

AI 위험관리대장

AI Risk Register

문서 목적	AI 시스템의 위험, 통제, 개선조치와 잔여 위험을 담당자·기한 기준으로 추적
가상 대상	주식회사 노바웍스 · Nova Assist
문서 상태	공개 미리보기 · 실제 제출본 아님
검토 기준일	2026. 7. 21.

가상 서비스에 대한 공개 샘플입니다. 실제 위험등급과 통제 적정성은 기술자료, 운영기록과 담당자 인터뷰를 바탕으로 평가합니다.

01 · 주요 위험 현황

ID	위험 시나리오	영향/가능성	현재 통제	개선조치	담당/기한
R-01	부정확한 답변이 검토 없이 고객에게 전달	높음 / 중간	상담원 승인·자동발송 차단	고위험 질문 이중 승인	Product / Q3
R-02	문의에 포함된 개인정보가 외부 모델로 과다 전송	높음 / 낮음	민감정보 필터·학습 미사용	차단 테스트 월별 수행	Security / 8월
R-03	고객별 검색 문서 접근권한 분리 실패	높음 / 낮음	테넌트 ACL·감사로그	침투시험 시나리오 추가	Platform / Q3

02 · 조치 추적과 잔여 위험 승인

위험 ID	증빙	진행 상태	잔여 위험	승인·재검토
R-01	승인 로그 표본·운영 가이드	진행 중 · 70%	중간	AI 책임자 · 2026 Q4
R-02	필터 테스트·DPA·설정 캡처	완료	낮음	보안책임자 · 분기 검토
R-03	ACL 설계서·접근 로그	진행 중 · 50%	중간	CTO · 시험 후 승인