경영유의사항 등 공개안

1. 금융기관명 : 악사손해보험㈜

2. 조치일 : 2025. 11. 11.

3. 조치내용

제재대상	조치내용
기 관	경영유의사항 1건, 개선사항 3건

4. 조치대상사실

가. 경영유의사항

(1) 제3자 서비스 관리체계 강화 필요

회사는 핵심업무에 대한 역량 집중 및 전자금융거래 업무 등의 효율적 운영을 위하여 다수의 외부 전문업체와 제휴 및 정보처리위탁 계약을 맺고 있으며, 2024.1월 제3자 서비스를 포함한 서비스 영향도 기준을 수립하는 등 제3자 위탁·제휴 서비스를 관리하기 위해 지속적으로 노력하고 있다.

하지만 제3자 서비스에 대한 상세 관리 기준 및 관리 체계, 총괄 관리부서가 부재한 상태로 외부 업체와 계약을 수행한 각 부서에서 해당 업체에 대한 관리를 개별적으로 수행하고 있다.

이로 인해 제3자 서비스 전체 현황 및 관련 전자금융거래 서비스, 단일 장애지점*, 제3자 서비스 장애 발생시 업무 영향도, 제3자 리스크 관련 문서**, 대체수단 등이 체계적으로 관리되지 않고 있다.

* 대체수단이 제공되지 않아 해당 기능 중단시 주요 전자금융업무에 영향을 주는 요소
** 리스크관리 활동 내역, 위탁 관련 의사결정사항, 실사 결과 등 주요사안

또한, 회사는 인증 및 결제 업무를 위해서 A, B 등과 정보처리업무 위탁계약을 체결하였는데, ITO(IT Outsourcing) 위탁 계약 등 일부 계약서에 감독당국의 감독·검사

수용의무 항목 등이 누락*되어 있고 구매·계약 관련 내규에도 동 항목이 필수로 포함되도록 규정하고 있지 않다.

* ITO 위탁기준 "IT 통합유지보수 계약서(C)" 및 "용역계약서(D)" 등 개별유지보수계약

아울러, 회사는 IT감사 업무를 위해 「감사업무 세부지침」 제3조 등에 따른 IT감사(일반·일상·특별) 및 「IT 자체프로세스점검 지침」 제2조 등에 따른 자체감사(정기·특별)를 구분하고 이를 위해 IT부문 감사조직을 E팀(◎명) 및 F팀(◉팀)으로 구성하여 운영하고 있다.

하지만 검사대상 기간(2022.1.1.~2025.4.4.) 중 외부주문 업체에 위탁한 업무*의 적정성 등에 대하여 IT감사 및 자체감사를 하지 않았다.

* (D, 2024.9.30. 계약 종료) IT개발운영 유지보수 등
(G, 2024.9.30. 계약 종료) 인프라 운영업무 위탁 등
(C) IT 개발 운영 및 인프라 유지보수 등

<조치할 사항>

따라서 회사는 제3자 서비스 총괄 관리부서 지정 및 제3자 서비스 계약 절차 등 관리 체계를 마련하여 단일 장애지점을 식별·관리하고 제3자 리스크 관련 문서를 집적하며, 계약시 필수항목이 누락되지 않도록 내규에 반영하고 서비스 영향도 기준에 따라 모든 제3자 서비스를 체계적으로 관리하는 등 제3자 서비스 관리를 강화하여 운영하시기 바랍니다.

또한, 외부주문 업무를 포함하여 감사계획을 수립 및 실시하는 등 외부주문 업체에 대한 업무 적정성 등 관리를 강화하여 운영하시기 바랍니다.

나. 개선사항

(1) 외부 연계기관 통신회선 연결 미흡

회사는 2024.1월 업무 및 서비스의 중요도에 따라 이중화, 재해복구시스템 등의 구축 여부를 결정하기 위한 전산시스템 구축 기준을 마련하였고, 동 기준에 따라 제3자 서비스에 대한 통신회선 이중화 구축 여부 등을 결정·운영하도록 하고 있다.

하지만 상기 기준 마련 전에 구축한 제3자 서비스의 경우 일부 중요 제3자 서비스를 단일 통신회선으로 구성하거나 회사 주전산센터로만 통신회선을 연결함에 따라, 통신

회선에 장애가 생기거나 재해 등으로 회사 재해복구센터로 전환·운영 시 업무연속성이 보장되지 못할 우려*가 있다.

* 단일회선 연결 : H(휴대폰인증), I(카드결제 등) 등
재해복구센터 미연결 : A(신용카드번호 위탁 저장 및 토큰 생성, 신용카드 인증), J(카카오인증), H(휴대폰인증), I(카드결제 등) 등

<조치할 사항>

따라서 회사는 제3자 서비스 구축 시에도 전산시스템 구축 기준에 따라 중요도 판단 및 통신회선 이중화, 회사 재해복구센터로의 통신회선 연결 등을 검토·결정하는 절차를 추가하고, 동 절차에 따라 기 구축한 제3자 서비스에 대해서도 통신회선 이중화, 회사 재해복구센터 통신회선 연결 필요성 등을 재검토하는 등 외부 연계기관과의 통신회선 연결을 강화하여 운영하시기 바랍니다.

(2) 제3자 서비스 관련 비상대책 및 재해복구전환훈련 미흡

회사는 그룹의 업무지속성확보 전략에 따라 IT서비스 업무연속성 확보방안을 수립하였고, 연 1회 재해복구전환훈련을 실시하고 있다.

하지만 IT서비스 업무연속성 확보방안에 제3자 서비스 장애 등에 대한 대응방안[1] 및 재해복구절차 등 주요 절차[2]가 상세히 마련되어 있지 않고 비상연락망 등 중요 정보[3]가 현행화되어 있지 않는 등 IT서비스 업무연속성 확보방안이 전반적으로 미흡하므로 재검토하여 수립할 필요가 있다.

또한, 재해복구전환훈련 시 제3자 서비스에 대한 연계 훈련을 실시하지 않았으며, 웹·모바일앱에 대해서는 재해복구전환훈련 시 웹페이지·앱 접속 테스트만 실시하고 계약조회, 보험료 계산 등 내부 기능을 테스트하지 않는 등 재해복구전환훈련을 미흡하게 실시하였다.

1) 카드 결제 제3자 서비스(K, I)를 대외계시스템에서 현재 50:50 비율로 배분하고 있으나, 제3자 서비스 장애 시 설정 변경 등 관련 절차 부재,
B(계좌주조회, 계좌이체 서비스 등) 통신회선 장애시 재해복구센터 통신회선 전환 절차 부재, 재해복구센터 전환시 각 제3자 서비스 기관에서 악사손보 대외계시스템 IP 변경 등 조치 필요하나 제3자 서비스 비상연락망 및 관련 절차 부재 등
2) 재해선포절차, 재해복구시스템 구동 절차, 정상시스템 전환 절차 등 미흡
3) 외부 업체 담당자, 책임자 및 본사 대체 근무장소 등 현행화 미흡

<조치할 사항>

따라서 회사는 2025.1월부터 수행중인 「업무연속성확보방안 수립 컨설팅」을 통해 업무영향분석을 실시하여 핵심업무를 도출하고, 핵심업무에 대해 목표시간 내 복구가 가능하도록 업무연속성 확보방안을 수립하며, 재해복구 절차 및 제3자 서비스 장애 등에 대비한 비상대책도 상세히 마련하시기 바랍니다.

또한, 업무연속성 확보방안에 따라 매년 비상대응훈련을 실시하며, 웹·모바일앱의 내부 기능을 테스트하고 핵심업무에 대해서는 외부 연계 테스트도 실시하시기 바랍니다.(대외기관 지원이 불가한 경우 유사 환경 구조로 대체하여 훈련 실시)

(3) 프로그램 변경통제 절차 미흡

회사는 내규 「어플리케이션유지보수지침서」 및 「형상관리지침서」에 따라 프로그램 변경 시 형상관리 시스템을 통해 개발의뢰자의 테스트 내용을 기록·관리하고, 운영시스템에 이관하고 있다.

하지만 프로그램 변경·테스트 업무를 수행함에 있어 개발의뢰자의 테스트 및 결과 자료 관리, 제3자에 의한 검증이 다소 미흡*하고

* 테스트 후 작성한 테스트 결과서가 미흡하게 작성되었거나 테스트 결과서가 형상관리 시스템에 등록되지 않은 사례, 일부 프로그램 변경 후 제3자 검증에 대한 증적이 미흡한 사례 등

감사부서는 프로그램 변경통제 관련 절차 준수 여부를 위주로 감사하고 프로그램 변경통제 업무의 적정성에 대한 감사는 미흡*하게 운영되고 있다.

* IT검사 업무편람에 업무 담당자별 직무만 명시되어 있고, 프로그램 변경통제 적정성 관련 세부 점검항목 부재

<조치할 사항>

따라서 회사는 테스트 결과서 작성 방법 및 기준 등 테스트 관련 매뉴얼을 수립하고 작성 대상자(현업 및 개발담당자)에게 전파교육을 시행하는 등 테스트 관련 업무 절차를 강화하시기 바랍니다.

또한, IT감사 업무편람에 프로그램 변경통제 적정성을 점검할 수 있도록 세부 점검 항목을 추가하고, IT자체감사 시 프로그램 등록·변경·폐기 절차 및 업무의 적정성이 검증되었는지 여부를 주기적으로 점검하는 등 프로그램 변경통제에 대한 점검을 강화하시기 바랍니다.