경영유의사항 등 공개안

1. 금융기관명 : ㈜케이비저축은행

2. 조치일 : 2025. 11. 11.

3. 조치내용

제재대상	조치내용
기 관	경영유의사항 2건, 개선사항 2건

4. 조치대상사실

가. 경영유의사항

(1) 외부주문 업무 감사 불철저

회사는 「IT감사업무지침」 제3조 등에 따라 IT감사(종합·특별·일상) 및 IT자체감사를 구분하여 IT감사업무를 수행하고 있다.

하지만 검사대상 기간(2022.1.1.~2025.4.16.) 중 일부 외부주문 업체에 위탁한 업무*의 적정성 등에 대하여 IT감사(종합·특별) 및 IT자체감사를 하지 않았다.

* (A) 전산설비 및 S/W, H/W 등의 통합유지보수, KB ONE클라우드 서비스 통합 운영/관리(MSP) 등
(B) FCC(미래컨택센터) 콜인프라 서비스

<조치할 사항>

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

(2) 핵심업무 선정 관리 강화 필요

회사는 2025. 3월 업무영향 분석을 위한 평가기준을 수립하고 동 기준에 따라 각 업무부서의 단위업무를 분석·평가하여 핵심업무를 선정*하였다.

* 단위업무를 113개의 소분류로 분류하여 이 중 43개의 단위업무를 핵심업무로 선정

하지만 핵심업무 선정을 위한 각 업무부서 단위업무 기초자료에 제3자 서비스 등 일부 단위업무*를 누락하였고, 핵심업무와 상호 연관성이 높은 제3자 서비스 등 일부 단위업무**가 핵심업무로 분류되지 않는 경우 비상상황 발생시 업무연속성이 보장되지 못할 우려가 있으며,

* 신용정보 조회, 안심이체, 알림서비스, 비대면 대출관리(대출해지, 조건변경 등) 등
** 신분증 진위확인, 고객 조회, 고객 등록/변경, 대출관리 등

핵심업무로 선정되지 않은 일반업무*에 대해서는 복구목표시간 및 복구우선순위 등을 설정하지 않아, 향후 재해 발생 시 관련 시스템 구축 등 복구가 원활하게 수행되지 못할 우려가 있다.

* 비대면 대출은 전체 대출의 ○○%를 차지하나, 비대면 신규 여·수신 업무를 핵심업무로 선정하지 않고, 복구목표시간도 설정하지 않아 복구가 장기간 지연될 경우 수익 감소 등 우려

또한, 전사 업무연속성계획관리지침은 업무영향 분석을 통해 핵심업무를 선별하도록 하고 있으나, 비상대책운영매뉴얼은 최고정보관리책임자가 각 부서장 면담을 통해 업무영향 평가를 실시하여 핵심업무·중요업무·일반업무를 설정하도록 하고 있는 등 핵심업무 선별·선정 절차에 일부 보완할 점이 있다.

<조치할 사항>

따라서 회사는 업무영향 분석 대상 분류시 제3자 서비스를 포함한 회사의 전체 단위업무가 포함되도록 분류하고, 업무영향 분석을 재수행하여 핵심업무 선정을 재점검하도록 하며, 선정된 핵심업무에 대해서는 3시간 이내 복구가 가능하도록 제3자 서비스를 포함한 재해복구시스템 구축 여부를 검토하시기 바랍니다.

또한, 일반업무에 대해서도 복구목표시간 및 복구우선순위 등을 설정하여 관리하고, 업무지속성 관련 내규를 정비하는 등 핵심업무 선정·관리 체계를 정비하시기 바랍니다.

나. 개선사항

(1) 제3자 서비스 관련 비상대책 및 재해복구전환훈련 미흡

회사는 업무지속성확보를 위해 「IT비상계획서」를 마련하고, 동 계획서 및 재해복구전환 대상 시스템의 상세 복구 절차가 기술된 「재해복구 모의훈련 계획서」에 따라 매년 재해복구전환훈련을 실시*하고 있다.

* 매년 자체 재해복구전환훈련 연 1회, 2023년 및 2024년도 KB금융그룹 통합 재해복구전환훈련 연 2회 실시

하지만 IT비상계획서 등에 실제 재해 발생 시 재해복구시스템 전환 및 제3자 서비스 복구 절차, 제3자 서비스 장애시 비상대응방안* 마련이 미흡하고,

* 저축은행중앙회 재해복구시스템 전환시 연계절차 등 중요 제3자 서비스 장애시 상세 대응방안 미흡

2024년 하반기에 핵심업무를 재정비하고 핵심업무와 연관된 제3자 서비스에 대해서도 재해복구시스템과 통신회선을 연결하는 등 핵심업무의 비상대책을 보강하여 재해복구전환훈련을 실시하였으나, 핵심업무 관련 제3자 서비스 중 저축은행중앙회에 대해서만 연계 훈련을 실시하였다.*

* 2024.4월 내규를 개정하여 5년 단위로 핵심 제3자 서비스에 대한 연계훈련 계획 중

<조치할 사항>

따라서 회사는 제3자 서비스 복구 절차를 포함한 재해복구 대상 시스템 전환에 대한 상세절차 및 제3자 서비스 장애 시에 대한 비상대응방안을 IT비상계획서 등에 마련하여 운영하시기 바랍니다.

또한, 핵심업무와 관련된 제3자 서비스에 대해서도 재해복구전환훈련 시 연계훈련을 강화하여 실시하시기 바랍니다.(대외기관 지원이 불가한 경우 유사 환경 구조로 대체하여 훈련 실시)

(2) 프로그램 변경통제 절차의 실효성 미흡

회사는 내규「전산정보운영매뉴얼」및「전산 개발 절차서」에 프로그램 신규 개발 및 변경작업에 대한 사전 정당성 검증, 운영시스템 반영 전 영향도 분석 및 인수자 테스트, 정보보호 영향평가 및 보안성 검토 등 일련의 프로그램 변경통제 절차를 규정하고 있고, ITSM* 및 형상관리시스템, 영향도 분석솔루션 등을 연계하여 프로그램 변경통제 프로세스를 시스템적으로 구축·운영하고 있다.

* IT Service Management : 조직의 IT서비스를 체계적으로 관리하기 위한 작업관리솔루션

하지만 회사는 총괄품질관리자(A부 소속)가 수행하는 사전 정당성 검증절차*에 대해 구체적인 검증 항목·방법을 정의하지 않았을 뿐 아니라 세부적인 검증 내용·결과 등은 별도로 기록하고 있지 않아 동 절차를 형식적으로 수행할 우려가 있다.

* 프로그램 변경 요청에 대해 필요성 및 기술적 타당성 등을 사전 검증·승인하는 절차

또한, IT부서의 자체 전산작업은 내규에서 정한 프로그램 변경통제 프로세스를 적용하지 않고 있어 운영체제(OS : Operating System) 업데이트 등 타 시스템에 영향을 줄 수 있는 자체 전산작업에 대해서는 충분한 영향도 분석 및 테스트가 이루어지지 않을 우려가 있다.

또한, 회사는 시스템적으로 구축·운영 중인 프로그램 변경통제 프로세스 내에 정보보호 영향평가 및 보안성검토 절차를 구현하지 않고 정보보호부가 개별적으로 수행하고 있어 정보보호부가 미처 인지하지 못한 프로그램 변경 건에 대해 동 절차를 누락할 우려가 있다.

<조치할 사항>

따라서 회사는 구체적인 정당성 검증 기준을 마련하고 세부적인 검증내용·결과를 기록하는 등 사전 정당성 검증절차의 실효성을 제고하시기 바랍니다.

또한, IT부서 자체 전산작업을 포함한 모든 프로그램 변경 건에 대해 충분한 영향도 분석 및 테스트가 이루어지고, 정보보호 영향평가 및 보안성검토 절차의 누락이 발생하지 않도록 관련 업무 프로세스 및 기준을 개선하시기 바랍니다.