경영유의사항 등 공개안

1. 금융회사명 : 모아저축은행㈜

2. 제재조치일 : 2026. 1. 26.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 1건, 개선사항 4건

4. 제재대상사실

가. 경영유의사항

① 내부 IT감사제도 운영 미흡

금융회사는 IT감사에 대한 지침을 내규화하고 IT감사(정기, 특별 등)를 수행하여 주요전산시스템의 신규 개발, 개선 등 전산 관련 주요 사항을 확인하고, IT자체감사를 통해 일상 업무의 처리결과, 업무산출물 작성 여부 및 내용 적정성 등을 점검할 필요가 있다.

하지만 감사부서는 회사 내규 「감사규정」에 IT감사 관련 사항을 규정하지 않은채 임의로 IT감사를 실시하고, IT부서는 IT자체감사 관련 내규를 보유하지 않고 검사실시일 현재까지 IT자체감사를 수행한 실적이 없어 IT부문 주요 내부통제가 부실화될 우려가 있다.

<조치할 사항>

따라서 회사는 실질적인 IT감사 및 IT자체감사 활동이 이루어질 수 있도록 감사 대상, 범위, 주기 및 절차 등 세부사항을 내규에 반영하고 내규에 따라 IT감사를 실시하시기 바랍니다.

② IT·정보보호 부문 자체감사 독립성 확보 필요

회사는 감사업무 수행을 위하여 이사회 직속의 감사실과 동 부서 소속 IT감사 자문역, IT자체감사자 등 인력을 갖추고 있다.

하지만 IT자체감사자가 감사업무 이외에 정보보호시스템 운영 등 타 업무를 겸직하면서 시스템 운영업무 관리자(정보보호실장)에게 인사고과를 받고 있어 소속 부서·팀 및 담당업무에 대해 자체감사를 독립적·객관적으로 수행하지 못할 우려가 있다.

<조치할 사항>

따라서 회사는 IT자체감사 전담인력 확보 또는 IT자체감사자를 추가 지정하는 등 상호 견제가 가능한 체계로 인사·조직 개편 방안을 마련하여 IT감사의 독립성 및 객관성을 제고하시기 바랍니다.

나. 개선사항

(1) IT부문 직무전결 불합리

회사는 내규「직제규정」및「직무전결규정」을 수립하여 부서별 업무를 분류하고 세부 업무를 지정하고 있으며, 업무별 전결 기준을「직무전결기준표」에 정의하고 있다.

하지만 회사 내규에 IT부서(정보보호실·IT개발팀)의 업무가 구체적으로 정의되어 있지 않아 업무 범위·한계 구분이 곤란한 경우가 존재하고,「직무전결기준표」에 일부 업무의 전결 기준이 누락되어 있거나 전결권자가 명시적으로 지정되지 않아 업무추진 책임소재가 명확하지 않다.

이에 따라, 업무 수행이 차질이 발생하거나 사고 발생 시 담당자가 불분명해질 우려가 있다.

<조치할 사항>

따라서 회사는 명확한 업무 소관 분장을 위하여「직무전결기준표」에 누락되어 있는 업무를 반영하고 전결권자를 지정하며 업무 범위를 구체적으로 정의하는 등 직무 관련 내규를 체계적으로 정비하시기 바랍니다.

(2) 비상대책 수립 및 운용 불합리

회사는 업무지속성 확보를 위해 내규 「전산 위기대응 행동 지침」 및 「전산 재해복구 시나리오」를 수립하여 운영하고 있다.

하지만,「전산 위기대응 행동 지침」은 IT조직·업무 현황, 보안·유지보수 업체 현황, 데이터 백업·소산정책 등 주요 사항이 '17년 이후 개정·검토되지 않고 있다.

또한,「재해복구시나리오」는 보안관제 업체, 네트워크 회선, 외부연계 서비스 등의

변경사항이 반영되어 있지 않고, 재해 발생 시 업무별 복구 우선순위 미수립, IT담당자 연락처의 비상연락망 누락 등으로 신속한 비상대응에 차질이 발생할 우려가 있다.

<조치할 사항>

따라서 회사는 실효성 있는 비상대응체계를 마련하기 위해 내규에 시스템·협력업체 현황, 업무별 복구 우선순위 및 담당자 연락처 등을 현행화하고, 매년 1회 이상 점검하여 최신상태로 유지·관리하시기 바랍니다.

(3) 전자금융기반시설 취약점 분석평가 불합리

회사 내규 「정보보호운영지침」에서는 홈페이지의 취약점 분석평가를 6개월에 1회 이상 수행하도록 정하고 있고, 이에 따라 정보보호실은 홈페이지 취약점 분석을 연 2회 수행하고 있다.

하지만 회사는 취약점 분석·평가 대상 및 범위를 대외 홈페이지 등 일부 서비스로 한정하여 실시하고 있으며, 평가 대상을 주기적으로 교체하는 등의 대체 방안을 마련하지 않아 다수의 시스템·서비스에서 점검 실적이 부재하다.

한편, 정보보호실은 전자금융기반시설 취약점 점검을 연 1회 수행하여 이행결과를 대표이사에 보고하고 있으나, 내규에 전자금융기반시설 취약점 분석·평가 관련 기준, 대상 및 이행절차 등을 명시하지 않아 일관된 평가가 이루어지지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 내규에 전자금융기반시설 취약점 분석·평가 관련하여 점검 대상·범위, 기준, 이행절차 등을 구체적으로 명시하고 다수의 서비스에 대한 일관성 있는 취약점 분석·평가를 수행하시기를 바랍니다.

(4) 정보처리시스템 성능관리체계 미흡

회사는 시스템 성능 관리를 위하여 자체 구축한 모니터링 시스템에서 서비스 종류별 사용량을 단계별로 설정하여 이상징후 시 알림을 받고, 서버 리소스 상태와 네트워크 트래픽 등을 실시간으로 확인하여 일일점검 결과보고서를 작성하는 등 현황을 관리하고 있다.

하지만, 회사는 성능관리 관련 내규를 제정하지 않고, 시스템 용량 확장 시점 예측을 위한 종합적인 성능·사용량 추이 분석 체계가 부재하여 시스템 용량 부족으로 인한 장애가 발생하는 등 전자금융 서비스가 제대로 제공되지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 시스템 용량 부족으로 인한 서비스 지연, 장애 등을 방지하기 위해 피크 타임(peak time) 기준의 시스템 상태, 이용도 등의 모니터링을 강화하고, 응답 시간 지연 등의 이상 징후 발생 시 원인 파악, 시스템 용량 확장 시점 예측을 위한 이용도 분석 등 종합적인 성능·사용량 추이 분석 체계를 마련하고 성능관리 지침을 수립하여 운영하시기 바랍니다.