경영유의사항 등 공개안

1. 금융기관명 : 상호저축은행중앙회

2. 조치일 : 2022. 3. 3.

3. 조치내용

대상	내용
기 관	개선사항 10건

4. 조치대상사실

가. 개선사항

(1) IT감사 실무조직 및 감사업무 미흡

회사는 내규에 감사실을 감사보조인으로 규정하고 있고 감사실 직원의 자격요건을 규정하고 있으나,

IT감사자의 자격요건이 내규에 명시되어 있지 않고, 외부기관의 감사 수감을 이유로 정기감사(매 1년)를 생략하고 있으며, 감사실 IT감사자 1명이 현업업무와 IT업무 감사를 겸임하고 있어 IT감사 업무가 충실히 이행되지 않을 우려가 있으므로

IT감사자의 자격요건, 정기감사 생략기준을 내규에 마련하고, IT감사 인력을 충원하는 등 IT부문에 대한 감사업무를 강화하시기 바람

(2) IT사업 관련 계약업무 관리절차 개선

㈎ IT사업 추진시 타당성검토 미흡

회사는 ○○○○.○.○.~○○○○.○.○. 기간 중 ◇◇◇ 구축사업을 추진하면서 사업범위에 부속된 과업이라는 이유로 별도의 사업 타당성 검토절차 없이 수의계약을 체결한 사례가 있는 등 IT사업 추진시 타당성 검토가 미흡하므로

IT사업 추진시 사업범위에 부속된 과업 수행을 위한 계약 건에 대해서도 제3자가 계약내용 등에 대한 사전 타당성 검토를 실시하도록 관련 업무절차를 개선하시기 바람

㈏ 외주계약 연장시 타당성 검토 미흡

회사는 내규에 따라 계약 종료시 기존 계약과 계약조건이 동일한 경우 기존 계약을 연장하고 있으나,

회사가 저축은행의 홈페이지 취약점 분석·평가를 위해 선정한 업체의 계약 연장시 업체 변경 또는 추가 등의 검토를 수행하지 않아 개별 저축은행의 홈페이지 취약점 분석·평가의 실효성이 저하될 우려가 있으므로

외주업체와 체결한 기존 계약 연장시 해당 업체의 재무건전성 및 서비스 품질 수준의 적정성 등에 대한 검토를 수행하도록 관련 업무절차를 개선하시기 바람

(3) 개별 저축은행의 이기종 시스템 관리대책 마련

회사의 □□□시스템을 이용하는 저축은행(○○개사) 중 ○○% 이상(○○개사)이 자체 운영중인 이기종 시스템을 □□□시스템과 연계하여 운영(○○개사)하거나 개별적으로 운영(○개사)하고 있으나

개별 저축은행의 경우 예산·인력 등 IT부문 인프라 부족으로 이기종 시스템에 대한 안전성이 확보되지 않아 보안사고로 인한 금융소비자 피해 발생 소지가 있으므로

개별 저축은행의 IT인프라 운영실태를 파악하여 저축은행의 이기종 시스템에 대한 통합 관리계획을 마련하여 운영하시기 바람

(4) 프로그램 변경 통제체계 개선

㈎ 프로그램 긴급변경 관련 사후관리 절차 미비

회사는 프로그램 긴급변경이 필요한 경우 내규에 따라 품질관리 부서에 운영 기간을 명시한 공문을 송부하여 일정기간 동안 품질관리(QA) 담당자의 검증 없이 소관 부서장의 승인만으로 프로그램을 변경하는 임시 프로세스를 운영하고 있으나

검사대상기간 중 시스템 오픈 전후 프로그램을 긴급 변경한 ○건의 경우 품질관리(QA) 담당자가 임시 프로세스에 따라 프로그램 긴급 변경 세부기준 및 작업내용을 확인하지 않는 등 사후 확인절차가 운영되지 않아, 프로그램 긴급 변경시 내부통제를 소홀히 할 우려가 있으므로

임시 프로세스에 따라 프로그램을 긴급 변경하는 경우 품질관리(QA) 담당자가 프로그램 긴급 변경 세부기준 및 작업내용을 사후적으로 확인할 수 있도록 관련 업무처리 절차를 체계적으로 개선하시기 바람

㈏ 프로그램 소스코드 분석절차 불합리

회사는 내규에 따라 변경된 프로그램을 운영시스템에 적용하는 경우 프로그램 소스코드에 대한 오류 분석을 수행하여야 하나

검사대상기간 중 형상관리시스템에 프로그램 소스코드분석 솔루션(△△△)을 연계하지 않아 ◇◇◇개발 과정에서 프로그램 소스코드에 대한 분석이 누락된 사례가 있으므로

앞으로 운영시스템에 프로그램을 변경 적용하는 경우 프로그램 소스코드 분석 절차가 누락되지 않도록 관련 시스템에 대한 내부통제 절차를 개선하시기 바람

㈐ 프로그램 연계기능 테스트 절차 불합리

회사는 내규에 따라 프로그램변경 시 작업계획서, 개발서버 반출, 영향도 분석, 기능테스트 등의 절차를 마련하여 수행하고 있으나

프로그램과 연계된 부분에 대한 테스트 시나리오를 작성·검토하는 과정이 내규에 명시되어 있지 않아 일부 프로그램을 변경하는 과정에서 연계기능과 관련된 오류가 발생할 수 있으므로

앞으로 프로그램 변경 테스트시 프로그램 연계 기능도 포함하여 테스트 시나리오를 작성·이행하도록 관련 업무절차를 개선하시기 바람

(5) 외부주문에 의한 프로젝트 관리절차 미흡

회사는 내규에 따라 외부주문에 의한 정보처리시스템 구축을 위한 프로젝트를 관리하고 있으나

검사대상기간 중 추진한 ◇◇◇ 및 ☆☆☆ 구축 사업의 프로젝트 관리를 점검한 결과, 사업 진척도 관리 및 진행상황 등에 대한 중간보고 절차가 없어 시스템 구축이 지연된 사례가 있으므로

앞으로 외부주문에 의한 IT부문 사업 추진시 프로젝트 지연이 발생하지 않도록 사업 진척도 관리 및 진행상황 등에 대한 보고 관련 업무절차를 개선하시기 바람

(6) 개별 저축은행의 통신망 관리체계 개선

회사는 ◇◇◇ 및 금융공동망 서비스를 제공하기 위하여 전용회선을 이중화하여 운영하고 있으나

일부 저축은행(○○개사)의 경우 전용회선과 가상사설통신망(VPN)의 백업망을 동일 통신사(▽▽▽)로 운영하고 있어 해당 통신사 장애 발생시 회사 전산 및 정보처리시스템에 접속이 차단될 우려가 있으므로

개별 저축은행이 전용회선 및 가상사설통신망(VPN)의 백업망을 다른 통신사로 이중화하여 회사의 ◇◇◇ 및 금융공동망 서비스를 중단없이 접속할 수 있도록 통신망 관리체계를 개선하시기 바람

(7) 운영서버에 대한 관리 미흡

회사는 서버, 네트워크 등 전산장비를 통합유지보수 업체를 통해 관리하면서 유지보수 실시 내역을 매월 점검하여 유지보수 대장에 기록하고 있으나

검사착수일(○○○○.○.○.) 현재 총 ○○○대의 서버 중 ○○대(○○%)가 제조사의 기술지원이 종료된 운영체제를 사용하고 있어 새로운 유형의 보안취약점 또는 시스템 오류 등에 대한 신속한 대응이 어려운 측면이 있으므로

시스템 중요도 및 영향도를 고려하여 기술지원이 종료된 운영체제는 업그레이드하고 교체가 필요한 경우 전환계획을 수립·이행하시기 바람

(8) 전산시스템 장애대응 체계 개선

회사는 전산장애에 신속히 대응하기 위해 온라인거래 모니터링 요원을 24시간 배치하고, 장애 모니터링 솔루션을 이용하여 서버 및 네트워크의 장애 발생을 파악하고 장애 복구 업무를 수행하고 있으나

검사대상기간 중 발생한 전산장애 중 야간(21:00~9:00) 및 휴일에 발생한 장애의 경우 장애 복구 관련 실무경험 및 지식을 갖춘 전문인력 부족 등으로 약 2시간 정도 장애가 지속되는 등 서비스 복구에 장시간이 소요되는 문제점이 있고

또한, 모바일 앱(APP)의 접속량 제어수단이 없어 특정 저축은행의 금융상품 특판 등으로 거래량이 폭증할 경우 전체 저축은행의 모바일 금융서비스가 지연될 우려가 있으므로

앞으로 야간·휴일에 발생하는 장애와 특정 저축은행의 거래량 폭증 등으로 인해 발생할 수 있는 장애에 대응하기 위해, 장애복구 조직을 확충하는 등 장애대응 체계를 개선하시기 바람

(9) 외부주문시 외부인력 관리체계 개선

회사는 내규를 통해 외부주문시 외주인력의 투입부터 종료까지 지켜야 할 보안통제절차를 마련하고 있으며

내부통제위원회를 구성하여 외주인력에 대한 보안통제 이행현황을 분기별로 점검하고 있으나

외주인력의 출입, 전산기기 및 시스템 접근권한 등 보안통제에 대한 내부통제 시스템 부재로 인해 내부 정기감사에서 외주인력 보안통제 부문에 대한 지적사항이 반복적으로 발생하는 등 외주인력 관리가 미흡하므로

앞으로 외부주문시 외주인력에 대한 보안통제(출입통제, 시스템 접속권한 관리 등)가 체계적으로 유지·관리되도록 내부통제시스템을 개선하시기 바람

(10) 전산기반시설 취약점에 대한 영향분석 절차 개선

회사는 내규에 따라 전자금융기반시설 및 홈페이지에 대한 취약점 분석·평가를 실시하고 그 결과에 따른 조치계획을 정보보호위원회의 의결 후 최고경영자에게 보고하고 있으나

검사대상기간 중 실시한 전자금융기반시설에 대한 취약점 분석·평가 결과, 운영 DB 서버와 관련하여 장애발생 가능성이 있는 취약점이 발견되었음에도, 취약점 수준에 대한 영향분석 절차 없이 정보보호위원회 의결 후 위험을 수용한 사례가 있으므로

앞으로 전자금융기반시설에 대한 취약점 분석·평가 결과에서 발견된 취약점에 대해서는 장애 가능성 등에 대한 영향분석을 실시하여 필요시 보완 조치를 취하도록 관련 업무절차를 개선하시기 바람