구조(G) 요구(내부통제·리스크관리·공급망 등)와 어떻게 연결되는지를 검증하기 위해 다음 세 가지 기준으로 전문가를 선정하였다. ESG-G의 세부 진단 항목 구조는 K-ESG 가이드라인(내부통제, 리스크관리, 공급망 등)의 틀을 참조하였고(산업통상자원부, 2021) 보안·연속성 영역은 ISO/IEC 27001(ISO 27001, 2022) 및 ISO 22301(ISO 22301, 2019), NIST SP 800-34(NIST, 2010) 등 국제 기준에서 공통적으로 강조하는 관리·운영 관점을 준거로 삼았다.

3.4.1.1 전문성 기준

전문성 기준은 ‘평가요소에 대한 판단 가능성’(judgement capability)을 확보하기 위한 최소 요건으로 설정하였다. 첫 번째, IT 보안 및 OT/제조 설비 환경 보안 실무 경험, 두 번째, DR/BCP 기획·훈련·복구 운영 경험, 세 번째, ESG 평가 또는 K-ESG 기반 컨설팅·보고 실무 경험, 네 번째, 스마트공장 구축·전환(DX) 프로젝트 수행 경험을 포함한다. ENISA는 중소·중견 기업 대상 보안 권고를 “실행가능한 조치(actionable guidance)”로 제시하면서 보안이 기술 설치를 넘어 조직 운영 수준에서 단계적으로 내재화되어야 함을 강조한다(ENISA, 2021). 또한 NIST CSF 2.0은 GOVERN 기능을 포함하여 사이버 리스크를 ‘운영화(operationalizing risk management)’하는 체계를 제시함으로써 평가·우선순위 도출에서 거버넌스 관점의 중요성을 뒷받침한다(NIST, 2024).

3.4.1.2 현장 적용성 기준

본 연구의 목적은 “현장에서 실제로 작동 가능한 우선순위”를 도출하는 데 있으므로, 전문가 패널은 다음과 같은 현장 기반 역할군(role-based groups)으로 선정하였다. 첫 번째, 제조 중소·중견 ·중견기업의 IT/보안·인프라 운영 담당자 두 번째, DR/BCP 운영 또는 장애·복구 대응 경험자 세 번째, 스마트공장 컨설턴트/구축 엔지니어(설비 네트워크·OT 포함) 네 번째, ESG 전략 수립 및 보고·평가 실무자 다섯 번째, 관련 분야 연구자 등이다. 특히 국내 실태조사에서는 중소·중견 ·벤처기업의 정보보호 전담 인력 보유율 예산·운영 제약 등이 반복적으로 관찰되며 이는 기술 자체의 문제라기보다 운영 자원과 책임체계의 제약이 보안 성숙도를 좌우할 수 있음을 시사한다(KISA, 2023).

3.4.1.3 균형성 기준

AHP 결과의 편향을 줄이기 위해서 다음과 같은 조건을 기준을 선별하였다. 첫 번째, IT/OT 관점의 균형 두 번째, ①제조기업(수요자) ②컨설턴트/구축자(공급자) ③ESG 평가자(평가자) 간 균형 세 번째, 보안·DR·ESG 각 영역의 비중 균형을 표본 설계의 핵심 원칙으로 두었다. AHP 적용 연구에서는 통계적 대규모 표본보다 ‘전문가 집단의 합리적 규모’가 일반적이며 국내 AHP 연구에서는 10명 이상 ~ 20명 이내 수준의 전문가 패널로 가중치를 도출한 연구들이 대부분이다. 이에 본 연구는 20명의 유효한 전문가 패널을 구성하여 연구를 진행하였다.

3.4.2 데이터 수집 절차

연구의 신뢰성과 일관성을 확보하기 위해 다음의 4단계 절차를 통해 데이터 수집이 이루어졌다.

3.4.2.1 1단계 : 예비조사(Pre-survey) 및 문항 정제

예비조사는 용어 해석 차이, 문항 중복, 비교 난이도, 응답 피로도 등을 점

검하기 위한 절차로 분야별 전문가 5인을 대상으로 실시하였다. 특히 제조 환경에서는 IT/OT 용어가 혼재하고 ESG·보안·DR 개념의 적용 범위가 응답자 배경에 따라 달라질 수 있으므로 지표 정의서(operational definition)와 예시(anchor)를 보완하여 문항의 명확성을 높였다. ENISA 보고서가 지표·조치의 실무적 명료성을 강조한다는 점은 이러한 예비정제의 필요성을 뒷받침한다.

또한 예비조사 단계에서 비교 부담이 과도하다고 판단된 항목은 통합·삭제하여 전체 설문의 응답 소요 시간을 조정하였다.

3.4.2.2 2단계 : 본 조사(Main AHP survey)

본 설문은 온라인과 오프라인을 병행하였고 Saaty의 1~9 척도에 기반한 쌍대비교로 구성하였다(Saaty, 1980). 설문은 기준(Criteria) 5개과 기준별 세부지표(Sub-criteria) 3개(총 15개)로 계층화하여 동일 상위 기준 내에서만 비교가 이루어지도록 구성함으로써 비교 가능성을 확보하였다.
응답자는 각 쌍대비교 문항에 대해 직관적 판단이 가능하도록 간단한 설명 문구와 판단 예시를 함께 제공받았다.

3.4.2.3 3단계 : 데이터 정제 및 일관성 검증(Consistency screening)

응답별로 일관성비율(CR)을 산출하여 기준을 초과한 응답은 재확인(역질문/비교쌍 재점검)을 요청하고 반복적으로 기준을 충족하지 못하는 경우 분석에서 제외하였다. 국내 AHP 적용 연구에서도 비일관성 지수/비율 기준을 설정해 결과를 선별하는 절차가 보고된다.

3.4.2.4 4단계 : 최종 데이터 통합 및 가중치 산출 준비

최종적으로 일관성 기준을 충족한 응답만을 사용하여 집단 판단을 통합하고 기준과 세부지표 그리고 전체 요소의 상대적 중요도(가중치)를 도출하였다. 이 결과는 4장에서 제시하는 ESG 기반 보안·DR 실행모델(우선순위 로드맵 및 지표안) 설계의 핵심 입력값으로 활용된다. 또한 NIST CSF 2.0이 제시하는 GOVERN–RECOVER 등 기능 구조는 결과 해석에서 '통제의 강도' 뿐 아니라 '운영·복원 관점'을 함께 논리화하는 틀로 활용하였다.

이를 통해 분석 결과가 단순 순위 제시에 그치지 않고 단계별 투자·구축 전략 수립에 직접 연계될 수 있도록 연구 절차를 설계하였다.

3.4.3 표본 구성 요약표

아래 [표 3-7]은 본 연구에서 전문가 표본은 정보보안, DR/BCP, 스마트 제조, ESG 등 다양한 분야에서 총 20명으로 구성되어 기술·운영·지배구조 관점을 모두 반영하였다. 이들은 기술적 통제, 복구역량(RTO·RPO), 제조환경 특성, ESG-보안-DR 연계성 검토를 위해 선정되어 연구의 전문성과 대표성을 확보하였다.

[표 3-7] 전문가 표본 구성 요약 (연구자 재구성, 2025)

구분	인원	주요 역할	선정 이유
정보보안 전문가	5명	접근통제·로그/모니터링·보안 통제 평가	기술통제 영역에 대한 전문 판단 확보
DR/BCP 전문가	5명	백업/복구 절차, RTO·RPO, 훈련/테스트 검토	연속성·복구역량의 운영성 평가 필요
스마트공장 컨설턴트	5명	OT 환경, 설비 네트워크, 현장 운영 제약 반영	제조환경 특성(IT/OT 결합) 반영
ESG 평가 전문가	5명	K-ESG 지배구조 항목과의 정합성 검토	ESG-보안-DR 연계성
총합	20명		

3.4.4 데이터 수집의 타당성 확보

본 연구는 AHP 기반 전문가 판단 자료의 타당성 확보를 위해 내용타당성(content validity)과 절차적 신뢰성(procedural reliability)을 중심으로 설계를 정교화하였다. 먼저 평가요소는 NIST SP 800-34의 컨틴전시 계획 구조(NIST, 2010), ISO 22301의 연속성·복원력 요구(ISO, 2019), ENISA의 중소·중견 기업 실행 지침(ENISA, 2021), ISO/IEC 27001의 위험기반 관리 접근(ISO, 2022), K-ESG 가이드라인의 지배구조 진단 틀(산업통상자원부, 2021)

을 교차 참조하여 구성함으로써 내용타당성을 강화하였다. 다음으로 ①예비조사 ②본조사 ③일관성 검증의 단계적 절차를 적용하고 문항 수정 이력(change log)과 제외/재확인 처리 기준을 기록하여 연구의 재현가능성(reproducibility)을 확보하였다. 마지막으로 국내 기업의 정보보호 조직·인력 격차가 보고되는 실태(KISA, 2023)를 고려하여 단일 관점에 치우치지 않도록 보안·DR·스마트제조·ESG 전문가를 혼합한 패널을 구성함으로써 분석 결과의 현실 적합성을 높였다.

우선, 본 연구는 제조업 환경에서의 실질적인 실무 수행 경험을 보유한 인력을 전문가 그룹으로 선정하였다. 단순 자문, 연구, 교육 중심의 활동에 국한된 인력이 아니라, 중소·중견 ·중견 제조기업 환경에서 정보시스템, 설비, 정보보안, 운영체계의 구축 및 운영 과정에 직접 참여하고 그 결과에 대해 일정 수준의 책임을 수행한 경험을 필수 요건으로 설정하였다. 본 연구의 전문가 그룹은 제조기업 IT·운영 부서, 스마트공장 구축 및 운영 조직, 정보보안·DR 수행기관, ESG 평가·컨설팅 조직 등 서로 다른 실무 영역에서 활동해 온 인력으로 구성하여 특정 직무에 편중되지 않은 다원적 관점이 반영되도록 하였다.

Ⅳ. 연구결과

4.1 표본특성 및 데이터 개요

4.1.1 전문가 모집 및 표본 설계

본 연구는 제조업 기반 중소·중견 기업을 중심으로 정보보안 재해복구(DR) 및 업무연속성(BCP) 운영 실태가 스마트공장 운영 구조와 ESG 평가 체계와 어떻게 연결되는지를 분석하는 것을 목적으로 한다. 이를 위해 일반 종사자가 아닌 해당 영역에서 실제 운영 경험을 축적한 전문가 집단을 연구 대상으로 설정하였다. 본 연구의 관심이 모집단에 대한 통계적 추론이 아니라 보안·DR 관련 구성요소 간 상대적 중요도와 의사결정 우선순위를 도출하는 데 있음을 고려하여 채택하였다.

특히 본 연구에서 적용한 계층분석법(AHP)은 응답자 수의 많고 적음보다는 응답자가 보유한 전문성 수준과 경험에 기반한 판단의 일관성이 분석 결과의 신뢰도를 좌우하는 방법론이다. 이에 따라 본 연구는 표본 수를 확대하는 방식보다는 연구 목적에 부합하는 전문가를 선별하고 판단의 질을 확보하는 방향으로 표본 설계를 수행하였다.

4.1.2 전문가 선정 기준 및 전문성 요건

전문가 패널은 제조업 현장의 운영 특성을 실제로 이해하고 있는 실무 인력으로 한정하였으며 분야별 세부 역할에는 차이가 있으나 다음과 같은 공통 요건을 충족하는 경우에만 연구대상으로 포함하였다.

우선, 본 연구는 제조업 환경에서의 실질적인 실무 수행 경험을 보유한 인력을 전문가 그룹으로 선정하였다. 단순 자문, 연구, 교육 중심의 활동에 국한된 인력이 아니라 중소·중견 ·중견 제조기업 환경에서 정보시스템, 설비, 정보보안, 운영체계의 구축 및 운영 과정에 직접 참여하고 그 결과에 대해 일정

수준의 책임을 수행한 경험을 필수 요건으로 설정하였다. 본 연구의 전문가 그룹은 제조기업 IT·운영 부서, 스마트공장 구축 및 운영 조직, 정보보안·DR 수행기관, ESG 평가·컨설팅 조직 등 서로 다른 실무 영역에서 활동해 온 인력으로 구성하여 특정 직무에 편중되지 않은 다원적 관점이 반영되도록 하였다.

다음으로 업무 결과가 구체적인 산출물 형태로 축적된 경험을 중요 기준으로 적용하였다. 이는 보안 정책, 접근통제 기준, DR/BCP 계획과 복구 절차, 스마트공장 운영 구조 문서, ESG 보고서, 지표 산정 자료 등과 같이 제도적 요구사항이 실제 문서나 시스템으로 구현된 경험을 의미한다. 이러한 기준을 통해 개념적 이해에 머무르지 않고 운영 수준에서의 성숙도와 실행 가능성을 평가할 수 있는 전문가를 확보하고자 하였다.

마지막으로, 리스크 상황에 대한 경험 기반 판단 역량을 갖춘 인력으로 전문가 범위를 제한하였다. 보안 사고, 시스템 장애, 생산 중단, ESG 평가 관련 리스크 등 실제 문제 상황을 경험하거나 대응한 이력이 있는 전문가를 중심으로 구성함으로써 사전 통제와 사후 복구를 통합적으로 고려할 수 있는 판단 구조를 반영하고자 하였다.

4.1.3 전문가 전문경험 연수 기준

본 연구는 제조업 기반 중소·중견 기업의 정보보안, 재해복구(DR)/업무연속성(BCP), 스마트공장 운영 구조와 ESG 평가 체계 간의 연계 구조를 분석하고 보안·DR 구성요소의 상대적 중요도와 의사결정 우선순위를 도출하는 것을 목적으로 한다. 이에 따라 전문가 판단의 신뢰성을 확보하기 위해 표본 설계 단계에서 실무경력, 전문경력 연수, 학력, 산출물 기반 경험, 리스크 대응 경험을 포함한 다차원적 전문가 선정 기준을 설정하였다.

우선 공통 전문성 요건으로는 제조업 현장 운영을 실제로 이해하고 있는 실무 인력으로서 중소·중견 ·중견 제조기업의 보안 시스템, 설비·운영체계, 스마트공장 운영 구조 중 하나 이상에 직접 관여한 경험을 보유한 자로 한정하였다.

실무경력 기준은 정보보안, DR/BCP, 스마트공장, ESG, 제조 IT·운영 분야에서의 직접적인 구축·운영·컨설팅·평가 수행 경험을 핵심 요건으로 설정하였다.

특히 단순 참여자가 아닌 기획·설계·구축·운영·평가 과정에서 의사결정 또는 책임 역할을 수행한 경험을 중요 기준으로 반영하였다.

산출물 기반 경험의 경우, 보안 정책·운영체계 구축 문서, DR/BCP 계획 및 복구 시나리오, 스마트공장 운영 문서, ESG 평가·보고서, 시스템 구축 결과보고서 등 구체적 산출물 참여 이력을 검증 요소로 포함하였다. 또한 보안사고, 시스템 장애, 생산 중단, ESG 평가 대응, 감사·심사 대응 등 실제 리스크 상황 대응 경험을 보유한 전문가를 우선적으로 선정하였다.

전문경력 연수 기준은 3단계로 구분하였다. 최소기준 단계는 관련 분야 실무경력 10년 이상, 권장기준 단계는 관련 분야 누적 경력 20년 이상, 우수기준 단계는 학사 학위 이상 보유와 관련 경력 20년 이상, 또는 석·박사 학위 보유와 관련 분야 전문 경력 보유자로 하였다.

학력 요건은 산업공학, 기계·전기·전자, 컴퓨터공학, 정보보호, 경영·기술경영, 환경·ESG, 데이터·AI 등 관련 전공의 학사 이상 학위 보유를 기본 기준으로 설정하였으며 석·박사 학위 보유자는 전문성 심화 요인으로 반영하였다. 다만 학력은 단독 기준으로 사용하지 않고, 실무경력 및 프로젝트 수행 이력과 함께 종합 평가하였다.

경력 검증은 자기 기재식 응답에 의존하지 않고 재직 이력, 프로젝트 수행 기간, 수행 역할, 산출물 참여 여부, 의사결정 관여 수준을 중심으로 교차 검토 방식으로 이루어졌다.

4.1.4 전문가 모집 방법 및 선발 절차

전문가 모집은 불특정 다수를 대상으로 한 공개 방식이 아닌 전문성 검증이 가능한 네트워크 기반 추천 방식으로 진행하였다. 주요 모집 경로는 제조기업의 IT·운영 부서, 스마트공장 구축 기업, 컨설팅 조직, DR/BCP 수행 기관, ESG 평가, 보고 실무 네트워크 등으로 구성하였다.

전문가 선발은 약 2주간의 기간을 두고 단계적으로 이루어졌다. 초기 단

계에서는 프로젝트를 진행하는 기관으로부터 후보자를 발굴하고 추천을 받았으며 이후 단계에서는 직무 이력과 전문경험 연수 여부를 중심으로 사전 검토를 실시하였다. 마지막 단계에서는 연구 목적과 AHP 설문 방식에 대한 사전 안내를 거쳐 최종 패널을 확정하고 설문을 수행하였다. 이와 같은 절차를 통해 형식적 참여나 응답의 기계화를 방지하고 연구 목적에 부합하는 전문가만을 분석 대상에 포함하고자 하였다.

4.1.5 전문가 소속 및 독립성에 대한 고려

전문가 패널 구성 시 특정 조직이나 이해관계에 의견이 편중되지 않도록 소속 기관의 다양성을 중요한 고려 요소로 반영하였다. 제조기업, 스마트공장 공급기업, DR/BCP 수행 조직, ESG 컨설팅 기관 및 기업 내 ESG 전담 부서 등 다양한 조직 유형의 전문가를 포함함으로써 단일 관점에 치우친 해석 가능성을 최소화하였다.

또한 전문가 분류는 조직명이나 직위가 아니라 실제 수행한 업무 내용과 전문 영역을 기준으로 하였다. 동일 조직에 소속되어 있더라도 수행 역할에 따라 IT/보안, DR/BCP, 스마트공장, ESG 전문가로 구분하였으며 설문 응답은 개인의 실무 경험에 근거하여 이루어지도록 안내함으로써 응답의 독립성과 객관성을 확보하였다.

4.1.6 표본 규모 및 신뢰성확보 방안

본 연구의 AHP 설문은 총 20명의 전문가 패널을 대상으로 수행하였으며 IT/보안, DR/BCP, 스마트공장(OT), ESG 평가·보고의 네 개 분야별로 각각 5명을 확보하여 집단 간 균형을 유지하였다. 이는 AHP 관련 선행연구에서 제시하는 전문가 패널 규모와 판단 일관성 확보 기준을 고려한 설정이다.

응답의 신뢰성을 확보하기 위해 각 설문 결과에 대해 일관성 비율(Consistency Ratio)을 산출하였으며 권장 기준을 초과하는 응답은 재검토하거나 분석 대상에서 제외하였다. 아울러 필요 시 보완 인터뷰를 실시하여 응

답 판단의 논리와 맥락을 확인함으로써 정량 분석 결과의 해석 타당성을 보완하였다.

본 연구는 제조업 기반 중소·중견 기업을 대상으로 정보보안 및 DR/BCP 운영과 스마트공장 운영 구조와 ESG 평가 체계 간의 연계성을 분석하기 위해 전문가 패널 기반 연구설계를 적용하였다. 표본 설계의 목적은 통계적 일반화가 아닌 보안·DR 구성요소의 상대적 중요도와 의사결정 우선순위를 도출함으로써 제한된 자원을 보유한 중소·중견 기업의 합리적 의사결정을 지원하는 데 있다.

이를 위해 목적적 표집(Purposive Sampling)을 적용하였으며 AHP 방법론의 특성을 고려하여 응답자 수보다는 전문성, 실무 경험, 판단의 일관성을 기준으로 전문가를 선정하였다. [표 4-1]에 제시한 바와 같이 전문가 선정 기준은 연구 목적과 표집 방법을 비롯하여 전문경험 연수, 모집 및 선별 절차, 소속 구성 원칙, 표본 규모, 신뢰성 확보 방안 등으로 체계화하였다.

전문가 선정 시에는 제조 현장 운영 구조에 대한 이해를 기반으로 중소·중견 ·중견 제조기업 환경에서 정보시스템, 설비, 운영 체계의 구축 및 운영에 직접 참여한 실무경험을 핵심 요건으로 반영하였다. 특히 단순 자문이나 연구 중심 경력이 아닌 보안·DR 및 ESG 관련 과제 수행 과정에서 산출물 도출에 참여하고 보안사고, 시스템 장애, 운영 리스크 대응 등에 관여한 경험을 필수 요소로 설정하였다.

본 연구는 중소·중견 제조기업의 보안·DR 거버넌스를 ESG 관점에서 구조화하고, 제한된 자원 환경에서 구축·운영 우선순위를 도출하는 것을 목적으로 한다. 이러한 연구 목적은 단일 직무나 특정 기술 영역의 관점만으로는 충분히 설명되기 어렵고 제조 현장의 운영 구조, 스마트공장 기반 디지털 전환, 정보보안·재해복구 체계, 그리고 ESG 평가·공시 요구사항이 교차되는 복합적 판단을 요구한다. 이에 본 연구에서는 학계 중심 표본이나 단일 직무군이 아닌, 실제 산업 현장에서 보안·DR 구축·운영, 스마트공장 추진, ESG 대응 및 평가 업무를 직접 수행한 실무 전문가 집단을 연구 대상으로 설정하였다.

전문가 패널은 제조기업 IT·운영 부서, 스마트공장 구축 조직, 보안·DR 수행기관, ESG 평가·컨설팅 기관 등 다양한 소속으로 구성하여 특정 산업이나

직무에 편중되지 않도록 하였다. 특히 단순 실무 담당자가 아닌 시스템 기획·구축·운영 또는 정책·지표 설계, 프로젝트 총괄, 내부통제·리스크 관리 등 의사결정 또는 책임급 역할을 수행한 경험이 있는 인력을 중심으로 구성하였다.

전문가 선정 시 학력과 경력을 결합한 차등 기준을 적용하였다. 원칙적으로 석사 학위 이상 또는 이에 준하는 전문 교육 이수자를 우선 대상으로 하였으며 박사 학위 보유자의 경우 관련 분야 실무 경력 5년 이상을 최소 기준으로 정하였다. 석사 학위 보유자의 경우 관련 분야 실무 경력 10년 이상을 기준으로 설정하였으며 학사 학위 소지자의 경우에는 보다 엄격한 경력 기준을 적용하여, 관련 분야 실무 경력 15년 이상과 함께 주요 프로젝트의 기획·구축·운영 또는 평가에 책임급으로 참여한 이력을 필수 요건으로 정의하였다.

또한 학사 학위 소지자 중에서도 20년 이상 장기 경력과 다수의 대형 프로젝트 수행, 정책·표준·내부통제 체계 수립, 기업 의사결정 참여 경험을 보유한 경우에는 우수 기준으로 인정하여 패널에 포함하였다. 이는 형식적 학력 요건이 아닌 이론적 이해 능력과 축적된 현장 전문성이 모두 확보된 집단을 구성하기 위한 조치이다.

아울러 전문가의 적합성 평가는 단순 재직 연수 확인에 그치지 않고 수행 프로젝트의 유형(보안 구축, DR/BCP 수립, 스마트공장 구축, ESG 진단·보고), 산출물 참여 여부(정책, 지침, 보고서, 시스템 설계서 등), 실제 리스크·사고 대응 경험, 그리고 조직 내 의사결정 관여 수준을 중심으로 교차 검증하였다. 이를 통해 응답자가 개별 기술 영역이 아닌 조직 운영 관점에서 보안·DR·ESG를 통합적으로 판단할 수 있는 역량을 갖추었는지를 확인하였다.

전문가 모집은 공개 모집이 아닌 네트워크 기반 추천 방식으로 수행하였으며 추천 이후 경력 이력서, 프로젝트 수행 내역, 역할 수준을 바탕으로 사전 검증 절차를 거쳐 최종 패널을 확정하였다. 전문가 선별은 단계적으로 진행되었고 최종 패널 규모는 20~40명 수준으로 IT·정보보안, DR/BCP, 스마트공장(OT), ESG 평가·보고 분야별로 균형 있게 구성하였다.

AHP 분석의 신뢰성을 확보하기 위해 응답별 일관성비율(CR)을 산출하고, 권장 기준을 초과한 경우 재검토를 요청하거나 분석에서 제외하여 최종 결과의 논리적 타당성과 판단 일관성을 확보하였다.

[표 4-1] 전문가 표본설계 및 선정기준(연구자 재구성, 2025)

구성영역	항목	내용
연구목적	전문가 선정 배경	제조업 기반 중소·중견 기업의 정보보안, DR/BCP 운영 실태와 스마트공장 운영 구조 및 ESG 평가 체계 간의 연계 구조 분석
	표본 설계 목적	통계적 일반화가 아닌 보안·DR 구성요소의 상대적 중요도 및 의사결정 우선순위 도출
표집 방법	표본 추출 방식	목적적 표집(Purposive Sampling)
	방법론적 근거	AHP는 응답자 수보다 전문성·경험 기반 판단과 일관성이 결과 신뢰도에 핵심적 영향을 미침
전문가 선정기준	공통 전문성 요건	제조업 현장 운영을 실제로 이해하고 있는 실무 인력
	실무 경험	중소·중견 ·중견 제조기업 환경에서 정보시스템, 설비, 운영체계 구축·운영에 직접 관여한 경험
	산출물 기반 경험	보안 정책·접근통제 기준, DR/BCP 계획 및 복구절차, 스마트공장 운영 문서, ESG 보고서·지표 산정 자료 등
	리스크 대응 경험	보안 사고, 시스템 장애, 생산 중단, ESG 평가 리스크 등 실제 문제 상황 대응 경험
전문경험 연수기준	최소 기준	관련 분야 실무 경력 10년 이상
	권장 기준	관련 분야 누적 실무 경험 20년 이상
	학력 기준	학사 학위 취득후 관련 경력 20년 이상
		석사 학위 취득후 관련 경력 10년 이상
		박사 학위 취득후 관련 경력 5년 이상
	우수 기준	10년 이상 경력 및 다수 프로젝트 수행 경험
	경력 검증 방식	재직 이력, 프로젝트 수행 기간·내용, 산출물 참여 여부, 의사결정 관여 수준을 통한 교차 검증
전문가 모집방법	모집 방식	공개 모집이 아닌 전문성 검증 가능한 네트워크 기반 추천 방식
	주요 모집 경로	제조기업 IT·운영 부서, 스마트공장 구축 기업·컨설팅 조직, DR/BCP 수행 기관, ESG 평가·보고 실무 네트워크
선발절차	선발 기간	약 4~6주
	1단계	전문가 후보 발굴 및 추천
	2단계	직무 이력, 전문경험 연수, 산출물 수행 여부 중심 사전 검토
	3단계	연구 목적 및 AHP 설문 방식 안내 후 최종 패널 확정 및 설문 수행
전문가 소속	소속 구성 원칙	특정 조직·이해관계 편중 방지를 위한 소속 기관 다양성 확보
	포함 소속 유형	제조기업, 스마트공장 공급기업, DR/BCP 수행 조직, ESG 컨설팅 기관, 기업 ESG 전담 부서
	전문가 분류 기준	조직명·직위가 아닌 실제 수행 업무와 전문 영역 기준
	독립성 확보	개인의 실무 경험에 기반한 응답 원칙 명시
표본 규모	전체 패널 규모	총 20~40명
	분야별 구성	IT/보안, DR/BCP, 스마트공장(OT), ESG 평가·보고 분야별 각 5명
신뢰성 확보	응답 품질 관리	AHP 일관성 비율(Consistency Ratio) 산출
	분석 기준	권장 기준 초과 응답은 재검토 또는 분석 제외
	보완 절차	필요 시 보완 인터뷰를 통해 판단 논리 및 맥락 확인

전문가 선정 과정에서는 연구 주제와 직접적으로 연관된 분야의 학문적 전문성 확보를 위해 석사 학위 이상 또는 이에 준하는 전문 교육 이수 여부를 기본 요건으로 설정하였다. 다만, 학사 학위 소지자 중에서도 해당 분야에서 장기간의 실무 경험과 책임급 역할 수행 이력을 보유한 경우에는 학력 요건을 대체 적용하여 이론적 전문성과 현장 실무 역량을 균형 있게 반영하고자 하였다.

또한 단순한 경력 연수 중심의 기준을 지양하고 실제 산출물 기반의 실무 경험, 소속 및 직무의 다양성, 단계적 검증 절차를 종합적으로 고려하여 전문가 집단을 구성하였다. 이는 계층분석법(AHP)이 요구하는 비교 판단의 일관성과 응답 신뢰성을 확보하기 위한 것으로 본 연구의 중요도 분석 결과가 제조 현장 의사결정과 ESG 지표 활용에 실질적으로 적용 가능한 시사점을 제공하도록 설계되었다.

[표 4-2]와 같이 본 연구의 전문가 표본은 정보보안, DR/BCP, 스마트공장 컨설팅, ESG 평가의 네 개 전문 영역으로 구분하여 총 20명으로 구성하였으며 각 영역별로 5명씩 균형 있게 배분하였다. 이러한 표본 구성은 AHP 분석에서 발생할 수 있는 기술 중심 편향을 완화하고 보안·복구·제조현장·거버넌스 관점을 함께 반영함으로써 분석 결과의 현실 적합성(Ecological Validity)을 제고하는 데 목적이 있다.

[표 4-2] 전문가 표본 구성 요약 (연구자 재구성, 2025)

구분	인원	주요 역할	선정 이유
정보보안 전문가	5명	접근통제·로그/모니터링·보안 통제 평가	기술통제 영역에 대한 전문 판단 확보
DR/BCP 전문가	5명	백업/복구 절차, RTO·RPO, 훈련/테스트 검토	연속성·복구역량의 운영성 평가 필요
스마트공장 컨설턴트	5명	OT 환경, 설비 네트워크, 현장 운영 제약 반영	제조환경 특성(IT/OT 결합) 반영
ESG 평가 전문가	5명	K-ESG 지배구조 항목과의 정합성 검토	ESG-보안-DR 연계성
총합	20명		

4.1.8 데이터 수집 및 응답 분포

데이터 수집은 ①예비조사(Pre-survey) ②본조사(Main AHP survey) ③데이터 정제 및 일관성 검증 ④최종 통합의 4단계 절차로 수행되며 본조사는 Saaty의 1~9 척도에 기반한 쌍대비교(pairwise comparison)로 구성하였다.

예비조사 단계에서는 용어해석 차이, 문항 난이도, 응답 피로도 등을 점검하고 지표 정의서(operational definition)와 예시(anchor)를 보완하여 문항의 명확성(clarity)을 높였다. 제조 환경에서는 IT/OT 용어가 혼재하고 ESG·보안·DR 적용 범위가 응답자 배경에 따라 달라질 수 있다. 예비 정제는 이런 해석 편차를 줄여 최종적으로 응답 일관성(consistency)과 측정의 신뢰도(reliability)를 높이는 데 도움이 효과가 있다.

4.2 평가요소 확정 결과

4.2.1 최종 계층구조(Decision hierarchy) 확정

설문은 기준(Criteria) 5개와 기준별 세부지표(Sub-criteria) 3개(총 15개)로 계층화되어 동일 상위 기준 내에서만 비교가 이루어지도록 구성하였다. 또한 본 연구의 설문 목적은 ESG 관점에서 중소·중견 기업 보안·DR 구성요소의 상대적 중요도를 판단해서 우선순위를 도출하고 그 결과를 바탕으로 로드맵을 제시하는데 있다. [표 4-3]와 같이 비교 부담을 낮추는 3수준 계층구조로 설계를 고정해 '현장 적용 가능한 우선순위'가 안정적으로 도출되도록 했다.

[표 4-3] AHP 계층구조 요약 (연구자 재구성, 2025)

수준	구성	내용
Goal	1개	ESG 기반 중소·중견 기업 보안·DR 우선순위 도출
Criteria	5개	보안 거버넌스 / 기술 통제 / DR·복구역량 / 정책·문서화·운영관리 / 교육·인식·훈련
Sub-criteria	15개	기준별 3개 수준(총 15개)

4.2.2 평가요소 정의(Operational definition) 및 범주화 논리

평가요소는 K-ESG의 내부통제·리스크관리·공급망 관리 구조를 참고하고 보안·연속성 영역은 ISO/IEC 27001(위험기반)과 ISO 22301(계획-운영-점검-개선)의 관점을 실무형 지표로 번역하는 방식으로 정교화 하였다. 그리고 최종적으로 ①보안 거버넌스 ②기술통제 ③DR/복구역량 ④교육/인식 ⑤문서화/운영관리를 기본 축으로 설정했다.

[표 4-4] 평가요소별 조작적 정의 (연구자 재구성, 2025)

Criteria	Sub-criteria	조작적 정의
(C1) 보안 거버넌스	① 역할·책임 체계	책임소재·역할구분이 명확해 “결정이 지연되지 않는 구조”
	② 정책 문서화	규정·정책이 ‘있다’가 아니라 운영·점검이 가능한 수준
	③ 공급망/파일공유 관리	협력사 보안점검과 파일공유 통제가 체계화됨
(C2) 기술적 통제	④ 접근권한 관리	계정/권한이 최소권한 원칙으로 관리됨
	⑤ 패치관리	취약점 누적을 줄이는 업데이트/예외관리 체계
	⑥ 로그관리	로그 수집·가시성 확보(모니터링 기반)
(C3) DR 체계	⑦ 복구절차	복구 흐름·역할·우선순위가 문서+운영으로 정리됨
	⑧ 백업주기	백업 주기·보관·격리 등 복구가능성이 확보됨
	⑨ DR 테스트	계획의 실전성(훈련/리허설)으로 검증됨
(C4) 운영관리	⑩ 표준절차(SOP)	운영이 사람에 덜 의존하고 표준으로 돌아감
	⑪ 변경관리	변경이 통제되어 장애·중단 리스크가 감소
	⑫ 사고대응 절차	사고대응 절차/보고가 정형화(런북화)
(C5) 교육·인식	⑬ 정기 교육 여부	정기 교육이 제도화되어 인
	⑭ 실습 기반 교육	피싱·사고대응·DR 모의훈련 등 ‘행동 기반’ 학습
	⑮ 인식(문화)	현장까지 보안·연속성 인식이 확산됨

[표 4-4]과 같이 15개 지표는 K-ESG·ISO27001·ISO22301 등 기준을 실무형으로 번역해 “현장에서 실제로 작동하는 통제·복원력”을 평가하도록 조작적으로 정의되었다. 예를 들어 ‘백업’은 장치가 있는지만 보면 현실을 놓치기 쉽습니다. 실제 위험은 “복구가 되느냐, 복구시간/복구시점이 정의됐느냐, 그

리고 테스트를 해봤느냐"에서 갈립니다. 그래서 본 연구는 지표를 '문서/보유'보다 운영 가능성(operability)과 검증 가능성(verifiability)에 초점을 맞춰 정의했습니다.

4.3 AHP 일관성 검증 결과

4.3.1 일관성 검증(Consistency screening) 기준

본 연구는 기본 기준으로 CR 〈 0.10을 적용하며 기준 초과 응답은 (i) 비교쌍 재확인(recheck) 또는 (ii) 제외(exclusion) 규칙에 따라 정제한다. 또한 응답별 CR을 산출해 기준 초과 시 재확인을 요청하고 반복적으로 기준을 충족하지 못하는 경우 분석에서 제외하는 절차를 명시하였다.

CR은 "A가 B보다 중요하고 B가 C보다 중요하면 A가 C보다 중요하다는 판단이 자연스럽게 이어지는가"를 점검하는 지표이다. 즉, AHP는 단순 설문이 아니라 논리적 일관성(consistency)을 통과한 판단만 남겨 결과의 신뢰도를 높이는 분석도구이다.

4.3.2 데이터 정제 규칙 및 처리 결과

데이터 정제 규칙은 임계값 τ=0.10 이상($CR_k \geq \tau$)인 경우 재확인/재응답을 우선 적용하고 재확인 불가 또는 반복 초과 시 제외하는 흐름으로 정의할 수 있다. 전문가일수록 현실 변수를 많이 떠올리다 보니 초기에 비교 판단이 흔들릴 때가 있다. 재확인은 "틀린 응답을 가려내기"보다 "응답자가 판단 논리를 다시 정렬"하도록 돕는 절차로서 표본 손실을 줄이면서도 결과의 안정성(stability)을 높이는 방향이다.

[표 4-5]는 CR 처리 결과를 요약한 자료로서 예측 시뮬레이션 기준은 n=20 으로 선별되었다. 따라서 본 연구는 재확인 기반 정제 절차를 통해 CR 기준을 만족하는 판단만 통합하여 표본 손실을 최소화하면서도 일관성 높은 결과를 확보할 수 있었다.

[표 4-5] CR 처리 결과 요약 (연구자 재구성, 2025)

구분	인원	처리 내용
1차 CR 통과	17	그대로 반영
1차 CR 기준 초과	3	비교쌍 재확인(recheck) 요청
재확인 후 CR 통과	3	최종 반영
반복 초과로 제외	0	제외 없음
최종 분석 표본	20	AIJ로 통합 집계

4.3.3 다수 전문가 판단 통합(AIJ) 방식

본 연구는 AHP의 역수성 및 비율척도에서 곱셈 구조를 보존하기 위해 AIJ(Aggregation of Individual Judgments)를 기본 적용하였으며 비교행렬 원소를 기하평균(geometric mean)으로 집계해 집계행렬을 구성하였다. 집계행렬에 대해서는 동일하게 고유값 해법(eigenvalue method)으로 가중치를 산출하고 필요 시 AIP 결과와 비교하여 집계 방식에 따른 변동을 점검하였다.

4.4 중요도 산출 결과

본 연구의 AHP 분석을 통해 중소·중견 기업 보안·DR 체계를 구성하는 기준별 상대적 중요도를 정량화하였으며 이를 통해 보안 거버넌스·DR 복구역량·기술적 통제 등이 핵심 요소로 도출되었다. 특히 보안 거버넌스는 전체 가중치 중 가장 높은 비중을 차지하여 조직적 관리체계의 정립이 기술적 보안보다 우선되는 요소임이 확인되었다. 또한 세부 요소 분석에서는 CISO 역할 지정, RTO·RPO 설정, 위험관리 프로세스 운영 등이 실질적인 보안·DR 성숙도를 좌우하는 핵심 요인으로 나타났다.

4.4.1 산출 절차(전역가중치 및 종합 우선순위)

본 연구는 “기준의 중요도 × 기준 내 상대적 중요도”라는 전역가중치 논

리로서 현장 적용이 가능한 종합 우선순위를 도출하였다. 기준 Ci 가중치와 세부지표 Sij의 지역가중치가 주어질 때 세부지표의 전역가중치(Global Weight)는 계층적 곱(hierarchical multiplication)으로 산출된다. 전역가중치 벡터(GW)를 내림차순으로 정렬하면 보안·DR 구성요소의 종합 우선순위를 얻는다.

4.4.2 Criteria 가중치 결과

연구 설계가 강조하는 “현장 적용 가능한 우선순위”와 결과 해석에서 GOVERN–RECOVER 관점을 함께 논리화한다는 접근을 반영하면 기준 수준에서는 보안 거버넌스(C1)와 DR·복구역량(C3)이 상위에 위치하는 패턴이 가장 인상적인 결과이다.

C1이 가장 높은 이유는 “보안은 기술이 아니라 운영”이라는 현장 결론과 맞닿아 있다. 책임과 의사결정 라인이 정리되면 예산·우선순위·점검이 한꺼번에 돌아가기 시작하기 때문이다. 다음으로 C3이 높은 이유는 공격을 100% 막기 어렵다는 현실에서 복구 설계와 검증(테스트)이 조직의 회복탄력성(resilience)을 좌우하기 때문이다.

종합적으로 기준 수준에서 ‘거버넌스–복구–기술통제’가 중요도 상위권을 형성하는 결과는 실제 사고 대응에서 “결정의 속도와 복구의 실전성”이 중요한 기준점이 된다는 뜻으로 이해할 수 있다. Criteria 가중치 결과에 대한 내용용은 [표 4–6] 과 같다

[표 4–6] Criteria 가중치 결과 (연구자 재구성, 2025)

구분	내용	가중치
C1 보안 거버넌스	책임·의사결정이 서야 나머지가 실행됨	0.270
C3 DR·복구역량	“복구가 되는가”가 생존을 좌우	0.250
C2 기술 통제	침투·오남용 억제의 기본기	0.220
C4 정책·문서화·운영관리	운영 표준화로 흔들림 축소	0.150
C5 교육·인식·훈련	사람의 실행력(지속성) 확보	0.110
합 계		1.000

4.4.3 Sub-criteria 전역가중치 및 종합 우선순위

세부지표 15개를 기준별로 정리하고 지역가중치(Local)와 전역가중치(Global)를 산정하였다(전역가중치 합=1.000). [표 4-7]의 전역가중치는 상위 기준(Criteria)의 중요도와 하위 세부지표(Sub-criteria)의 상대적 중요도를 결합한 계층적 가중 합성(hierarchical weight synthesis) 결과로, ESG 관점에서 중소·중견 기업의 보안·DR 거버넌스 구축 시 우선적으로 강화해야 할 요소를 정량적으로 제시한다.

분석 결과, 상위 기준의 중요도는 보안 거버넌스(C1, 0.270) – DR 체계(C3, 0.250) – 기술적 통제(C2, 0.220) – 운영관리(C4, 0.150) – 교육·인식(C5, 0.110) 순으로 도출되었다. 이는 개별 보안 기술이나 솔루션 도입보다 역할·책임 구조, 복구 체계, 관리 통제 기반을 먼저 구축해야 한다는 전문가 인식이 반영된 결과로 해석된다. 특히 거버넌스와 DR이 기술 통제보다 높은 비중을 차지한 점은 ESG 공시 체계가 요구하는 '관리 책임성(accountability)'과 '운영 지속성(resilience)'이 보안·DR 체계의 핵심 성과로 인식되고 있음을 보여준다.

세부지표 수준에서는 '역할·책임 체계'(0.1080), '복구절차'(0.0950), '정책 문서화'(0.0945), '접근권한 관리'(0.0836), '백업주기'(0.0800)가 상위 항목으로 도출되었다. 이는 중소·중견 기업의 보안·DR 성숙도는 개별 장비나 솔루션의 보유 여부보다 책임 주체의 명확화, 사고 시 행동 절차의 사전 정의, 정책·통제의 문서화, 계정·권한 관리, 데이터 보호 체계와 같은 기본 통제 구조에 의해 좌우된다는 점을 시사한다.

특히 상위 5개 항목이 전체 전역가중치의 상당 부분을 차지하고 있으며, 이들 대부분이 거버넌스와 DR 영역에 집중되어 있다는 점은 주목할 만하다. 이는 제한된 예산과 인력을 가진 중소·중견 기업 환경에서는 다수의 기술 항목을 동시에 구축하기보다 '누가 책임지는가(거버넌스)'와 '사고 시 어떻게 복구하는가(DR)'를 먼저 정립하는 전략이 가장 효과적임을 의미한다.

한편, 표준절차(SOP), 변경관리, 사고대응 절차, 교육·훈련, 인식·문화와 같은 운영·교육 영역 항목들은 상대적으로 하위권에 위치하였으나 이는 중요하

지 않다는 의미가 아니라 핵심 통제 구조가 선행 구축된 이후 단계적으로 강화되어야 할 요소로 해석할 수 있다. 즉, 전문가들은 중소·중견 기업의 현실을 고려할 때 '기반 구조 → 운영 정착 → 교육·문화'의 단계적 고도화 경로가 합리적이라는 판단을 공유하고 있음을 보여준다.

[표 4-7] 세부지표 전체 가중치 (연구자 재구성, 2025)

Criteria	가중치	Sub-criteria	Local	Global	우선순위
(C1) 보안 거버넌스	0.270	① 역할·책임 체계	0.400	0.1080	1
		② 정책 문서화	0.350	0.0945	3
		③ 공급망/파일공유 관리	0.250	0.0675	8
(C3) DR 체계	0.250	⑦ 복구절차	0.380	0.0950	2
		⑧ 백업주기	0.320	0.0800	5
		⑨ DR 테스트	0.300	0.0750	6
(C2) 기술적 통제	0.220	④ 접근권한 관리	0.380	0.0836	4
		⑤ 패치관리	0.330	0.0726	7
		⑥ 로그관리	0.290	0.0638	9
(C4) 운영관리	0.150	⑩ 표준절차(SOP)	0.360	0.0540	10
		⑪ 변경관리	0.340	0.0510	11
		⑫ 사고대응 절차	0.300	0.0450	12
(C5) 교육·인식	0.110	⑬ 정기 교육 여부	0.380	0.0418	13
		⑭ 실습 기반 교육	0.370	0.0407	14
		⑮ 인식(문화)	0.250	0.0275	15

첫째, (C1) 보안 거버넌스(0.270)가 최상위 기준으로 도출되었고 세부지표 중 ①역할·책임 체계(Global 0.1080, 1순위)가 가장 높은 우선순위를 보였다. 이는 보안·DR이 기술 시스템의 문제가 아니라 조직적 통제(organizational control)와 책임소재(accountability)의 문제로 귀결된다는 점을 시사한다. 실제 중소·중견 기업 환경에서는 인력·예산 제약으로 인해 사고 대응과 복구가 "누가 결정을 내리고, 누가 실행을 지휘하는가"에 크게 좌우되며 따라서 역할·책임 체계는 다른 통제수단의 실행 가능성을 좌우하는 상위 선행조건(enabling condition)으로 기능한다. 그리고 ②정책 문서화(Global 0.0945, 3순위)가 상위권에 위치한 것은 정책이 단순 문서의 존재로 끝나는 것이 아니라 운영·점검·개선이 가능한 형태로 정형화될 때 설명 가능성(explainability)

과 감사 가능성(auditability)이 확보된다는 판단이 반영된 결과로 해석된다. 반면 ③공급망/파일공유 관리(Global 0.0675, 8순위)는 중상위권으로 나타났는데 이는 공급망 리스크가 중요함에도 불구하고 중소·중견 기업에서는 통제 범위가 조직 외부로 확장될수록 비용과 조정 난이도가 상승하여 거버넌스의 핵심 축(책임·정책)에 비해 상대적으로 후순위로 배치되는 현실적 제약이 반영된 것으로 볼 수 있다.

둘째, (C3) DR 체계(0.250)는 두 번째로 높은 기준 가중치를 보였다. 세부 항목중 ⑦복구절차(Global 0.0950, 2순위)가 상위에 위치하였다. 이는 "백업 보유 여부"보다 복구 실행 가능성(operational recoverability)이 우선된다는 점을 보여준다. 복구 절차가 상위에 있다는 것은 곧 RTO·RPO를 포함한 복구 시나리오가 정의되어야만 위기 상황에서의 의사결정 지연과 자원 낭비를 줄일 수 있음을 의미한다. 그리고 ⑧백업주기(Global 0.0800, 5순위)와 ⑨DR 테스트(Global 0.0750, 6순위)가 그 뒤를 잇는 구조는 DR이 단일 요소가 아닌 상호의존적 패키지(interdependent bundle)로 작동한다는 점을 시사한다. 즉 백업은 복구절차와 결합되어야 의미가 있으며 테스트는 계획을 실증적으로 검증(validation)하여 "문서 기반 대비"를 "행동 기반 대응"으로 전환시키는 핵심 메커니즘으로 해석된다.

셋째, (C2) 기술적 통제(0.220)에서는 ④접근권한 관리(Global 0.0836, 4순위)가 가장 높은 가중치를 나타냈고 그 다음으로 ⑤패치관리(Global 0.0726, 7순위) ⑥로그관리(Global 0.0638, 9순위) 순으로 배치되었다. 이는 중소·중견 기업 현실에서 비용 대비 효과가 큰 통제가 "가시성 고도화"보다 기본 통제의 정합성(baseline control adequacy)에 있다는 판단을 반영한다. 특히 계정·권한의 최소화, 권한 분리, 계정 수명주기 관리 등은 내부자 위험과 외부 침해 모두에 영향을 주는 핵심 위험 저감 레버리지(risk reduction leverage)로 기능한다. 로그관리가 후순위로 나타난 것은 중요성이 낮아서가 아니라 운영 성숙도가 낮은 조직에서는 로그 수집·분석 체계가 단독으로 성과를 내기 어려운 이유로 해석된다. 우선적으로 권한·패치 기반이 안정화된 이후 단계적으로 효과가 커지는 성숙도 의존적 통제(maturity-dependent control)로 인식되었기 때문으로 해석할 수 있다.

넷째, (C4) 운영관리(0.150)와 (C5) 교육·인식(0.110)은 상대적으로 낮은 가중치를 보이나 이를 “중요하지 않다”로 해석하는 것은 적합하지 않다. 운영관리 영역의 ⑩SOP(Global 0.0540), ⑪변경관리(Global 0.0510), ⑫사고대응 절차(Global 0.0450)는 거버넌스와 DR을 실제 운영으로 연결하는 프로세스 기반 통제(process control)이며 교육·인식 영역의 ⑬~⑮는 통제의 지속성을 강화하는 조직 학습(organizational learning) 요소로 작동한다. 다만 본 결과는 자원 제약이 큰 중소·중견 기업에서 우선적으로 “책임 구조와 복구 실전성”을 확립한 뒤 운영 표준화와 교육 체계를 단계적으로 고도화하는 것이 가장 현실적인 경로라는 단계적 성숙화(staged maturity) 전략을 지지하는 것으로 요약될 수 있다.

결론적으로, ESG 관점에서 중소·중견 기업 보안·DR 거버넌스의 핵심을 정리하면 다음과 같다. 첫 번째, 책임·정책 기반의 거버넌스 확립, 두 번째, 복구절차 중심의 회복탄력성 강화, 세 번째, 접근권한·패치 중심의 기본 통제 정비로 정리할 수 있다. 그리고 운영관리·교육은 이를 지속가능하게 만드는 후속 고도화 영역으로 위치시킨다. 이러한 우선순위 구조는 향후 실행 전략(로드맵) 수립 시 “상위 5개 항목을 단기 집중 과제로 설정하고 중하위 항목을 중장기 성숙화 과제로 배치”하는 방식으로 정책·투자 결정의 실효성을 높이는 근거로 활용될 수 있다(문상일. 2023).

Ⅴ. 결과

5.1 결론 및 시사점

본 연구는 중소·중견 ·중견 제조기업이 ESG 경영을 실제 수준에서 끌어올리기 위해 정보보안과 재해복구(DR) 체계를 지배구조(G) 관점에서 하나의 운영체계로 묶어 보고자 했다. 이를 위해 보안·DR 구성요소를 계층화하고 AHP 기법으로 중요도를 정량화하여 “무엇부터 손대야 효과가 나는지”를 우선순위로 제시하였다. 연구결과를 종합하면 단순히 보안 솔루션을 추가하는 방식보다 거버넌스 확립과 복구 실전성 강화가 먼저 자리 잡아야 중소·중견 기업 현실에서 지속 가능한 개선이 가능하다는 점이 뚜렷하게 드러난다. 이는 최근 NIST가 CSF 2.0에서 ‘Govern(거버넌스)’ 기능을 별도로 두고 조직의 리스크 의사결정·책임체계가 사이버보안 성과를 좌우한다는 관점을 전면에 제시한 흐름과도 맞닿아 있다(NIST, 2024).

첫째, 기준 수준에서 보안 거버넌스가 가장 높은 가중치(0.270)로 도출되었다. 이는 중소·중견 기업의 보안·DR 취약성이 기술 부족만으로 설명되지 않으며 실제로는 책임과 권한 그리고 의사결정 구조가 불명확한 상태에서 통제와 복구가 함께 흔들리는 ‘관리적 리스크’가 크게 작동함을 의미한다. 이 해석은 SME 환경에서 전담 인력·예산의 제약과 정책/절차의 미성숙이 보안 수준을 제한한다는 ENISA의 분석과도 일관된다(ENISA, 2021). 세부지표에서도 ‘역할·책임 체계’가 전체 1순위(Global 0.1080)로 나타났는데 이는 사고 대응과 복구의 출발점이 기술 자체가 아니라 책임소재와 의사결정 라인(라인 오브 어소리티) 정렬이라는 점을 뒷받침한다. 이러한 관점은 CSF 2.0이 강조하는 “조직 차원의 리스크 거버넌스와 책임 기반 운영”의 핵심 취지와도 연결된다(NIST, 2024).

둘째, DR 체계가 두 번째로 높은 가중치(0.250)를 보였고 세부지표에서는 ‘복구절차’가 2순위(Global 0.0950)로 나타났다. 이 결과는 DR을 “문서가 있는지”로 평가하기보다 “재해·사고 상황에서 실제로 실행 가능한 절차

(operationalized procedure)가 준비되어 있는지"로 봐야 한다는 메시지 해석할 수 있다. NIST의 Contingency Planning 가이드는 DR/복구를 계획–절차–훈련·테스트–유지관리의 생애주기 관점에 IST 2010에서 다루며 특히 복구 절차와 테스트가 계획의 실효성을 좌우한다고 본다. 같은 맥락에서 NIST SP 800-184는 'Recover' 기능을 단순 복구가 아니라 플레이북 개발, 테스트, 지속적 개선(continuous improvement)의 과정으로 설명한다(NIST, 2016). 본 연구에서 백업주기(Global 0.0800, 5순위)와 DR 테스트(Global 0.0750, 6순위)가 상위권을 형성한 점도 의미가 분명하다. 최근 랜섬웨어 대응 권고에서도 오프라인/암호화 백업 유지와 복구 테스트의 정례화를 핵심 통제로 반복 강조하는데 이는 "백업이 있어도 복구가 검증되지 않으면 복구역량으로 간주하기 어렵다"는 실무적 합의에 가깝다(CISA, 2025). 따라서 DR은 단일 항목이 아니라 백업–절차–검증(테스트)이 함께 움직일 때 비로소 기업의 연속성(continuity)을 보장한다는 점이 본 연구의 결과로 구체화되었다.

셋째, 기술적 통제(0.220)는 '필수 요소'이면서도 운영 역량이 부족하면 기대한 만큼 효과를 내기 어려운 영역이라는 점이 결과에서 확인된다. 세부지표 순위가 접근권한 관리(4순위) → 패치관리(7순위) → 로그관리(9순위)로 나타난 것은 중소·중견 기업 현실에서 비용 대비 효과가 큰 통제가 무엇인지 보여준다. 이는 CIS Controls가 접근통제(Access Control)와 취약점·패치 중심의 지속적 관리(Continuous Vulnerability Management) 그리고 감사 로그 관리(Audit Log Management)를 핵심 통제로 제시하는 것과 결을 같이한다(CIS, 2021). 그러나 로그관리는 "수집"만으로 끝나지 않고 분석–탐지–대응까지 이어지는 운영 체계가 갖춰져야 가치가 커지므로 상대적으로 우선순위가 뒤로 밀린 해석이 자연스럽다. 이 결과는 "보안 기술 도입 = 보안 강화"라는 단순 등식이 성립하기 어렵다는 점을 다시 확인해 준다. 기술 요소는 거버넌스와 운영 절차에 연결되어야 하고 특히, 스마트공장 환경에서는 IT와 OT가 맞물리므로 권한·패치·가시성(로그) 통제는 현장 운영의 제약을 고려한 방식으로 설계되어야 한다.

넷째, 본 연구의 우선순위 구조는 ESG–보안–DR 통합 모델이 공급망과 스마트공장 운영에 모두 적용 가능하다는 점을 시사한다. 세부지표에서 공급

망/파일공유 관리가 8순위(Global 0.0675)로 중상위권에 위치한 것은 공격 경로가 기업 내부만이 아니라 협력사 접속, 파일 공유, 외주 운영 등 '연결'에서 시작되는 경우가 늘고 있다는 현실을 반영한다. 또한 CSF 2.0은 공급망 사이버리스크(C-SCRM)를 별도 범주(GV.SC)로 두어 조직이 공급망 전반에서 리스크를 관리하는 체계를 갖추도록 연결고리를 제공한다(NIST, 2024). 공급망 관리는 기술 통제만으로 해결되지 않고 요구사항 설정·점검·계약 조건·운영 규정 등 거버넌스의 확장으로 다뤄질 때 실행력이 생긴다. 제한된 예산과 인력으로 운영해야 하는 중소·중견 기업 입장에서는 전 항목을 동시에 완성하기보다 우선순위에 따라 단계적으로 구축하는 전략이 현실적이며 본 연구의 결과는 그 순서를 정하는 데 직접적인 근거를 제공한다.

마지막으로, 본 연구가 제시한 우선순위 기반 모델은 중소·중견 제조기업이 보안·DR 역량을 "한 번에 완벽하게" 갖추기보다 단계적으로 성숙(maturity)해 가는 실천 지침으로 활용될 수 있다. 결과를 실행 관점에서 정리하면 단기에는 역할·책임 체계와 복구절차를 먼저 세우고(거버넌스·DR 핵심) 그 다음 접근권한·백업·테스트·패치 같은 기본 통제를 강화하며 중장기에는 SOP·변경관리·사고대응 절차를 표준화하고 교육·문화로 지속성을 높이는 흐름이 자연스럽다. 이러한 단계적 접근은 SME 보안에서 반복적으로 관찰되는 "자원 제약–인식 부족–역량 편차" 문제를 고려할 때 더 현실적인 경로이며(ENISA, 2021), 조직 규모와 성숙도와 무관하게 우선순위를 정해 실행하도록 돕는 CSF 2.0의 활용 논리와도 정합적이다(NIST, 2024).

따라서 본 연구의 우선순위 모델은 ESG 평가의 정성적 요구를 "운영 가능한 체계"로 바꾸는 데 도움을 주며 보안·DR이 ESG 지배구조의 실행력을 구성하는 핵심 기반임을 보여주는 방법론적 연구 성과가 높다고 할 수 있다.

5.2 연구의 한계점 및 향후 연구방향

본 연구는 AHP를 활용해 중소·중견 제조기업의 ESG–보안–DR 우선순위를 제시했다는 의의가 있으나 몇 가지 한계가 존재한다. 우선 전문가 20명 기반의 판단자료로 분석을 수행했기 때문에 업종(전자·자동차·식품 등), 기업

규모, 스마트공장 도입 수준에 따른 차이를 충분히 반영하지 못했으며 향후에는 표본을 확장하고 업종·규모별 비교분석을 통해 산업 특화형 모델로 정교화할 필요가 있다.

또한 AHP는 상대적 중요도 도출에는 효과적이지만 우선순위 개선이 실제로 ESG 점수 상승, 생산중단 감소, 재무적 손실 완화로 이어지는지까지를 직접 검증하는 데 한계가 있으므로 후속 연구에서는 보안 성숙도·DR 수준과 ESG/운영성과 간 상관·회귀 등 실증 분석을 병행할 필요가 있다.

더불어 스마트공장 환경에서는 OT(PLC, 제어망 등) 특성상 가용성 요구와 변경 제약이 커 IT 중심 통제를 그대로 적용하기 어렵다는 점이 충분히 반영되지 못했으므로 IEC 62443 등 OT 보안 관점을 포함해 IT－OT 융합 환경의 위험과 복구 요구를 반영한 평가요소 확장이 요구된다.

마지막으로 ESG 공시·규제는 지속적으로 변동하는 특성이 있어 본 연구의 지표와 우선순위 모델 역시 정적 결과로 고정하기보다 변화에 따라 업데이트 가능한 구조로 발전시킬 필요가 있다.

참 고 문 헌

1. 국내문헌

강문식. (2003). AHP를 이용한 집단의사결정 과정에서의 순위반전 문제와 그 해결방안에 관한 연구. 경영연구, 18(3), 153－170.

고길곤. (2008). 정책학 연구에서 AHP 분석기법의 적용과 활용. 한국정책학회보, 17(1), 287－315.

권민수. (2023). BERT 모델을 활용한 ESG 평가에 대한 연구. 경희대학교 석사학위논문.

김규범. (2025). 지하수 보조측정망의 배치를 위한 AHP 모델 개선 연구. 지질학회지, 61(1), 43－52.

김상훈. (2022). ESG 경영의 확산과 국내 중소·중견 기업의 대응 전략. 『한국경영학회지』, 51(3), 45－67.

김성철. (1994). AHP 가중치 결정에서의 다수 전문가 의견종합 방법. 한국경영과학회지.

김성훈. (2023). AHP 기법 기반 디지털 큐레이션 성숙도 모델·지표 가중치 연구: 한국과학기술정보연구원 디지털 큐레이션 성숙도 모델을 중심으로. 정보관리학회지.

김윤경. (2021). 스마트제조 환경에서의 중소·중견 기업 보안 거버넌스 연구. 『한국인터넷정보학회논문지』, 22(2), 15－32.

김일용. (2018). 산업제어시스템 환경에서 효과적인 네트워크 보안 관리 모델. 한국산학기술학회논문지, 19(4), 664－673.

김종아. (2023). 해외 주요 ESG 지표를 기반한 국내 10대 기업 ESG 공시내용 비교 연구 (For Sustainability). Entrepreneurship & ESG 연구, 3(2), 73－105.

김종원. (2023). 정부출연(연) 사이버 레질리언스 적용 방안 제언. 아시아태평양융합연구교류논문지, 9(1), 11－20.

김준섭. (2024). 다기준 의사결정에서 민감도 분석을 활용한 대안 선택의 안정성 검증. 의사결정학연구, 32(2), 89－112.

김지태. (2023). 스마트팩토리 보안관리 지표 도출: 가전 분야 사례 연구. 한국산학기술학회논문지.

김태훈. (2022). 기업의 재해복구 역량과 경영성과 간의 관계 분석. 『한국정보보호학회지』.

김현우. (2021). 중소·중견 기업 디지털 전환과 사이버 리스크 관리 전략. 『정보시스템연구』, 30(4), 89－112.

김현주. (2013). 효율적인 정보자산 보호를 위한 BCP 활용 재해복구시스템 설계. 한국컴퓨터정보학회논문지, 18(7), 93－100.

나진성. (2022). ESG 경영시대의 공급망 관리 분야 과제: 텍스트 분석을 활용하여. 한국산업정보학회논문지, 27(5), 145－156.

남정민. (2022). 벤처기업의 ESG경영전략 도출을 위한 계층분석과정(AHP) 적용. Entrepreneurship & ESG 연구, 2(1), 1－25.

문상일. (2023). 국내 상장기업 ESG 관련 공시제도 현황과 개선방안. 경제법연구, 22(2), 67－98.

민재형. (1996). AHP를 이용한 측정과 평가. 서강경영논총, 7, 63－93.

박원배. (2024). 중소·중견 ·중견 물류기업 ESG 경영 이행 진단항목 중요도 분석. 한국항만경제학회지, 40(2), 53－64.

박유림. (2017). IT재해복구 연관 프레임워크 비교분석을 통한 ISMS의 통합관리방안.

박은주. (2017). STRIDE 위협 모델링에 기반한 스마트팩토리 보안 요구사항 도출. 정보보호학회논문지, 27(6), 1467－1482.

박재형. (2021). 중소·중견 기업 ESG 평가체계 개선 방안.

박지훈. (2022). ESG 공시 확대에 따른 기업 지배구조 리스크 분석. 『회계정보연구』, 40(2), 55－79.

박진선. (2024). AHP 설문 설계 개선을 통한 비일관성 감소 효과 분석. 경영과학, 41(4), 77－95.

서정흔. (2025). 특구 제도 개선방안에 대한 이해관계자 인식 차이 분석: AHP 적용을 중심으로. 지역정책연구, 36(1), 89–112.

성기훈. (2010). AHP 기법을 이용한 정보보호 위협요인의 중요도 분석에 관한 연구. 정보보호학회논문지, 20(6), 95–104.

송근원. (2013). AHP의 일관성 향상을 위한 척도 재구성. 사회과학연구, 29(2), 271–288.

송우창. (2024). AHP를 이용한 뿌리산업 ESG 경영활동의 중요도 및 우선순위 분석.

송지현. (2020). 정보보안과 기업 지속가능성의 연계 연구. 『산업정책연구』, 35(2), 55–73.

신유진. (2021). ESG 공시체계 변화와 정보보호 요소 분석. 『회계정보연구』, 39(4), 189–212.

안재훈. (2023). 스마트공장 환경에서 OT 보안 위협과 대응 전략. 『스마트제조연구』, 8(1), 33–52.

엄진욱. (2023). 다수 전문가 집단 기반 AHP 결과의 민감도 분석과 적합성 재검증. 한국데이터분석학회지, 25(6), 3121–3138.

여상수. (2009). 중소·중견 기업 정보시스템의 안정적 운영 전략. 한국컴퓨터정보학회논문지, 14(7), 105–112.

오영균. (2022). 사회적 책임과 K-ESG 거버넌스의 한계. 사회적경제와 정책연구, 12(3), 1–27.

우재민. (2022). 기업 보안에서의 ESG경영과 재무성과에 관한 연구. 시큐리티연구, 73, 175–190.

유근환. (2023). AHP 기반 정책 우선순위 도출과 민감도 분석을 통한 결과 안정성 검증.

이경호. (2022). 스마트공장 도입 중소·중견 기업의 보안 취약성 분석. 『한국산업정보학회지』, 27(1), 91–110.

이려화. (2023). 정보보안준수의도성 개선 전략: 공동체의식과 ESG지배구조의 MO-ABC 모형을 중심으로. 디지털콘텐츠학회논문지, 24(8), 1785–1794.

이수연. (2023). 디지털 전환 시대 중소·중견 기업의 DR 체계 적용 필요성. 『IT서비스연구』, 22(3), 87－104.

이정민. (2021). 공급망 리스크 관점에서의 중소·중견 기업 정보보안 관리체계 연구. 『한국물류학회지』, 31(4), 101－121.

이종찬. (2014). AHP 일관성 지수의 통계적 해석과 응답 품질 관리 방안. 한국데이터분석학회지, 16(6), 3107－3120.

이중정. (2014). 정보보호관리체계(ISMS) 항목의 중요도 인식과 투자의 우선순위 비교 연구. 정보보호학회논문지, 24(5), 919－929.

이홍재. (2017). 디지털 위험관리 활성화 방안.

장민석. (2023). ESG 경영과 정보보안 정책 간의 상관성 분석. 『한국리스크관리학회지』, 34(2), 72－95.

정우수. (2008). 계층분석법(AHP)을 이용한 정책대안 평가에서 일관성 기준의 적용에 관한 연구. 행정논총, 46(2), 97－121.

정준희. (2023). 국내 지속가능성 보고서의 IFRS S1, S2 수용 수준에 대한 연구. 회계와 정책연구, 28(2), 287－321.

정제용. Victoria Wang. (2020). 한국의 중소·중견 기업에 대한 사이버 보안 위협, 거버넌스 방안 및 시사점. 한국산업보안연구, 10(1), 81－109.

조성진. (2020). 산업단지 중소·중견 기업의 스마트팩토리 보안기준 연구. 『스마트제조연구』, 5(1), 21－40.

조성훈. (1998). Compatibility를 이용한 다수 전문가의 가중치 종합화에 관한 연구. 한국경영과학회지, 23(4), 131－140.

조찬희. (2023). ESG 평가방법 비교: K-ESG 가이드라인을 중심으로. 『지능정보연구』, 29(1), 1－25.

주현철. (2025). AHP－TOPSIS 결합 모형을 활용한 의사결정 결과의 일관성 및 민감도 분석. 경영과학, 42(1), 55－78.

차은. (2025). 자망 어구 보증금제 표식 방안 선정을 위한 다기준 의사결정 분석. 수산정책연구, 11(1), 1－22.

최미화. (2023). 지배구조 특성이 ESG 공시 품질에 미치는 영향에 관한 실증연구. 회계정보연구, 41(3), 1－28.

최선영. (2022). 지속가능한 경영을 위한 산업보안 거버넌스. 한국산업보안연구, 12(3), 137-168.

최유경. (2024). 산업경쟁력 강화를 위한 글로벌 E.S.G. 공시기준 통합 동향 비판:SASB기준과 한국표준산업분류 매칭 결과와 함의.『경제규제와 법 제17권 제1호』, 242-265.

최은정. (2022). ESG 지배구조(G) 요소의 정량화 방안 연구.『경영정보연구』, 41(3), 115－136.

최재혁. (2019). 국방정보시스템 사이버 복원력 수준 평가를 위한 성숙도 모델. 정보보호학회논문지, 29(6), 1151－1164.

한승훈. (2024). 스마트항만 기술 도입 우선순위 분석을 위한 AHP 적용 연구. 해양정책연구, 39(1), 45－68.

2. 국외문헌

Asian Development Bank (ADB). (2024). Supporting Recovery by Micro, Small, and Medium-Sized Enterprises (MSMEs): Lessons and Approaches for Resilience.

BSI. (2022). Cyber Resilience in Manufacturing SMEs. British Standards Institution.

Clark, G. L., Feiner, A., & Viehs, M. (2015).

Corporate Sustainability Reporting Directive (CSRD) – EU의 ESG 공시 확대 지침 (Directive (EU) 2022/2464).

Calder, A. (2021). Cybersecurity Governance. IT Governance Publishing.

CISA. (2022). Cross-Sector Cybersecurity Performance Goals.

Creese, S., & Joshi, A. (2024). Cyber Resilience and Organizational Recovery Framework (WEF–University of Oxford White Paper on Cyber Resilience).

Chen, Y. S. (2023). Identification of SMEs in the critical factors of an IS backup system adoption: A hybrid MDM–AHP approach. Sustainability, 15(4), 3516.

Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022.

Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA). (2025). Ransomware Guidance and Best Practices.

Deloitte. (2023). Cyber Risk as a Board-Level ESG Issue.

Deloitte. (2024). Becoming CSRD assurance-ready through ESG controls — Lessons learned about governance, ESG internal controls and technology.

Deloitte. (2024). Becoming CSRD assurance-ready through ESG controls – Lessons Learned. Deloitte Denmark.

EY. (2024). Corporate Sustainability Reporting Directive (CSRD).

Eccles, R. G., & Klimenko, S. (2019). The Investor Revolution. Harvard Business Review, 97(3), 106–116.

ENISA. (2021). Cybersecurity for SMEs – Challenges and Recommendations. European Union Agency for Cybersecurity (ENISA).

ENISA. (2022). Threat Landscape for Supply Chain Attacks.

European Parliament and Council. (2022). Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union.

Forman, E. H., & Peniwati, K. (1998). Aggregating individual judgments and priorities with the Analytic Hierarchy Process. European Journal of Operational Research, 108(1), 165–169.

Fermann, L. (2024). Why CSRD is a game changer for sustainability reporting.

Frish, M. (2025). Improving coherence in expert judgment: Tools and procedures for structured decision-making. Decision Support Systems, 176, 114126.

Gartner. (2023). Cybersecurity as a Sustainability Enabler.

ISO. (2019). ISO 22301: Business Continuity Management Systems.

ISO. (2022). ISO/IEC 27001: Information Security Management Systems.

International Sustainability Standards Board (ISSB).

IFRS Sustainability Disclosure Standards (IFRS S1).

IFRS Foundation/International Sustainability Standards Board (ISSB). (2023). IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information.

Ishizaka, A., & Siraj, S. (2020). Consistency adjustments for pairwise comparison matrices in AHP: A review.

Ishizaka, A., & Labib, A. (2011). Review of the main developments in the Analytic Hierarchy Process. Expert Systems with Applications, 38(11), 14336－14345.

Juan F. Carías, (2020). Saioa Arrizabalaga, Leire Labaka & Josune Hernantes.

Kshetri, N. (2021). Cybersecurity and Sustainable Development. Telecommunications Policy, 45(7).

KPMG Advisory. (2024). Get your Data & Tech ready for the CSRD: Understanding the CSRD.

KPMG. (2024). Survey of Sustainability Reporting 2024.

Kammerer, R., Picard, N., & Lord, G. (2024). Internal controls: Building sustainability reporting on strong foundations. PwC.

Li, X., & Wu, J. (2022). Cyber Risk and Corporate ESG Performance. Journal of Cleaner Production, 350.

McKinsey. (2022). Why Cybersecurity Is Central to ESG.

National Institute of Standards and Technology (NIST). (2016). Guide for Cybersecurity Event Recovery (Special Publication 800-184).

NIST. (2024). NIST Cybersecurity Framework (CSF) 2.0.

NIST. (2020). SP 800-34 Rev.1 Contingency Planning Guide. National Institute of Standards and Technology.

OECD. (2021). Enhancing the Digital Security of SMEs.

Philippine Disaster Resilience Foundation (PDRF). (2023). MSME Guide to Disaster Resilience (Guidebook for micro, small, and medium enterprises).

PwC. (2023). ESG Reporting and Cyber Resilience.

PwC. (2024). Global CSRD Survey 2024: Preparing for the Corporate Sustainability Reporting Directive — ESG data, controls and reporting readiness.

Radanliev, P. et al. (2021). Supply Chain Cyber Risk and Resilience. Technological Forecasting & Social Change, 166.

Saaty, T. L. (1980). The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill.

Suttipun, M., Lakkanawanit, P., Saramolee, A., Yaacob, Z., & Srijunpetch, S. (2025). Environmental, Social, and Governance Disclosures and Market Reaction of Thai-Listed Companies in the Alternative Capital Market. Journal of Risk and Financial Management, 18(3), 113.

S&P Global. (2022). ESG Risks and Cybersecurity Exposure.

SASB. (2021). Cybersecurity Disclosure Guidance.

Shackleford, S. (2020). Managing Cyber Attacks in International Law.

TCFD. (2021). Guidance on Risk Management Integration.

Tsang, A., Frost, T., & Cao, H. (2023). Environmental, Social, and Governance (ESG) disclosure: A literature review. The British Accounting Review, 55(1), 101149.

UNIDO. (2022). Digital Transformation and SME Security Risks.

Vinogradova-Zinkevič, I. (2023). Fuzzy AHP and sensitivity analysis for decision problems with interdependent criteria. Applied Soft Computing, 132, 109884.

Więckowski, J., & Sałabun, W. (2023). Sensitivity analysis in multiple-criteria decision analysis: A systematic literature review. Expert Systems with Applications, 212, 118704.

WEF. (2022). Cyber Resilience in Global Value Chains.

WEF. (2023). Global Risks Report – Digital Risks.

World Economic Forum & Stockholm University (2024). Unpacking Cyber Resilience:Strengthening Defenses and Ensuring Operational Continuity (White Paper on Cyber Resilience).

Xu, H., & Zhang, Y. (2021). Disaster Recovery Capability and Firm Performance. International Journal of Production Economics, 235.

Yoon, S. (2022). Cybersecurity Investment and Corporate Reputation. Information & Management, 59(5).

Zhang, L. et al. (2023). ESG Governance and Information Security. Sustainability, 15(9).

Zurich Insurance. (2023). Cyber Insurance and SME Risk Mitigation.

3. 정부기관 및 연구기관

산업통상자원부, (2021), K-ESG 가이드라인 - 국내 ESG 정보공시 진단 항목 및 거버넌스 구성 체계.

중소·중견 벤처기업부. (2023). 중소·중견 기업 ESG 경영 지원 정책 백서.

한국인터넷진흥원(KISA). (2022). 중소·중견 기업 정보보호 수준평가 보고서.

한국인터넷진흥원(KISA). (2023). 2023년 지역 중소·중견 ·벤처기업 정보보호 실태조사 보고서.

한국인터넷진흥원(KISA). (2024). 국내 정보보호산업 실태조사. 한국정보보호산업협회.

한국표준협회(KSA). (2023). ESG 가이드라인과 정보보안 시스템 연계분석.

한국산업기술진흥원(KIAT). (2022). 스마트제조 확산에 따른 산업보안 대응 전략 보고서.

한국산업기술진흥원(KIAT). (2022). 스마트제조 보안 가이드라인.

한국거래소(KRX). (2025). 지속가능경영보고서 발간 확대 현황. KRX ESG 통계 자료 (2025 상반기 기준), 한국거래소 ESG 포털.

한국개발연구원(KDI). (2011). 공공사업 예비타당성조사를 위한 다기준분석(MCA) 지침.

『부록 : 설문지』

ESG 경영을 위한 중소·중견 기업 보안·DR 거버넌스 방법론 연구

안녕하십니까?
먼저 바쁘신 중에도 설문에 응해주심에 감사의 말씀을 드립니다.

저는 한성대학교 지식서비스&컨설팅대학원 스마트융합컨설팅학과에서 “ESG 경영을 위한 중소·중견 기업 보안·DR 거버넌스 방법론 연구”를 주제로 석사학위 논문을 준비중에 있습니다.

본 설문은 ESG 경영을 추진하는 제조 기반 중소·중견 기업의 정보보안(Security)과 재해복구(DR)/업무연속성(BCP)을 통합적으로 강화하기 위해, 무엇을 먼저 구축해야 하는지(우선순위)를 도출하고 실행 가능한 보안·DR 방법론(로드맵·지표 모델)을 제시하는 연구 목적으로 수행됩니다.
디지털 전환이 확산되면서 보안은 “침해 예방”을 넘어 사고를 전제로 한 복원력(resilience)과 업무연속성(continuity)까지 포함하는 관리체계로 확장되고 있습니다. 그러나 많은 중소·중견 기업은 인력·예산 제약으로 보안과 복구를 동시에 체계화하기 어렵고, 자원 배분을 위한 의사결정 기준이 부족한 실정입니다. 본 연구는 이러한 현실을 반영하여 현장 적용 가능한 우선순위와 실행 단위를 제시하는 데 초점을 둡니다.

본 설문은 AHP(Analytic Hierarchy Process) 방식으로 구성되며, 응답자께서는 보안 거버넌스, 기술적 통제, DR·복구역량, 정책·문서화·운영관리, 교육·인식·훈련 등 평가요소를 쌍대비교로 판단해 주시게 됩니다. 수집된 결과는 요소별 가중치 산출, 단계별 실행 로드맵 설계, ESG 공시·거버넌스 개선에 활용 가능한 지표(안) 도출에 활용됩니다.

본 설문을 통해 수집된 정보는 비밀을 유지하고 통계 목적으로만 활용될 것이며, 본 연구 목적 이외의 다른 용도로는 절대 사용하지 않을 것임을 약속드립니다. 귀하께서 답변하신 내용들은 모두 귀중한 연구 자료로 이용 될 것이므로 가능한 성실한 응답을 부탁드리며, 빠진 문항이 없도록 답변해주시길 부탁드립니다.
본 설문조사에 협조해 주심에 다시 한 번 깊은 감사를 드립니다.

2025년 10월

한성대학교 지식서비스&컨설팅대학원 스마트융합컨설팅학과
지도교수 : 원 종 혁
연 구 자 : 이 재 철
연 락 처 : 010-5321-7069
helpkorea2002@daum.net

『부록 A』 AHP 쌍대비교 문항 (총 25문항)

A-1. 응답 안내

본 설문은 AHP 방법론에 따라 동일 계층 내 요소를 2개씩 비교하는 쌍대비교 방식으로 구성되었다. 각 문항에 대해 “두 요소 중 상대적으로 더 중요한 요소”와 “그 중요도 정도”를 Saaty 1~9 척도로 응답한다(1=동일, 3=약간 중요, 5=중요, 7=매우 중요, 9=절대적으로 중요; 2·4·6·8은 중간값).

A-2. 전체 문항요약 (전체 : 25문항)

(1) 기준(Criteria) 비교: 10문항

(2) 세부지표(Sub-criteria) 비교: 15문항

A-2. 블록 A : 기준(Criteria) 간 쌍대비교(총 10문항)

(1) C1 : 보안 거버넌스

(2) C2 : 기술적 통제

(3) C3 : DR·복구역량

(4) C4 : 정책·문서화·운영관리

(5) C5 : 교육·인식·훈련

■ 질문 문항

문항 ID	비교쌍 (질문 문장)
A1	• C1(보안 거버넌스) vs C2(기술적 통제) 중, ESG 관점의 보안·DR 우선순위에 더 중요한 것은 무엇인가?
A2	• C1 vs C3(DR·복구역량) 중 더 중요한 것은 무엇인가?
A3	• C1 vs C4(정책·문서화·운영관리) 중 더 중요한 것은 무엇인가?
A4	• C1 vs C3(DR·복구역량) 중 더 중요한 것은 무엇인가?
A5	• C2 vs C3 중 더 중요한 것은 무엇인가?
A6	• C2 vs C4 중 더 중요한 것은 무엇인가?
A7	• C2 vs C5 중 더 중요한 것은 무엇인가?
A8	• C3 vs C4 중 더 중요한 것은 무엇인가?
A9	• C3 vs C5 중 더 중요한 것은 무엇인가?
A10	• C4 vs C5 중 더 중요한 것은 무엇인가?

A-3. 블록 B : 세부지표(Sub-criteria) 간 쌍대비교(총 15문항)

(1) C1 : 보안 거버넌스 하위 세부지표(3문항)

① S11 : 역할·책임(R&R) 및 책임자 지정

② S12 : 보안정책·규정 및 준수관리(문서화/개정/승인)

③ S13 : 사고대응 체계(보고·의사결정·커뮤니케이션)

■ 질문 문항

문항 ID	비교쌍 (질문 문장)
B1-1	• S11(R&R/책임자 지정) vs S12(보안정책·규정 관리) 중 더 중요한 것은 무엇인가?
B1-2	• S11(R&R/책임자 지정) vs S13(사고대응 체계) 중 더 중요한 것은 무엇인가?
B1-3	• S12(보안정책·규정 관리) vs S13(사고대응 체계) 중 더 중요한 것은 무엇인가?

(2) C2 : 기술적 통제 하위 세부지표(3문항)

① S21 : 접근권한·계정관리(공용계정 금지, 퇴사자 계정 회수 등)

② S22 : 패치·취약점 관리(주기, 예외 승인, 자산 식별)

③ S23 : 로그관리·모니터링(보관기간, 점검 주기, 관제 연계)

■ 질문 문항

문항 ID	비교쌍 (질문 문장)
B2-1	• S21(접근권한·계정관리) vs S22(패치·취약점 관리) 중 더 중요한 것은 무엇인가?
B2-2	• S21(접근권한·계정관리) vs S23(로그관리·모니터링) 중 더 중요한 것은 무엇인가?
B2-3	• S22(패치·취약점 관리) vs S23(로그관리·모니터링) 중 더 중요한 것은 무엇인가?

(3) C3 : DR·복구역량 하위 세부지표(3문항)

① S31 : 백업 정책(주기·보관·격리/오프라인)

② S32 : 복구절차 및 복구목표(RTO/RPO) 정의·운영

③ S33 : DR 테스트/모의훈련(정기성, 결과 조치, 개선 반영)

■ 질문 문항

문항 ID	비교쌍 (질문 문장)
B3-1	• S31(백업 정책) vs S32(복구절차·RTO/RPO 운영) 중 더 중요한 것은 무엇인가?
B3-2	• S31(백업 정책) vs S33(DR 테스트/모의훈련) 중 더 중요한 것은 무엇인가?
B3-3	• S32(복구절차·RTO/RPO 운영) vs S33(DR 테스트/모의훈련) 중 더 중요한 것은 무엇인가?

(4) C4 : 정책·문서화·운영관리 하위 세부지표(3문항)

① S41 : 표준운영절차(SOP) 및 기록관리(증적)

② S42 : 변경관리(Change Management) 및 구성관리(CM)

③ S43 : 공급망·협력사 보안관리(점검·계약·파일공유 통제)

■ 질문 문항

문항 ID	비교쌍 (질문 문장)
B4-1	• S41(SOP·기록관리) vs S42(변경·구성관리) 중 더 중요한 것은 무엇인가?
B4-2	• S41(SOP·기록관리) vs S43(공급망·협력사 보안관리) 중 더 중요한 것은 무엇인가?
B4-3	• S42(변경·구성관리) vs S43(공급망·협력사 보안관리) 중 더 중요한 것은 무엇인가?

(5) C5 : 정책·문서화·운영관리 하위 세부지표(3문항)

① S51 : 정기 보안교육(이수율, 직무별 커리큘럼)

② S52 : 실습형 훈련(피싱훈련, 랜섬웨어 대응 모의)

③ S53 : 인식 제고 활동(캠페인, 취약 사례 공유, 학습 문화)

■ 질문 문항

문항 ID	비교쌍 (질문 문장)
B5-1	• S51(정기 보안교육) vs S52(실습형 훈련) 중 더 중요한 것은 무엇인가?
B5-2	• S51(정기 보안교육) vs S53(인식 제고 활동) 중 더 중요한 것은 무엇인가?
B5-3	• S52(실습형 훈련) vs S53(인식 제고 활동) 중 더 중요한 것은 무엇인가?

『부록 B』 Criteria·Sub-criteria 코드 매칭표

B-1. AHP 요소 코드 매칭(Goal – Criteria – Sub-criteria)

구분	코드	명칭	영문명칭
Goal	G0	ESG 기반 중소·중견 기업 보안·DR 우선순위 도출	Goal
Criteria	C1	보안 거버넌스	Security Governance
Criteria	C2	기술적 통제	Technical Controls
Criteria	C3	DR·복구역량	DR/Recovery Capability
Criteria	C4	정책·문서화·운영관리	Policy/Documentation & Ops
Criteria	C5	교육·인식·훈련	Training & Awareness
Sub-criteria(C1)	S11	역할·책임(R&R) 및 책임자 지정	R&R/Accountability
Sub-criteria(C1)	S12	보안정책·규정 및 준수관리	Policy & Compliance
Sub-criteria(C1)	S13	사고대응 체계(보고·의사결정·커뮤니케이션)	Incident Response
Sub-criteria(C2)	S21	접근권한·계정관리	Access & Account Mgmt
Sub-criteria(C2)	S22	패치·취약점 관리	Patch/Vuln Mgmt
Sub-criteria(C2)	S23	로그관리·모니터링	Log & Monitoring
Sub-criteria(C3)	S31	백업 정책(주기·보관·격리/오프라인)	Backup Policy
Sub-criteria(C3)	S32	복구절차 및 RTO/RPO 운영	Recovery Process (RTO/RPO)
Sub-criteria(C3)	S33	DR 테스트/모의훈련	DR Test/Exercise
Sub-criteria(C4)	S41	SOP 및 기록관리(증적)	SOP & Evidence
Sub-criteria(C4)	S42	변경관리 및 구성관리	Change/Config Mgmt
Sub-criteria(C4)	S43	공급망·협력사 보안관리	Supply-chain Security
Sub-criteria(C5)	S51	정기 보안교육	Regular Training
Sub-criteria(C5)	S52	실습형 훈련(피싱/랜섬웨어 모의)	Practical Drill
Sub-criteria(C5)	S53	인식 제고 활동(캠페인·사례 공유)	Awareness Program

B-2. 설문 문항 인덱스 표(문항 ID ↔ 비교쌍)

■ 블록 A(기준 비교 10문항)

문항 ID	블록	계층	비교쌍(코드)	비교쌍(요소)
A1	A	Criteria	C1 vs C2	보안 거버넌스 vs 기술적 통제+
A2	A	Criteria	C1 vs C3	보안 거버넌스 vs DR·복구역량
A3	A	Criteria	C1 vs C4	보안 거버넌스 vs 정책·문서화·운영관리
A4	A	Criteria	C1 vs C5	보안 거버넌스 vs 교육·인식·훈련
A5	A	Criteria	C2 vs C3	기술적 통제 vs DR·복구역량
A6	A	Criteria	C2 vs C4	기술적 통제 vs 정책·문서화·운영관리
A7	A	Criteria	C2 vs C5	기술적 통제 vs 교육·인식·훈련
A8	A	Criteria	C3 vs C4	DR·복구역량 vs 정책·문서화·운영관리
A9	A	Criteria	C3 vs C5	DR·복구역량 vs 교육·인식·훈련
A10	A	Criteria	C4 vs C5	정책·문서화·운영관리 vs 교육·인식·훈련

■ 블록 B (기준 비교 15문항)

문항 ID	블록	계층	비교쌍(코드)	비교쌍(요소)
B1-1	B	C1	S11 vs S12	R&R/책임자 지정 vs 보안정책·준수관리
B1-2	B	C1	S11 vs S13	R&R/책임자 지정 vs 사고대응 체계
B1-3	B	C1	S12 vs S13	보안정책·준수관리 vs 사고대응 체계
B2-1	B	C2	S21 vs S22	접근권한·계정관리 vs 패치·취약점 관리
B2-2	B	C2	S21 vs S23	접근권한·계정관리 vs 로그관리·모니터링
B2-3	B	C2	S22 vs S23	패치·취약점 관리 vs 로그관리·모니터링
B3-1	B	C3	S31 vs S32	백업 정책 vs 복구절차·RTO/RPO 운영
B3-2	B	C3	S31 vs S33	백업 정책 vs DR 테스트/모의훈련
B3-3	B	C3	S32 vs S33	복구절차·RTO/RPO 운영 vs DR 테스트/모의훈련
B4-1	B	C4	S41 vs S42	SOP·증적관리 vs 변경·구성관리
B4-2	B	C4	S41 vs S43	SOP·증적관리 vs 공급망·협력사 보안관리
B4-3	B	C4	S42 vs S43	변경·구성관리 vs 공급망·협력사 보안관리
B5-1	B	C5	S51 vs S52	정기 보안교육 vs 실습형 훈련
B5-2	B	C5	S51 vs S53	정기 보안교육 vs 인식 제고 활동
B5-3	B	C5	S52 vs S53	실습형 훈련 vs 인식 제고 활동

『부록 C』 AHP 쌍대비교 설문 응답지 양식(배포용)

C-1. 응답 안내

본 설문은 AHP(Analytic Hierarchy Process) 쌍대비교 방식으로 구성됩니다. 각 문항에서 좌측 요소와 우측 요소 중 더 중요한 요소를 선택하고, 그 중요도 정도를 Saaty 1~9 척도로 표시해 주십시오.

- **1 : 동일하게 중요**
- **3 : 약간 더 중요**
- **5 : 중요**
- **7 : 매우 중요**
- **9 : 절대적으로 중요**
- **2·4·6·8 : 중간값(판단이 애매할 때 사용)**

C-2. 공통 응답지 작성 기준

문항 ID	좌측요소 (Left)	좌측이 더 중요함 (9 → 2)								동일 (1)	우측이 더 중요함 (2 → 9)								우측요소 (Right)	비고 (선택 근거)
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9		
A1	(C1)보안 거버넌스																		(C2)기술적 통제	

표기 방법 : “좌측이 더 중요”하면 좌측 영역(좌측 열)에 체크(✔), “우측이 더 중요”하면 우측 영역(우측 열)에 체크(✔)합니다. “1(동일)”은 가운데(동일) 칸에 체크합니다. 작성기준은 아래와 같습니다.

- **좌측이 더 중요하면 좌측(9~2) 중 1개 체크**
- **동일하면 1 체크**
- **우측이 더 중요하면 우측(2~9) 중 1개 체크**
- **체크는 반드시 1개만**

C-3. 기준(Criteria) 비교 (10문항)

문항 ID	좌측요소 (Left)	좌측이 더 중요함 (9 → 2)								동일 (1)	우측이 더 중요함 (2 → 9)								우측요소 (Right)	비고 (선택 근거)
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9		
A1	(C1) 보안 거버넌스																		(C2) 기술적 통제	
A2	(C1) 보안 거버넌스																		(C3) DR·복구 역량	
A3	(C1) 보안 거버넌스																		(C4) 정책·문서화·운영관리	
A4	(C1) 보안 거버넌스																		(C5) 교육·인식·훈련	
A5	(C2) 기술적 통제																		C3) DR·복구 역량	
A6	(C2) 기술적 통제																		(C4) 정책·문서화·운영관리	
A7	(C2) 기술적 통제																		(C5) 교육·인식·훈련	
A8	C3) DR·복구 역량																		(C4) 정책·문서화·운영관리	
A9	C3) DR·복구 역량																		(C5) 교육·인식·훈련	
A10	(C4) 정책·문서화·운영관리																		(C5) 교육·인식·훈련	

C-4. 세부지표(Sub-criteria) 비교(15문항)

(1) C1 : 보안 거버넌스 하위 세부지표(3문항)

문항 ID	좌측요소 (Left)	좌측이 더 중요함 (9 → 2)								동일 (1)	우측이 더 중요함 (2 → 9)								우측요소 (Right)	비고 (선택 근거)
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9		
B1-1	(S11) R&R/책임자 지정																		(S12) 정책·준수 관리	
B1-2	(S11) R&R/책임자 지정																		(S13) 사고대응 체계	
B1-3	(S12) 정책·준수 관리																		(S13) 사고대응 체계	

(2) C2 : 기술적 통제 하위 세부지표(3문항)

문항 ID	좌측요소 (Left)	좌측이 더 중요함 (9 → 2)								동일 (1)	우측이 더 중요함 (2 → 9)								우측요소 (Right)	비고 (선택 근거)
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9		
B2-1	(S21) 접근권한·계정관리																		(S22) 패치·취약점 관리	
B2-2	(S21) 접근권한·계정관리																		(S23) 로그·모니터링	
B2-3	(S22) 패치·취약점 관리																		(S23) 로그·모니터링	

(3) C3 : DR·복구역량 하위 세부지표(3문항)

문항 ID	좌측요소 (Left)	좌측이 더 중요함 (9 → 2)								동일 (1)	우측이 더 중요함 (2 → 9)								우측요소 (Right)	비고 (선택 근거)
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9		
B3-1	(S31) 백업 정책																		(S32) 복구절차·RTO/RPO	
B3-2	(S31) 백업 정책																		(S33) DR 테스트/훈련	
B3-3	(S32) 복구절차·RTO/RPO																		(S33) DR 테스트/훈련	

(4) C4 : 정책·문서화·운영관리 하위 세부지표(3문항)

문항 ID	좌측요소 (Left)	좌측이 더 중요함 (9 → 2)								동일 (1)	우측이 더 중요함 (2 → 9)								우측요소 (Right)	비고 (선택 근거)
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9		
B4-1	(S41) SOP·증적 관리																		(S42) 변경·구성 관리	
B4-2	(S41) SOP·증적 관리																		(S43) 공급망·협력사 보안	
B4-3	(S42) 변경·구성 관리																		(S43) 공급망·협력사 보안	

(5) C5 : 교육·인식·훈련 하위 세부지표(3문항)

문항 ID	좌측요소 (Left)	좌측이 더 중요함 (9 → 2)								동일 (1)	우측이 더 중요함 (2 → 9)								우측요소 (Right)	비고 (선택 근거)
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9		
B5-1	(S51) 정기 보안교육																		(S52) 실습형 훈련	
B5-2	(S51) 정기 보안교육																		(S53) 인식 제고 활동	
B5-3	(S52) 실습형 훈련																		(S53) 인식 제고 활동	

ABSTRACT

Research on security system methodologies for ESG management in small and medium-sized enterprises

LEE, Jae-Chul

Major in ESG Convergence Consulting

Dept. of Smart Convergence Consulting

Graduate School of Knowledge Service & Consulting

Hansung University

As ESG (Environmental, Social, and Governance) management rapidly enters a phase of institutional and market consolidation, information security and disaster recovery (DR) are being redefined not as peripheral IT operational issues but as core elements of control, accountability, and assurance within the Governance (G) pillar. In particular, the EU's Corporate Sustainability Reporting Directive (CSRD) expands both the scope and rigor of sustainability reporting and signals increasing sophistication in future assurance practices. Likewise, the ISSB's IFRS S1 requires companies to explicitly disclose the governance processes and control procedures they operate to manage sustainability-related risks and opportunities. Within this evolving regulatory environment, "security" is no longer limited to technical defense mechanisms; rather, it has become a governance practice under executive responsibility, encompassing risk

identification and management, minimization of operational disruption, and the preservation of data reliability (Directive (EU) 2022).

Despite this shift, small and medium-sized enterprises (SMEs) face structural constraints in embedding security and DR into their management systems at a pace commensurate with digital transformation. ENISA (2021) notes that SMEs are particularly vulnerable to external shocks such as supply-chain-based cyberattacks, and that deficits in awareness, budget, skilled personnel, and executive support accumulate as weaknesses in response and recovery capabilities. Furthermore, a recent study of Danish manufacturing SMEs reports that approximately one in five firms has experienced a cyberattack in recent years, indicating that security vulnerabilities in manufacturing SMEs are not isolated national anomalies but a recurring international phenomenon. In Korea as well, the rapid diffusion of smart factories has led to increasingly dense interconnections among data, equipment, and external access points; yet, in practice, investments in automation and datafication often coexist with the absence of security and DR measures or with merely formalistic implementations. This situation is better understood not as a simple technological gap, but as the cumulative result of governance deficiencies —namely in accountability, policy, control, training, and investment prioritization (ENISA, 2021).

Based on long-term experience in smart factory and ICT infrastructure deployment and consulting, the author has repeatedly observed how SMEs' perception of security as a "cost" or as a "post-incident remedial measure" manifests across corporate strategy, budgeting, and organizational structures. In ESG-related assurance and diagnostic engagements, security and business continuity indicators have also been shown to respond in a fragmented manner to the demands of rating agencies or client firms, rather than being standardized and systematically

linked to internal control frameworks. By contrast, larger enterprises tend to operate multi-layered security and DR governance structures, including ISMS-based management systems, incident response processes, backup and recovery mechanisms, and supply chain security requirements. As a result, disparities in security and DR governance maturity increasingly affect supplier evaluations and the continuity of business relationships. This trend aligns with the introduction and emphasis of the "GOVERN" function in NIST CSF 2.0, which explicitly connects cyber risk management to enterprise-wide risk management, underscoring the need for SMEs to reframe security and DR using the language of governance (NIST, 2024).

Against this backdrop, the present study aims to enhance the ESG performance of small manufacturing enterprises by reconfiguring security and DR from an integrated governance perspective and by proposing a methodology that is practically applicable under conditions of limited resources. First, the study synthesizes ENISA's SME security recommendations, the management system perspectives of NIST CSF 2.0 and ISO/IEC 27001, the contingency planning principles of NIST SP 800-34, and the diagnostic items of the Korean K-ESG Guidelines to structure security and DR vulnerabilities across five dimensions: organization, policy, technology, operations, and evidence. Second, the Analytic Hierarchy Process (AHP) is applied to quantify the relative importance of security and DR components, thereby deriving evidence-based investment priorities and a phased implementation roadmap. Third, based on the analytical results, the study proposes a set of security and DR governance indicators applicable to ESG disclosure and evaluation contexts. Fourth, a cyber resilience-based execution framework scalable to supply chain requirements is designed to enhance on-site applicability. In particular, from a supply chain risk perspective,

the framework examines approaches aligned with the supply chain-related category (GV.SC) of NIST CSF 2.0, thereby ensuring that supplier security requirements evolve beyond ad hoc requests into institutionalized governance processes (ENISA, 2021).

The significance of this study lies in supporting SMEs to achieve effectiveness not by attempting to rapidly replicate large-enterprise security and DR systems, but by adopting a phased approach grounded in governance maturity. The advancement of security and DR governance is likely to translate into tangible outcomes, including reduced risks of operational disruption affecting production, delivery, and quality; improved recovery time objectives (RTO) and recovery point objectives (RPO); enhanced data integrity; and increased reliability of ESG disclosures. Moreover, in an environment where supplier security maturity is increasingly a prerequisite for sustained participation in global value chains (GVCs), the methodology proposed in this study is expected to provide a practical foundation for mitigating ESG risks across supply chains and strengthening the sustainable management capabilities of domestic manufacturing SMEs (EU, 2022).