2026.11.23.

KiRi 리포트

| 글로벌 이슈 |

EU 디지털 운영 복원력법(DORA) 시행과 보험산업 영향

김유미 연구원

요 약

EU의 디지털 운영 복원력법(DORA)이 2025년 1월부터 적용되면서 보험회사의 사이버 위험관리와 IT 서비스 중단 대응 의무가 강화됨. 이에 보험회사들은 중대 ICT 사고 보고, 복원력 테스트, 외부 IT업체 관리 등에 따른 비용과 실무 부담 완화를 요구하고 있음. 한편 일부 유럽 보험회사들은 기존 정보보안 인증 활용, IT 관리 체계 정비, AI 기반 규제 점검 기술의 시험 적용 등을 통해 대응 역량을 강화하고 있음

○ EU 디지털 운영 복원력법(Digital Operational Resilience Act; DORA)은 금융권 정보통신기술(ICT) 리스크 관리, 중대 사고 보고 등을 의무화한 규제로 시행 2년 차를 맞아 이행 경험 축적과 규제 간소화 논의가 본격화됨[1)]

- 국가와 업권별로 달랐던 ICT 위험관리 규제를 통일하고 제3자 ICT 리스크 관리(Third Party Risk Management; TPRM)를 포괄적으로 수행하도록 하며, 은행, 보험, 암호화폐 사업자 및 핵심 ICT 공급자 등 EU 국가의 약 22,000개 기관에 적용됨[2)]
- 2023년 발효 후 2025년 1월부터 시행되었으며, 이중 보고 등에 따른 축적된 실무 부담을 완화하고자 2025년 11월 유럽집행위원회의 디지털 옴니버스 제안에 따라 사고 보고를 일원화하는 단일 EU 허브를 신설하는 등 제도적 보완이 추진됨[3)]
- 최근 유럽감독기구(ESAs)는 글로벌 빅테크 등 19개 핵심 ICT 공급자를 지정하였으며, 합동검사팀을 구성하여 본격적인 검사 및 감독 절차를 개시함[4)]

○ DORA의 5대 핵심 규제 요건은 금융 서비스 전반에 걸쳐 ① ICT 리스크 관리 체계 수립, ② 사고 탐지 및 보고, ③ 디지털 운영 복원력 테스트, ④ 제3자 ICT 리스크 관리 및 감독, ⑤ 정보 공유 체계 마련임

- 이사회와 경영진이 디지털 운영 복원력에 대한 최종 책임을 지며, 기존 Solvency Ⅱ의 내부통제 체계와 업무영향 분석을 바탕으로 계리·언더라이팅 등 핵심 업무시스템의 ICT 리스크를 체계적으로 관리해야 함
- 보험금 청구 지연, 계리 시스템 장애 등이 중대 ICT 사고로 분류될 경우, 사고 분류 시점부터 4시간 내 최초 통보, 최초 통보 후 72시간 내 중간 보고, 중간 보고 후 1개월 내 최종 보고를 단계적으로 수행하고 신속한 복구 조치를 이행해야 함
- 취약점 점검을 정례화하고 감독당국이 지정한 금융회사는 3년마다 위협 중심 모의 침투 테스트(Threat-Led

1) European Union(2022. 12. 27.), "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations"
2) Sopra Steria(2024), "One year after, the Digital Operational Resilience Act (DORA) came into force: Initial lessons learned"
3) European Commission(2025. 11. 19.), "Proposal for a Regulation of the European Parliament and of the Council (Digital Omnibus)"
4) ESAs·EBA·EIOPA·ESMA(2025. 11. 18.), "The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act"

Penetration Testing; TLPT)를 실시해 방어 역량을 검증해야 하며, ICT 공급자 외부 의존도 통제를 위한 계약 정보 등록부와 실효적 출구 전략을 마련해야 함

- 금융 생태계 전반의 사이버 리스크 전이를 선제적으로 억제하기 위해, 신뢰할 수 있는 금융기관 간 최신 해킹 수법과 취약점 등 사이버 위협 정보를 안전하게 교환하는 자발적인 협력 체계 참여를 장려하고 있음

○ DORA의 규제 요건은 보험회사의 규모와 위험 수준에 따라 차등 적용됨[5)]

- 보험업은 장기계약 관리로 축적된 방대한 데이터를 처리하고 기존 전산시스템과 최신 클라우드가 혼재된 복잡한 IT 환경에서 생명·건강 정보, 재무 상태, 사고 이력 등 보험계약자의 민감한 개인정보를 대량으로 보유함
- 이러한 특성으로 인해 시스템 장애나 정보 유출 시 제재 및 평판 훼손 위험이 크며, 기존 건전성 규제인 Solvency Ⅱ에 더해 DORA에 따른 ICT 사고 보고와 디지털 운영 복원력 테스트 등 구체적인 의무가 부과됨
- Solvency Ⅱ 적용 보험·재보험회사는 원칙적으로 일반 규제를 적용받고 소규모 연금기관은 간소화된 ICT 리스크 관리 체계를 적용받으며, 중소형 이하 보험중개인 및 Solvency Ⅱ 미적용 소형 보험회사는 규제 대상에서 제외됨

○ 보험회사는 핵심 ICT 서비스 제공업체에 대한 높은 의존도와 복잡한 규제 준수 절차로 인해 실무 부담과 비용이 증가하고 있으며, 이에 유럽보험협회를 중심으로 규제 간소화 및 제도 개선 요구가 제기되고 있음

- 계약 정보 등록부 관리 등 수작업에 의존하는 행정적 부담이 가중되고 있으며, 이미 국제 인증이나 합동 검사를 통과한 주요 IT 공급자에 대해서도 개별 보험회사가 반복적으로 자체 감사를 수행해야 하는 등 중복 업무와 비용이 발생하고 있음[6)]
- 유럽보험협회는 이중 보고 등 실무 부담을 완화하기 위해 사고 보고 기준의 합리적 상향 및 보고 창구 일원화를 제안하고 공신력 있는 외부 인증 및 합동 검사 결과를 활용해 보험회사의 자체 감사 의무를 대체할 것을 권고함[7)]
- 또한 ICT 공급자와의 협상력 제고를 위한 EU 표준 계약서 도입과 그룹 내부 IT 제공자에 대한 유럽 네트워크 정보보안 지침(Network and Information Security Directive 2; NIS2) 등 타 지침과의 이중 규제 해소를 핵심 과제로 제시함

○ 일부 유럽 보험회사들은 DORA 시행에 대응해 기존 보안 인증을 활용하고 통합 IT 관리 플랫폼을 구축하며 AI 기반 규제 점검 기술을 시험하는 등 디지털 운영 복원력 관리 체계를 정비하고 있음

- 벨기에 AG 보험회사는 기존 정보보안 국제표준(ISO 27001)을 활용해 DORA 요건과의 차이를 점검하고, 전사 전담팀과 부서 간 협업체계를 구축해 규제 준수에 따른 부담을 줄이고 ICT 리스크 관리 체계를 정비했다고 밝힘[8)]
- 이탈리아 제네랄리(Generali)는 DORA 규제 요건에 대응하기 위해 전사 IT 시스템 구조를 통합 관리하는 플랫폼을 활용하여 복잡한 외부 ICT 공급망의 연결 구조를 파악하고 컴플라이언스 관리 체계를 정비한 바 있음[9)]
- 독일 국가 AI 이니셔티브(MISSION KI)는 AI 기업 녹스투아(Noxtua) 및 알리안츠(Allianz)와 협력하여 제3자 ICT 공급자와의 데이터 교환 시 규제 준수 여부를 자동 검증하는 AI 컴플라이언스 점검 시스템을 시험 적용함[10)]

5) Regulation DORA, DORA for the Insurance Sector(https://www.regulation-dora.eu/insurance)
6) ESAs(2024), "Final report on draft RTS to specify the policy on ICT services supporting critical or important functions", p. 41; p. 49
7) Insurance Europe(2025), "Insurance Europe messages on the upcoming Digital Omnibus"
8) AG(2025. 1. 16.), "How IT helped AG prepare for DORA"
9) Orbus Software(2025), "Case study: Generali Italia: Transforming IT Architecture for Regulatory Excellence"
10) MISSION KI(2025. 7. 25.), "AI-based Compliance Checking System for Secure Data Exchange"