반응에서 대비로: 조직 회복탄력성으로의 전환

세계 유수의 파생상품 및 증권 거래소 네트워크 중 하나인 Cboe Global Markets의 수석부사장 겸 상임감사 책임자(CAE) 인 짐 엔스트롬(Jim Enstrom)에 따르면, 조직들은 잠재적 위험을 다루는 방식에서 전환기를 맞고 있다. 과거에는 위험관리 기능의 목표가 주로 업무 연속성(Business Continuity)에 있었고, 사건이 발생한 뒤 대응하며 가능한 한 빠르게 업무 운영을 복구하는 데 집중했다. 그러나 최근에는 조직 회복탄력성(Organizational Resilience)에 대한 강조가 커지고 있다. 이는 보다 포괄적이고, 선제적이며, 전략적인 접근으로, 변화하는 환경에서 조직이 더 유연하게 적응할 수 있도록 돕는다. 일상 업무 전반에 회복탄력성을 내재화해, 사전에 새로운 위협에 직면하기 대비하고 피해를 최소화하는 것을 목표로 한다.

조직 회복탄력성은 기술과 같은 내부 이슈뿐 아니라, 클라우드 솔루션과 핵심 제3자(중요 외부 공급업체) 벤더 등 외부 영역까지 보다 총체적으로 살펴본다. 엔스트롬은 "위험이 발생하기만을 기다리는 것이 아니라, 총체적이고 미래지향적인 접근을 취하는 것"이라고 말한다.

새로운 규제에 적응하는 일은 강화된 회복탄력성을 요구하는 대표적 변화이며, 회복탄력성 자체가 최근 일부 규정의 핵심 주제로도 자리 잡고 있다. 이번 Global Best Practices 에서는 이 분야의 새로운 규제를 검토하고, 한 기업의 적용 경험에서 얻은 인사이트를 공유하며, 더 큰 회복탄력성 필요에 대응하는 데 있어 내부감사 역할을 논의한다.

규제당국의 우려 확대

코로나19 팬데믹으로 업무 방식이 바뀐 경험은 회복탄력성에 대한 관심을 높이는 데 영향을 미쳤다. 엔스트롬에 따르면, 기업들은 이 주제에 대한 사고방식을 바꿔야 한다는 필요성을 인식했고, 규제당국은 기업들이 접근 방식을 강화하도록 요구하는 데 더욱 적극적이 되었다.

예를 들어, 유럽연합(EU)의 디지털 운영 회복탄력성 법(Digital Operational Resilience Act, DORA) 은 2025년 1월부터 집행(적용)되기 시작한 중요한 신규 법률로, EU 내 금융서비스 기업과 그 제3자 서비스 제공업체에 영향을 미친다. 또한 EU 밖에 있는 자회사와 서비스 제공업체에도 영향을 줄 수 있으며, 다양한 금융기관의 기술 보안 강화를 목표로 한다.

엔스트롬은 "현재 DORA는 운영 회복탄력성 관련 입법의 매우 중요한 사례"라고 말한다. DORA는 위험평가에 관한 우려를 다루는 동시에, 제3자(third-party) 고려사항과 현재 환경에서 보증(assurance)의 중요성도 언급한다.

엔스트롬은 DORA가 단순히 컴플라이언스에만 초점을 맞추는 것이 아니라, 보다 견고한 접근을 도입·정착시키는 과정에서 실질적인 위험관리 및 운영 가치를 얻을 기회를 제공한다고 설명한다. 과거 기업들이 직원들에게 사이버보안 위험과 피싱 시도 등 잠재적 리스크를 인지하는 중요성을 교육했던 것처럼, 오늘날에는 조직 전체 인력에게 회복탄력성과 그 가치를 선제적

으로 교육해야 한다고 강조한다.

> "전 세계적으로 사이버보안 규제가 수렴하는 가운데, DORA는 기업이 엄격하고 국제적으로 인정되는 운영 회복탄력성 기준의 새로운 시대에 적응해야 함을 보여주는 핵심 사례이다."
> – 아바니 데사이(Avani Desai), Schellman CEO,
> 「DORA Compliance Is a Strategic Necessity for U.S. Companies Serving EU Financial Institutions」

런던 기반 Cboe Global Markets의 펠릭스 알름그렌(Felix Almgren) 글로벌 운영리스크 총괄 및 유럽 리스크 총괄은 DORA가 본질적으로 원칙 중심(Principle-based) 이며 지나치게 세부적으로 규정된 규제는 아니지만, 기업들에게 위험과 운영 회복탄력성에 관한 모범사례 프레임워크를 도입·구축할 것을 요구한다고 말한다. 그는 자사의 준수(Compliance) 접근을 수립하는 과정에서 다음 프레임워크로부터 아이디어와 영감을 얻었다고 설명한다.

- COSO 전사적 위험관리(ERM) - 통합 프레임워크
- ISO 31000-2018: 위험관리 - 가이드라인
- ISO 22316-2017: 보안 및 회복탄력성 - 조직 회복탄력성 - 원칙 및 속성
- ISO 22301-2019 보안 및 회복탄력성 - 업무연속성관리시스템(BCMS) 요구사항

DORA 준수를 준비하기 위해 "전사적 위험관리 프레임워크와 운영 회복탄력성 프레임워크를 모두 검토해야 했고, 여기에는 거버넌스, 리스크 관리, 컴플라이언스(GRC) 솔루션도 포함됐다"고 그는 설명한다. DORA의 구현과 대비(Readiness)는 2024년 한 해 동안 ERM 및 IT 리스크 팀의 핵심 과제였다.

알름그렌의 경험에 따르면, 다음과 같은 모범사례가 프로세스 개선에 도움이 되었다.

- **유연한 GRC 솔루션 확보.** 새로운 프로세스로 사업부에 과도한 부담을 주지 않으면서도 프레임워크 구현을 촉진할 수 있어 **핵심적인 강점이 된다.**

- **적합한 데이터 구조와 워크플로우 설계 준비**는 의무화된 방법론 및 운영 회복탄력성 활동을 포함해 신규 규제를 충족할 수 있도록 데이터 구조·업무흐름을 마련할 준비가 필요하다.

기타 주요 규제 동향은:

- 영국 FCA 및 영란은행(Bank of England)의 PS21/3 '운영 회복탄력성 구축(Building Operational Resilience)' 2022년 3월 전면 시행함. 금융시장 부문을 대상으로 하며, 위협에 노출된 핵심 비즈니스 서비스를 식별하고, 영향 허용치(Impact Tolerance)를 설정하며, 의존성을 매핑하고, 스트레스 테스트를 요구하는 것이 주요 목적.

- 호주 CPS 230 '운영리스크 관리(Operational Risk Management)': 2025년 7월 1일 시행 예정임. 특정 규제 대상 금융기관이 운영리스크를 식별·평가·관리하고, 심각한 장애 상황에서도 핵심 운영을 유지하며, 서비스 제공업체와 관련된 위험을 효과적으로 관리하도록 요구함.

미국 증권거래위원회(SEC) 검사부(Division of Examinations)의 2025 회계연도 검사 우선순위 문서에서도, 다양한 시장 참여자에 영향을 미치는 위험 영역으로 정보보안과 운영 회복탄력성을 언급한다. SEC는 특히 사이버보안, 고객정보 보호, 신원 도용 식별 및 대응과 관련된 이슈를 구체적으로 언급한다.

> 미국 조직의 52%는 위험 및 회복탄력성 역량·책임·조직구조를 통합하지 못하고 있다.
> – 2025 KPMG Risk & Resilience Survey

알름그렌은 "규제당국과 핵심 이해관계자 입장에서 시스템적 의존성(Systemic Dependencies)에 대한 우려가 커지고 있다"고 말한다. 과거에는 온프레미스(사내) 서버에 의존하던 기업이 많았지만, 이제는 서비스 제공 전반에 다양한 공급망이 얽혀 있다는 것이다. 그는 또 "조직에 중대한 운영 사고가 발생했을 때 그 영향은 단일 기업에만 국한되는 경우가 매우 드물다"며 "시장 문제나 산업 전반의 문제로 이어질 수도 있다"고 덧붙인다. 예로 그는 작년에 보안 소프트웨어 벤더 CrowdStrike의 실패한 소프트웨어 업데이트로 발생한 장애를 들며, 항공·금융서비스·의료 등 다양한 조직과 산업에 광범위한 혼란을 초래했다고 설명한다.

회복탄력성 강화의 동력

회복탄력성을 가능하게 하는 자원은 무엇일지에 대해 엔스트롬은 IIA의 Three Lines Model(3선 모델)을 언급한다.

- 1선(경영/관리 라인)은 의존성과 제3자 관련 위험을 포함해 위험 프로파일을 이해하는 데 집중해야 함.
- 2선은 경영진이 견고한 위험평가 프레임워크를 이해하고 적용하도록 지원해야 하며, 1선과 2선 모두 정책과 절차를 평가해야 함.

알름그렌은 조직 회복탄력성으로 초점을 전환하는 가치가, 경영진과 이사회가 수용 가능한 수준(Comfort Level) 과 취약성 인식(Perceived Vulnerability)을 놓고 대화하도록 격려하고, 이를 해결하는 데 드는 다양한 비용과의 균형을 논의하게 한다는 점이라고 말한다. 회복탄력성 강화에는 시간과 비용의 투자가 필요하므로, 경영진과 이사회의 전폭적 지지가 핵심이다.
중요한 단계로는 엔스트롬에 따르면 제3자 벤더 관리 및 핵심 의존성과 같은 위험 영역에서 더 엄격한 관리가 필요한지 판단하는 것이 포함된다. 또한 새로운 규제의 초기 도입 단계에서 적절한 구현과 준수를 가능하게 하려면 역할과 책임(R&R)을 명확히 하는 것이 중요하다. 성과 지표를 정의하고, 사고 관리 테스트를 수행하면 프로그램의 건전성과 준비 상태를 모니터링할 수 있으며, 기술 인프라 개선 가능성도 검토할 수 있다.
3선(내부감사)의 기여는 다음과 같다.

- **준수(compliance) 관련 테스트 서비스 제공**: 예컨대 DORA는 독립적 검토와 보증을 규정하며, 정보통신기술(ICT) 리스크 관리 프레임워크에 대한 감사를 요구합니다. 또한 ICT 거버넌스 평가, ICT 제3자 관리에 대한 책임성, 그리고 핵심 ICT 감사 지적사항의 개선조치(Remediation)를 모니터링·확인하기 위한 관련 보고 및 후속조치 프로세스에서 내부감사의 역할을 강조한다.

> 많은 기업이 공급망 강화나 사이버 위협 대응처럼 중요하지만 방어적인 조치를 취하는 데 그치고, 대비 태세를 보다 포괄적으로 바라보지 못하고 있다. Resilience Pulse Check 설문에 따르면, 기업 중 단 13%만이 회복탄력성 핵심성과지표(KPI)를 전략에 포괄적으로 반영하고 있으며, 이는 회복탄력성이 전략 이슈라기보다 운영 이슈로 인식될 가능성을 시사한다.
> –「Deploying Resilience for Success in a Volatile World」, 세계경제포럼(WEF)

- **리스크 및 내부통제**에 대한 전문성을 바탕으로, 경영진에 **적절한 정책·절차**와 **대비상태(Readiness) 점검**에 대해 자문 제공
- **회사 위험 프로파일**과 위협 감시 목록(Watch List) 평가
- 사고 대응 계획(Incident Response Planning)에 대한 **자문 또는 보증 제공**
- **도입 후 검토(post-implementation review) 수행**: 기업이 합리적으로 준수를 보장하기 위해 변경한 사항에 대한 보증 제공
- **회복탄력성 강화를 위한 변화 필요성에 대한 옹호**: 경영진과 이사회가 운영 회복탄력성을 강화하도록 촉구하고 도전 과제를 제시

미션 크리티컬한 노력

엔스트롬은 규제가 위험을 초래할 수 있지만, 동시에 문제 해결을 위한 프레임워크를 제공하는 비즈니스 조력자(Enabler) 가 될 수도 있다고 말합니다. 규제 적용 대상이 아닌 기업도, 해당 규정의 권고사항을 활용해 운영을 개선할 수 있다는 것이다.
현재 환경에서 엔스트롬은 "회복탄력성을 갖추는 것은 미션 크리티컬한 목표"라고 말한다. "사건이 발생했을 때의 반응적 복구에 의존하기보다, 전략적 의사결정에서 운영 원칙에 대한 지속적 인식을 유지해야 한다는 '지속적·상시적 필요'를 더 비판적으로 고민하는 일"이라는 것이다.
내부감사인은 보다 전략적인 관점을 수용하는 조직에, 필요한 객관적이고 신뢰할 수 있는 정보와 조언을 제공할 수 있는 독보적인 위치에 있다.

역량을 키우고 있는가?

회복탄력성은 부분적으로 기술 역량을 갖춘 인력에 달려 있다. 그러나 세계가 점점 더 디지털화되면서, 미국 기업은 역량 격차(Skill Gap)를 겪을 수 있다고 기술기업 Jack Henry & Associates의 부사장 겸 최고리스크책임자(CRO)인 찰리 라이트(Charlie Wright)는 말한다. 기업들이 사이버보안, 암호화폐, 인공지능 관련 과제에 대응하는 가운데, 거대 기술기업과 자금력이 풍부한 기업들이 기술 인재를 빠르게 흡수하고 있다는 것이다.
그렇다면 기업의 민첩성(Agility)을 유지하는 데 도움이 되는 기술 역량을 어떻게 끌어올릴 수 있을까? 라이트는 현직 직원에 대한 기술 교육과 역량 개발을 강화하는 것이 해답이라고 말한다. 또한 이 과정에서 내부감사 기능은 인사(HR) 기능—교육 프로그램, 채용, 유지(Retention) 노력 등을 포함—을 감사할 수 있도록 새로운 역량을 개발해야 하며, 이를 통해 조직이 미래 성공에 필요한 역량을 갖추고 있는지 확인할 수 있다고 설명한다.
IIA는 감사인의 기술 지식 향상을 돕기 위해 Cybersecurity Topical Requirement, AI Auditing Framework, AI Knowledge Center 등 여러 도구를 제공하고 있다.