

예시 합성 데이터 / 제출 준비 초안

금융권 취약점 분석·평가
제출 준비 보고서

취약점 분석·평가 결과 및 보완조치 이행계획 준비자료

공식 평가·인증·접수 완료 문서가 아닙니다. 기준 매핑·추가 자료·검토와 승인이 필요합니다.

구분	내용
보고서 ID	DEMO-shop-20261020-financial-v1.0
사이트	가상 쇼핑몰 / shop.example
진단 회차·환경	2026-10-20 10:30 KST / 스테이징
제출·심사 경로	법정 보고: 금융위원회 / 실무 제출: 해당 금융감독원 보고 절차 확인
점검 범위	로그인·주문 승인 API와 결제 페이지의 합성 시나리오
제외 범위	운영 DB, 서버 설정, 조직·물리 보안
프로파일 버전	guardian-submission-demo-v1.0

진단 결과 요약

취약 1건 / 미확인 1건 / 양호 1건 / 공식 기준 연결: 전체 검토 필요

세부 ID	확인 항목	진단 판정	조치 상태
PAY02-03	거래 전문 재사용 방지	취약	조치 예정
IAM03-01	고객별 접근 권한	미확인	추가 자료 필요
PAY01-01	서버 결제 금액 검증	양호	검증 유지

전자금융업무의 대상 시설·조직·내부통제·사고 대응까지 평가 범위를 확인해야 합니다.

555점은 가디언 자체 지표입니다. 기관의 공식 평가점수·기준 충족 판정으로 환산하지 않습니다.

추가 제출 준비사항

전체 전자금융기반시설 자산 목록, 조직·내부통제 증빙, 평가 수행 요건, 책임자 검토·승인, 현행 전산 제출 양식

검토자·승인자: 미지정 / 검토·승인: 미완료 / 원문 양식 버전: 현행 확인 필요

1. 거래 전문 재사용 방지 / PAY02-03

항목	내용
판정·위험	취약 / 높음
점검 근거	SHOP-1020-E01 / 합성 전문을 재전송했을 때 별도 작업 두 개가 생성됨
개선안	업무 범위를 포함한 맥등 키와 원자적 중복 판정을 적용
재점검 기준	격리 환경에서 재전송·동시 요청 후 중복 작업 여부 확인
담당·기한	결제 개발팀(예시) / 2026-10-23
조치 상태	조치 예정
기관 기준 연결	공식 ID 미매핑. 관련 기술 증빙 후보이며 원문 버전·항목·대응 범위의 검토가 필요합니다.

2. 객체별 접근 권한 / IAM03-01

항목	내용
판정·위험	미확인 / 미산정
점검 근거	SHOP-1020-E02 / 비인증 요청은 거부했으나 다른 가맹점 역할의 테스트 계정이 없음
개선안	합성 가맹점 B와 읽기·변경·반출 테스트 역할 연결
재점검 기준	가맹점 간 객체 접근을 작업별로 비교
담당·기한	인증 개발팀(예시) / 2026-10-24
조치 상태	추가 자료 필요
기관 기준 연결	공식 ID 미매핑. 관련 기술 증빙 후보이며 원문 버전·항목·대응 범위의 검토가 필요합니다.

3. 서버 결제 금액 검증 / PAY01-01

항목	내용
판정·위험	양호 / 해당없음
점검 근거	SHOP-1020-E03 / 서버 주문 금액과 다른 합성 결제 요청 거부, 상태 변경 없음
개선안	결제 어댑터 변경 시 회귀 검증 유지
재점검 기준	금액·통화 변경 합성 요청이 거부되는지 확인
담당·기한	결제 개발팀(예시) / 해당없음
조치 상태	검증 유지
기관 기준 연결	공식 ID 미매핑. 관련 기술 증빙 후보이며 원문 버전·항목·대응 범위의 검토가 필요합니다.

참고 근거

전자금융거래법 제21조의3·전자금융감독규정 제37조의2

공식 자료 열기

출처 확인일: 2026-10-20 / 실제 제출 전 현행 기준·양식 확인