경영유의사항 등 공개안

1. 금융기관명 : 하나카드㈜

2. 제재조치일 : 2024. 7. 22.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 7건, 개선사항 25건

4. 제재대상사실

가. 경영유의사항

(1) 신용카드자산의 한도 관리 강화

내규「직무전결규정」제2조 별표에 따르면 신용카드자산의 운용전략 변경 등으로 신용리스크가 일정 수준 이상으로 변동할 경우* 리스크관리집행위원회에 보고하여야 한다.

* (기존회원정책) 전략 변경 대상이 최근 월 유효회원의 OO% 초과 또는 총 Exposure의 OO% 초과
(금융상품기준) 전년 월평균 대비 예상취급액 OO% 이상 증감 시

또한, 내규「신용관리지침」제52조에 따르면 회사는 매분기 실행된 신규 대출의 평균 DSR을 OO% 이내로 유지하여야 함에도 불구하고 카드론 취급액이 예상과 달리 급증하여 분기 중에 평균 DSR이 OO%를 초과함에 따라, 2022.8.30. ~ 2023.5.31. 기간 중 카드론 예상취급액을 O차례 걸쳐 전년 월평균 카드론 취급액의 OO%이상 축소하였으나 사안의 긴급성을 이유로 리스크관리집행위원회에 보고하지 않았다.

나아가, 회사는 2022.5.27. ~ 2023.7.26. 기간 중 현금서비스의 이용고객기반 확대 및 연체율 관리를 위해 현금서비스 부여 대상을 O차례에 걸쳐 최근 월 유효회원수의 OO%를 초과하여 변경하였음에도 현금서비스 한도관리는 리스크관리집행위원회에 보고대상이 아닌 것으로 잘못 판단하여 보고를 누락하였다.

<조치할 사항>

회사는 앞으로 리스크관리집행위원회 부의안건은 사전 보고를 원칙으로 하되 긴급한 조치가 필요한 경우 O개월 내 사후 보고하도록 관련 절차를 개선하시기 바랍니다.

(2) 신용카드자산의 리스크 관리 강화

내규「리스크관리집행위원회규정」제5조에 따라 신용관리부가 신용카드자산의 저신용·다중채무자 취급비중 등 신용리스크 관리현황을 점검하고 리스크관리집행위원회에 보고하고 있다.

하지만 2023년 8월말 현재 신용리스크 관리지표 중 '카드론 저신용자 취급비율'이 내부평점기준으로 O.O%에 불과하다고 보고하고 있으나 외부 CB사 평점기준으로 O.O%에 달하고, 2022년 이후 DSR규제강화로 '거치식 장기카드대출 취급비중'이 크게 감소하여 2023년 8월말 현재 OO.O% 수준이나 여전히 동 취급비중의 내부관리 목표치를 DSR규제강화 이전 수준인 OO%로 관리하고 있는 등 일부 신용리스크 관리지표들이 회사의 신용리스크를 측정·관리하는데 불합리한 것으로 나타났다.

또한 리볼빙의 경우 최근 저신용자의 연체율 상승 등으로 건전성이 악화되고 있음에도 리스크관리집행위원회에 보고되지 않고 있어 상품별 리스크 관리가 미흡한 것으로 나타났다.

<조치할 사항>

회사는 앞으로 리스크관리집행위원회에 보고하는 신용리스크 관리지표 및 내부관리 목표치의 적합성 등을 주기적으로 평가하고, 경기침체 지속 등으로 신용리스크가 확대되고 있는 신용카드자산에 대하여 상품별로 세부적인 리스크관리 방안을 마련하고 리스크관리집행위원회에 보고하시기 바랍니다.

(3) 자체 대환대출 리스크관리 기준 강화

회사는 2023년 이후 신용카드자산의 연체율이 급격히 증가하자 연체채권자의 신용회복 지원을 위해 자체 대환대출 취급을 확대하여 관련 신용리스크가 크게 증가하고 있다.

하지만 회사는 연체회수 수단으로 자체 대환대출을 집중적으로 취급한 기간이 짧아 리스크 요인 분석이 어렵다는 사유로 총액한도(월취급한도 OO억원 이내) 위주로 리스크 관리항목을 축소하여 운용하고 있다.

<조치할 사항>

회사는 앞으로 자체 대환대출의 연체율, 회수율 현황 등을 주기적으로 분석하고 유의미한 리스크 관리 항목을 추가하여 자체 대환론 리스크관리 기준을 강화하시기 바랍니다.

(4) 유동성리스크 조기경보체계 실효성 강화

회사는 내규「유동성리스크 관리지침」제11조에서 리스크관리 담당 부서가 조기경보지표를 설정하고 주기적으로 모니터링하도록 정하고 있다.

그러나「자금운용 및 조달지침」제12조에서는 재무관리부가 조기경보지표(O개)를 선정·관리하고 있어 부서 간 책임과 역할이 중첩되고 있으며, 동 조기경보지표를 수기로 산출하고 있어 관리자의 업무오류 가능성이 존재한다.

또한 회사는 조기경보지표를 이용하여 위험을 사전에 인지하고 유동성리스크에 대한 관리 절차를 강화해야 하나, 조기경보지표 산출 주기가 길어 조기경보지표의 사전예방적 기능을 수행하지 못하고 있다.

<조치할 사항>

회사는 앞으로 유동성리스크 조기경보지표 관련 부서별 담당업무 범위를 명확하게 규정하고, 조기경보지표 산출과정을 합리화하는 등 조기경보체계를 강화하시기 바랍니다.

(5) IT부문 자체감사 업무 여건 및 독립성 확보

회사 내규「A지침」에 따라 IT경력 5년 이상인 B부 소속 직원을 IT자체감사인으로 지정하고 IT·정보보호 부문 정기·비정기 감사를 수행하고 있다.

또한, 동 내규에 따르면 IT자체감사자는 불가피한 경우를 제외하고는 IT감사 관련 업무 이외에는 겸직하지 않아야 한다.

하지만, IT자체감사인은 사내 인력부족을 이유로 B부, C부, D부를 담당하면서 a, b, c 등 IT감사업무와 무관한 여러 업무를 겸직하고 있다.

이에 따라, 감사 결과 발견된 문제점 등에 대해 IT자체감사인이 깊이 있게 파악·관리할 업무여건을 보장받기 어려워 IT자체감사 업무가 부실하게 수행될 우려가 있다. 또한, IT자체감사인은 소속 부서장(B부)에게 인사고과를 받고 있어 소속 부서의 담당업무에 대해 자체감사를 독립적·객관적으로 수행하기 어려울 우려가 있다.

<조치할 사항>

회사는 IT자체감사자의 업무 여건 보장, 독립성 및 객관성을 확보할 수 있도록 업무조정, 조직 개편 등 인력운영 개선방안을 마련하시기 바랍니다.

(6) IT부문 정보화사업 추진체계 효율화

회사는 매년 IT부문 정보화사업 계획을 수립하여 추진하고 있으나 아래와 같이 정보화사업에 대한 관리가 미흡하므로 이를 개선할 필요가 있다.

㈎ IT사업 추진·관리체계 강화

B부는 매년 공문을 통해 각 현업부서에게 추진이 필요한 IT사업내용을 제출하도록 요청하고 이후 제출받은 내용을 토대로 IT연간사업계획을 수립하고 있다.

하지만 동 계획에 최종 반영여부를 공식 절차가 아닌 해당 실무자 간 비공식 협의를 통해 결정하여 공정성 및 객관성을 담보하기 어렵고, 사업추진의 타당성 분석·평가도 취약하게 이루어져 IT사업의 변경·취소가 빈번하게 이뤄지고 있다.

이에 따라, 2023년 11월 말 현재, 최근 3년간 IT사업 추진율은 평균 OO.O%, IT자본예산 집행률은 평균 OO.O%에 그치고 있으며 취소된 사업의 대부분이 '사업전략변경' 사유에 해당되는 등 IT사업 및 예산이 체계적으로 계획·관리되지 않아 전략적인 IT사업 추진이 어렵다.

㈏ 변경·취소된 IT사업에 대한 심의 강화

「E지침」에 따라 IT심의위원회(이하, '위원회')에서 심의·의결된 IT연간사업계획, O억 원 이상 IT투자사업 등이 계획변경, 취소 및 장기지연(심의 후 O개월 이상) 시 해당 안건의 소관부서장은 그 사유를 위원회에 보고하여야 한다.

하지만 회사는 O억 원 이상인 IT투자사업이 변경·취소되는 경우에만 위원회에 사유 등을 보고하였고, 시장환경변화 등으로 IT연간사업이 일부 변경·취소되는 경우에는 위원회에 보고하지 않았다.

또한, 위원회 의사록에는 취소·변경에 따른 보고 결과는 기록하지 않는 등 IT사업의 변경·취소 타당성 검토 및 이력 관리가 미흡하여 IT투자가 비효율적으로 이루어질 우려가 있다.

<조치할 사항>

회사는 IT사업추진 평가위원회를 구성하여 자체적으로 수립한 IT사업 타당성 평가기준에 따라 각 현업부서에서 요청한 IT사업을 평가한 후 동 위원회에서 의결된 건만 IT연간사업계획에 반영하고 해당 평가 결과를 각 요청부서에 공문으로 통보하고

IT심의위원회의 심의·의결을 받은 안건은 변경·취소 시에도 동일한 절차를 거치도록 하며 의사록에는 모든 안건에 대한 내용, 결과 및 의견을 기록하는 등 IT사업이 체계적으로 관리되도록 관련 내규를 보완하고 업무절차를 마련하시기 바랍니다.

(7) 외부주문 업무에 대한 내부통제 강화

회사 내규 「F규정」에서는 정보화 업무 구축, 인프라 및 정보보호시스템 운용을 외부주문 업체에 위탁할 수 있도록 정하고 있다. 서버·네트워크 장비, 정보보호시스템 운용 업무를 외부주문 업체에 위탁하는 경우, 회사는 정보처리시스템의 안전한 관리를 위해 외주직원의 작업계획 및 수행내역을 정기적으로 점검하는 것이 바람직하다.

하지만 회사는 정보처리 및 전산설비, 정보보호시스템의 운용 업무를 외부주문 업체에 위탁함에 따라 외주직원이 서버·네트워크 장비, 정보보호시스템 관련 정책 설정·변경 등 중요 작업을 수행하고 있음에도 외주직원의 시스템 접속 이력과 작업수행 내역의 적정성을 점검하고 있지 않다.

또한, 인프라 작업계획 등록, 특권계정 사용 신청 등 중요 업무처리와 시스템 변경에 대한 회사 책임자의 승인이 누락*되어 있는 등 위탁·운영 중인 IT·정보보호 업무에 관한 관리·감독이 미흡하다.

* 서버·데이터베이스 관리업무를 수행하는 외부주문업체 직원이 작업계획을 등록하고 현장대리인이 승인

이에 따라, 외주직원이 서버·네트워크 장비, 정보보호시스템 관련 중요 작업을 회사 책임자 승인 없이 수행하는 과정에서 정보처리시스템에 장애 또는 보안상 위협이 발생할 우려가 있다.

<조치할 사항>

회사는 외주직원의 시스템 접속이력과 작업수행 내역의 적정성을 정기적으로 점검하고 중요 업무처리 및 시스템 변경에 관한 사항은 회사 내부 책임자가 승인하도록 외부주문 업무에 대한 내부통제를 강화하시기 바랍니다.

나. 개선사항

(1) 카드대출 금리산정 방식 등의 불합리

① 카드대출 목표이익율 산정 근거 미흡

「대출금리 기준가격 산정 준칙」 제8조에 따르면 목표이익율 산정을 위한 금리전망 마진율은 평균조달비용 추이 및 시장 전망 등을 고려하여 산출하여야 하며 회사는 금리전망 마진율의 예측지표로 '회사채 1년만기 평균 금리 변동분' 및 '평균조달 Cost 변동분'을 적용하고 있다.

하지만 회사는 상기 예측지표를 정성적으로 선별·운용하고 있고, 특히 '평균조달 Cost 변동분'의 경우 조달원가에 반영되어 있어 비용이 중복 계상될 우려가 있다.

<조치할 사항>

회사는 앞으로 예측지표의 통계적분석 등을 통해 정확성을 제고하고, 비용이 중복으로 계상되지 않도록 기준가격 산정 체계를 검토하시기 바랍니다.

② 카드대출 할인금리 적용 대상자 선정 업무 미흡

회사는 카드대출 취급을 확대하기 위해 「카드대출 운용가격 관리 지침」 제4조에 따라 매분기 대출금리심사위원회에서 할인금리 적용 대상 및 최저·최대 할인율 등을 포함한 카드대출의 운영가격 산정기준을 의결하고 있다.

하지만 영업부서가 카드대출 마케팅을 수행하면서 신용등급간 금리역전이 발생하는 것을 방지하기 위해 별도로 금리할인 마케팅 대상자 선정기준을 마련 · 운용하고 있어 대출금리심사위원회에 의결한 운영가격 산정기준에 따른 할인금리 적용 대상자와 실제 금리할인 마케팅 대상자수 간에 큰 차이가 발생하고 있다.

<조치할 사항>

회사는 앞으로 영업부서에서 월별로 금리할인 마케팅 대상자 선정을 위한 세부기준을 품의하고 그 결과를 매 분기 대출금리심사위원회에 보고하시기 바랍니다.

(2) 법인카드 일시한도 부여기준 미마련

「기업여신 업무지침」 제3조 및 제15조는 법인한도 외 별도로 특수목적 경비성 대금 사용 또는 일시적, 계절적인 요인으로 한도가 필요한 경우 12개월 범위 내에서 일시한도를 부여할 수 있도록 하고 있다.

하지만 회사는 일시한도의 부여대상 및 한도부여 지침 등을 마련하지 않고 일시한도를 빈번하게 부여하고 있어 업무의 일관성이 저해되고 법인회원의 신용도 대비 과도한 한도가 부여될 우려가 있다.

<조치할 사항>

회사는 앞으로 일시한도 부여대상의 정의를 명확히 하고 일시한도 부여 시 신용도 등을 고려한 한도부여 기준을 수립하는 등 관련 업무를 개선하시기 바랍니다.

(3) 자동차 구입자금 대출 및 할부금융 업무 관련 내규 미마련

회사는 자동차 구입자금 대출 및 할부금융(이하 '오토금융') 취급금액이 급증하고 있으므로 「여신전문금융업법」 관련 등 관련 법규를 준수할 수 있도록 내규 「할부금융 업무지침」 등에 따라 세부 운영기준·절차를 마련할 필요가 있다.

하지만 회사는 오토금융에 대한 별도의 내규를 마련하지 않고 동 업무의 특성*이 반영되지 않은 업무매뉴얼 등으로 업무를 수행하고 있어 세부적인 업무수행 근거 등이 명확하지 않아 이로 인해 업무의 일관성이 저해되고 부실하게 상품을 취급할 가능성이 있다.

* (예) 오토금융 심사원칙, 대출한도, 중개수수료 한도 준수, 근저당 설정대상 등

<조치할 사항>

회사는 오토금융의 특성을 반영한 별도의 내규를 마련하고 업무매뉴얼 등으로 운영 중인 기준·절차 등을 내규에 반영하시기 바랍니다.

(4) 담보물 취득 및 평가 업무 미흡

여신전문금융업협회의 「여신전문금융회사의 기업여신 심사 및 사후관리 모범규준」 제9조에 따르면 금융회사는 영업부서와 구분되는 조직에서 담보취득의 적정성을 점검하고 담보가치를 정확하게 평가하여야 한다.

하지만 회사는 여신위원회 결의 시 담보물을 취득하였다고 보고*한 기업여신들을 신용대출로 분류하고 취득한 담보물의 전산 등록 및 평가 업무를 수행하지 않았다.

* 내규「기업여신업무지침」제23조에서 여신위원회가 담보로서 인정하는 물건은 취득가능한 담보의 종류로 정하고 있음

<조치할 사항>

회사는 앞으로 취득대상 담보물을 전산 등록하고 담보가치를 적정하게 평가하시기 바라며,「여신전문금융회사의 기업여신 심사 및 사후관리 모범규준」에 맞게 담보 취득 및 평가 업무가 이루어질 수 있도록 관련 내규를 개정하는 등 관련 업무를 개선하시기 바랍니다.

(5) 여신감리업무 미흡

내규「기업여신감리지침」제6조 및 제8조에 따르면 감리부서는 기업여신에 대하여 감리를 수행하여 감리등급을 산정·관리하고, 감리업무 수행 결과 나타난 업무개선 사항을 관련 부서에 통보하여야 하나, 아래와 같이 업무절차에 미흡한 점이 있으므로 이를 개선할 필요가 있다.

① 신용등급감리 미이행 및 감리결과 미통보

내규「기업여신감리준칙」제3조에 따르면 감리부서는 '기업신용등급감리'를 반기 O회 이상 실시하여야 하나 회사는 2021~2022년도에 해당감리를 수행하지 않았다.

<조치할 사항>

회사는 앞으로 내규에 맞게 감리가 수행될 수 있도록 감리계획 수립 및 이행여부를 주기적으로 점검하여 감리항목이 누락되지 않도록 관련 업무를 개선하시기 바랍니다.

② 감리결과 미통보

내규「기업여신감리준칙」제6조 및「기업여신감리지침」제8조에 따르면 감리부서는 감리업무 수행을 통해 여신의 부실 방지 및 체계적 관리 사항에 대하여 관련부서에 해당 내용을 통보하여 개선조치를 수행할 수 있도록 하여야 한다.

하지만 회사는 여신심사 및 건전성 분류업무 개선 등에 참고할 내용이 있는 수시감리 등을 실시하였음에도 감리결과를 유관부서*에 통보하지 않았다.

* (예) 수기심사, 상장폐지법인 및 기업등급하락 법인에 대한 수시 감리 등 결과를 심사부 및 신용관리부에 통보하지 않음

<조치할 사항>

회사는 앞으로 내규에 따라 주요 감리 결과가 유관부서에 통보될 수 있도록 감리프로세스 등을 개선하시기 바랍니다.

③ 조기관리업무 미흡

내규「기업여신감리준칙」제5조 등에 따르면 고객사 및 대표자의 연체, 부도, 법정관리 및 휴·폐업 등 한도조정 사유가 발생한 경우 사전에 규정한 '조기관리 한도감액 전략'에 따라 한도를 조정하여야 한다.

하지만 회사는 연체 발생 회원에 대하여 '조기관리 한도감액 전략'에서 정한 감액비율과 다른 한도감액 비율을 임의로 적용하면서 조정결과에 대해 제3자의 검토도 이루어지지 않고 있다.

<조치할 사항>

회사는 앞으로 한도조정사유가 발생하는 경우 내규에 따라 한도를 감액하시기 바랍니다. 또한 감액비율 조정이 필요한 경우 내규에 명확한 근거를 마련하고 조정근거* 등을 구체적으로 명기하여 제3자가 검토할 수 있도록 하는 등 임의로 감액비율을 조정하지 않도록 조기관리 업무 프로세스를 개선하시기 바랍니다.

* (예) 회원사의 신용도, 타사 연체 현황 등을 고려하여 감액비율을 OO~OO%내외로 조정

④ 감리등급별 조치 이행사항 미마련

내규「기업여신감리지침」제6조에 기업감리등급*을 정의하고 있으나 감리등급별 조치이행사항이 마련되지 않아 감리 이후 일관성 있는 조치사항이 이행되지 않을 우려**가 존재한다.

* A(양호), B(모니터링), C(중점관리), D(퇴출)

** (예) 퇴출등급인 D등급 부여 후 단순히 한도만 조정하거나 B, C등급 기업에 대해 근거 없이 한도를 감액

<조치할 사항>

회사는 내규에 감리 등급별 세부 감액 기준 등 구체적인 등급별 조치 이행사항을 마련하시기 바랍니다.

(6) 대체 투자심사 및 사후관리 업무 미흡

여신전문금융업협회의 「여신전문금융회사 대체투자 리스크관리 모범규준」 제7조 및 제9조, 내규 「대체투자리스크 관리지침」 제6조 및 제9조 등에 따르면 심사담당부서는 대체투자 안건 부의 시 안건에 대하여 심사의견을 작성하여야 하며, 심사의견 작성시 거래상대방 위험, 사업성 및 투자회수계획 등을 종합적으로 검토하여야 하고, 사후관리담당부서는 대체투자업무와 관련한 투자건별 모니터링 및 사후관리 업무를 수행하여야 한다.

하지만 회사는 투자안건에 대한 별도의 심사의견을 제시하지 않았고*, 내규 「대체투자리스크 관리지침」 제9조에 따라 마련된 투자업무매뉴얼에 따라 투자이후 수익률 및 사업추진 현황 등을 점검하여 대체투자자산별 체크리스트를 작성하여야 하나 이를 작성하지 않고 있다.

* (예시) 대체투자 신청시 영업부서가 신청의견 및 주요조사내용이 포함된 투자승인신청서를 작성하고 있으나 심사담당부서는 동 내용에 대해 별도의 의견을 제시하고 있지 않음

<조치할 사항>

회사는 앞으로 여신전문금융업협회의 「여신전문금융회사 대체투자 리스크 관리 모범규준」 등에 맞게 투자심사(심사보고서 작성) 및 사후관리(투자건별 모니터링) 업무가 이루어지도록 관련 업무 프로세스를 개선하시기 바랍니다.

(7) 비소매여신 대손충당금 적립 업무 미흡

회사의 「IFRS정책서」 제83조에 따르면 비소매 여신의 경우 내부신용등급의 하락을 신용위험의 유의적 증가로 정의하면서, 연체 30일 및 추가적인 질적정보 등을 고려하여 신용위험의 유의적인 증가에 대한 추가적인 요건을 정의하고 이에 따라 대손충당금을 적립하여야 한다.

하지만 회사는 추가적인 질적정보 항목을 구체적으로 정의하지 않아 자산건전성 기준 등에만 국한하여 신용위험의 유의적인 증가여부를 판단하고 있어 차주의 재무적 위험 및 부실징후 등에 대한 위험이 반영되지 않아 대손충당금이 과소 적립될 우려가 존재한다.

<조치할 사항>

회사는 차주의 재무상황 등 유의적 신용위험 변동을 판단할 수 있는 구체적인 분류기준*을 마련하여 대손충당금을 적절하게 적립하도록 관련 업무를 개선하시기 바랍니다.

* (예) 감사의견 부적정 및 의견거절, 최근 결산일 완전자본 잠식 등

(8) 대출계약 철회권 관련 업무 미흡

내규 「장기카드대출(카드론) 업무 준칙」등에 따르면 회사는 장기카드대출(카드론) 및 신용대출 실행 후 OO일 이내 고객이 대출금(사용기간만큼의 이자 포함)을 전액 상환하는 경우 대출계약철회권(이하 '철회권') 행사가 가능하도록 운영하여야 한다.

하지만 ① 철회권 행사단계에서 대출금을 상환하도록 하지 않고, 철회권 행사 후 개별적*으로 대출금을 상환하도록 하고, ② 철회권 행사 없이 OO일 이내 대출금을 완납하는 경우 대출계약철회권 행사 여부를 별도로 확인하고 있지 않는** 등 철회권 행사 절차가 복잡하여 고객이 대출계약철회권 행사를 못 하게 될 가능성이 있다.

* (장기카드대출) 청약철회 신청 완료후 버튼을 클릭해야 선결제 메뉴로 이동
(신용대출) 홈페이지 등을 통해 청약철회 신청시 상담원 연결 및 상담예약 안내
** OO일 이내 대출금을 전액 상환 완료후 대출계약철회권 신청 안내문자(LMS)를 발송

<조치할 사항>

회사는 앞으로 고객이 OO일 이내 대출금을 전액 상환하는 등 철회권 적용 대상에 해당하는 경우 권리행사에 불편이 없도록 철회권 행사 단계에서 원리금을 납부할 수 있도록 화면을 구성하는 등 철회권 관련 절차를 개선하시기 바랍니다.

(9) 법인회원에 대한 경제적 이익제공 금지 관련 내규 미마련

2021.3.23.「여신전문금융업법 시행령」개정(2021.7.1. 시행)으로 법인회원에 대한 과도한 경제적 이익을 제공하는 것이 금지*된 이후, 회사는 법규 준수를 위해 관련 경제적 이익 제공 모니터링 시스템을 마련·운영하고 있다.

* 총비용의 총수익 초과 금지, 경제적 이익 합산액이 신용카드 연간 이용총액의 0.5% 초과 금지

하지만 회사는 검사착수일(2023.11.27.) 현재까지 법인회원에 대한 경제적 이익 제공 기준, 기준 초과 여부 점검 방법 및 소기업확인 절차 등 구체적인 업무절차를 내규 또는 업무매뉴얼 등에 반영하지 않았다.

<조치할 사항>

회사는 법인회원에 대한 과도한 경제적 이익제공 금지업무 수행에 필요한 구체적인 업무 절차를 내규 또는 업무매뉴얼 등에 반영하시기 바랍니다.

(10) 비대면 발급 신용카드 교부(수령)시 본인확인 절차 미흡

내규「카드 발급 업무 준칙」제13조에 따르면 인터넷, 모바일 신청 등을 통해 접수된 카드의 경우 본인지정 방법(본인만 수령 가능)으로 배송하여야 한다.

하지만 회사는 비대면 방식(TM채널)으로 접수된 신용카드 배송시 고객의 수령요청지가 변경(영업점→자택·직장)되어 본인만 수령가능하도록 배송방법의 변경(일반배송→본인지정배송)이 필요함에도 배송방법을 변경하지 않아 신용카드를 타인이 수령하도록 하는 등 본인확인을 소홀히 한 사례가 있었다.

<조치할 사항>

회사는 비대면으로 발급된 신용카드 교부시 수령요청지가 변경되더라도 본인에게 직접 카드가 교부될 수 있도록 프로세스를 개선하여, 신용카드 부정사용 등으로 인한 금융소비자의 피해를 최소화하시기 바랍니다.

(11) 전화마케팅(TM) 불완전판매 예방 미흡

① 전화마케팅(TM) 위탁업체에 대한 평가기준 개선

내규「전화마케팅처리지침」제8조 등에 따르면 회사는 전화마케팅(TM) 상담원의 표준스크립트 준수 여부 등을 평가하여 완전판매 여부를 정기적으로 점검하고, 동 평가결과를 전화마케팅 위탁업체의 수수료에 적절히 반영하여야 한다.

하지만 회사가 운용하는 전화마케팅 위탁업체에 대한 평가기준의 변별력이 낮아, 회사는 2021년 하반기 이후 대부분의 전화마케팅 위탁업체를 B등급(도급료 OO% 지급)으로 평가하고 있다.

<조치할 사항>

회사는 앞으로 전화마케팅 위탁업체에 대한 평가기준(평가등급별 구간 및 통화품질 부실 감점기준 등)을 보완하여 전화마케팅(TM) 위탁업체에 대한 평가의 실효성을 제고하시기 바랍니다.

② 신규 부가상품 전화마케팅(TM)의 불완전판매 예방 미흡

회사는 2023년부터 오토케어, 펫케어 등 신규 부가상품 판매를 개시하고 관련 가맹점 이용고객을 대상으로 전화마케팅(TM) 활동을 확대하고 있다.

하지만 회사는 신규 부가상품 전화마케팅 대상자 선정시 가맹점 이용고객의 사용금액 수준을 고려하지 않고 있고, 특히 2023년 3분기 기준 전화마케팅 성공률이 O.O ~O.O% 수준으로 기존 부가상품 전화마케팅 성공률(O.O%)에 비해 낮게 나타나고 있는 점을 감안할 때 일부 불필요한 전화마케팅으로 인해 민원 등이 발생될 우려가 있다.

<조치할 사항>

회사는 앞으로 신규 부가상품 전화마케팅 대상자 선정시 사용금액 수준을 고려한 기준을 적용하고, 추가적으로 표준 스크립트에 마케팅 대상자로 적합한지 확인하는 문구를 포함하는 등 부가상품의 불완전판매 예방 활동을 강화하시기 바랍니다.

(12) PG가맹점의 하위사업자 거래에 대한 적정성 점검 미흡

가맹점 담당부서가 반기별로 전자결제대행사(payment gateway, 이하 'PG') 가맹점(OO개사)에게 하위사업자의 불량매출* 발생 여부를 점검하고 계약해지 등 필요한 조치를 하도록 공문으로 요청하고 있으나 모든 PG가맹점이 이상 없다고 회신하고 있다.

* 유사수신행위, 다단계, 가상통화(비트코인), 현금융통, 유사투자자문(주식리딩) 등

하지만 FDS팀에는 카드 매출거래내역 중 의심거래 검출·분석을 통해 지속적으로 다수의 불량 하위사업자를 적발하고, 하위사업자와 가맹점계약을 해지하고 있어 PG가맹점의 자체 점검에 실효성이 의심되는 상황이다.

<조치할 사항>

회사는 앞으로 부실 점검 PG가맹점 대한 페널티 부여 방안을 마련하고, 특히 불량거래 민원 빈도가 높은 하위사업자 등에 대한 조치를 강화하는 방안을 마련하시기 바랍니다.

(13) 도난·분실 등 청구보류시 업무절차 개선

한국신용정보원 「일반신용정보관리규약」 제28조에 의하면 일반신용정보가 등록된 이후 고객이 신용정보에 대한 정정청구 등을 요청한 때에는 사실여부를 조사하여 사실과 다르거나 확인할 수 없는 경우 등록된 신용정보를 삭제하거나, 사실과 같은 내용으로 정정하여야 한다.

하지만 회사는 단기카드대출(이하 '현금서비스') 이용고객의 명의도용, 보이스피싱 등의 부정사용에 대한 조사 진행을 이유로 현금서비스 이용대금 청구를 보류(청구보류)하는 경우 현금서비스를 '해제'하고 있어 조사 진행 중 고객이 현금서비스를 이용한 것으로 조회되는 등 「일반신용정보관리규약」에서 정하고 있는 업무절차와 일부 다르게 운영되고 있다.

<조치할 사항>

회사는 앞으로 부정사용 등의 사유로 조사진행을 위해 청구를 보류하는 경우 현금서비스 이용내역을 삭제하고, 조사 완료 후 확인된 내용에 따라 신용정보를 정정하도록 관련 절차를 개선하시기 바랍니다.

(14) IT부문 감사업무 불합리

회사는 정보처리시스템의 안전성 및 효율성 확보를 위하여 회사 내규 「A지침」과 「B규정」을 수립하고 있으나 아래와 같이 자체감사 업무에 미흡한 점이 있으므로 이를 개선할 필요가 있다.

㈎ 자체감사 지적사항의 조치요구 기준 마련 필요

내규에 지적사항의 조치요구(개선, 주의 등) 기준이 마련되지 않아 IT 자체감사인이 지적사항에 대해 필요에 따라 임의로 시정권고, 현지조치, 진행 요구 등 상이한 조치요구를 하고 있어 업무에 혼선을 초래할 우려가 있다.

㈏ 자체감사 사후조치 관리 강화

내규에 감사 지적사항의 사후관리업무는 부서장이 전결하도록 정하고 있다. 하지만 C부 및 D부의 본부장은 IT자체감사 지적사항의 사후조치현황을 '감사결과 보고' 등 타 보고서에 포함하여 참고자료 정도로만 간략히 보고받고 있어 사후관리가 부실화될 우려가 있다.

<조치할 사항>

회사는 체계적이고 일관성 있는 업무수행을 위해 IT자체감사결과 조치요구 기준을 수립하여 내규에 반영하고 C부 및 D부의 본부장은 조치완료, 미정리 등 지적사항의 최종 이행 여부를 확인하고 결재할 수 있도록 업무절차를 강화하시기 바랍니다.

(15) 비상대책 수립·운용 불합리

회사 내규 「E지침」에는 F부에서 연 1회 사업영향도분석(BIA)을 통해 전체 업무에 대해 복구우선순위를 설정하여 복구목표시간을 설정하도록 정하고 있다.

또한 내규 「E지침」에 따라 C부는 전체 정보시스템에 대해 '핵심', '중요', '일반'으로 복구우선순위 및 복구목표시간을 설정하였으며 핵심 정보시스템은 3시간 이내에 복구할 수 있도록 재해복구시스템을 구축·운용하고 있다.

하지만 C부는 내규「E지침」등 관련 내규에 복구우선순위(핵심, 중요, 일반) 선정기준을 마련하지 않은 채 핵심업무 등을 임의로 선정하였고, 일반업무에는 복구목표시간을 설정하지 않았으며, 복구우선순위의 적정성에 대해 정기적으로 검토하지 않았다.

한편, D부 및 C부는 복구우선순위별로 복구목표시간을 각자 설정하면서 상호 간에 일치 여부를 확인·조정하지 않음으로써, 동일 업무임에도 복구우선순위가 과대 또는 과소하게 설정되거나 일부 업무는 복구우선순위가 설정되지 않는 등 비상대책을 다르게 운영하였다.

이에 따라, 비상상황 시 혼선이 발생하여 복구가 지연되거나 재해복구 관련 시스템의 운영·유지보수비용이 효율적으로 집행되지 못할 우려가 있다.

<조치할 사항>

회사는 D부 및 C부는 사업영향도분석(BIA) 시 협업하여 현업업무와 관련 정보시스템을 연계한 후 복구우선순위 및 복구목표시간을 설정·관리하고, 내규「E지침」에 복구우선순위 선정기준을 마련하며 일반업무에도 복구목표시간을 설정하는 등 비상대책이 일관성 있고 체계적으로 수립 및 운영될 수 있도록 개선하시기 바랍니다.

(16) 오픈소스 프로그램 관리체계 미비

회사는 프로그램 개발 및 정보처리시스템 운영 등을 위해 업무용 오픈소스프로그램을 다수 도입·운영하고 있다. 오픈소스 프로그램을 안전하게 이용하기 위해서는 라이선스 정책 준수 및 보안관리 등에 관한 표준화된 관리체계를 마련하는 것이 바람직하다.

하지만 2023년 말 현재 회사는 오픈소스 프로그램 식별·관리, 라이선스 정책 및 보안점검 등에 관한 관리체계를 마련하고 있지 않다. 그리하여 오픈소스 사용현황을 수기로 관리하고 있고 라이선스 정책과 보안 리스크도 정기적으로 점검하고 있지 않아 오픈소스 프로그램 이용에 따른 운영리스크*가 발생할 우려가 있다.

* (보안 리스크) 공개된 소스코드로 인한 중요 취약점 노출, 패치 무결성 훼손 등
(법적 리스크) 오픈소스 라이선스 사용 저작물의 상업적 이용 등

<조치할 사항>

회사는 오픈소스 프로그램이 활용되는 전체 주기(도입·활용·유지보수)에 관한 관리체계를 내규로 마련하시기 바랍니다. 또한, 오픈소스 프로그램별로 라이선스 정책 준수 여부를 정기적으로 확인하고 보안 리스크에 관한 점검을 수행하는 등 오픈소스 프로그램에 대한 관리·통제를 강화하시기 바랍니다.

(17) 운영체제 등 시스템 소프트웨어 관리 불합리

내규 「O지침」에 따르면, 회사는 주요 전산장비, 소프트웨어 등의 위험을 관리하고 문제가 발생하는 경우 시스템을 신속하게 복구할 수 있도록 운영하여야 한다.

하지만 회사는 2023년 말 현재 운영 중인 시스템 OO대 중 OO대(OO.O%)에서 제조사 기술지원이 종료된 운영체제(OS)와 데이터베이스(DBMS)를 사용하고 있다. 이에 따라, 신규 보안 취약점에 대한 조치가 곤란하거나 장애 대응이 원활하게 수행되지 않을 우려가 있다.

<조치할 사항>

회사는 기술지원이 종료된 시스템 소프트웨어를 상위 버전으로 업그레이드 혹은 교체하거나 제조사 등과 장애 대응을 위한 기술지원 확약 계약을 체결하는 등 대응 방안을 마련하시기 바랍니다.

(18) 전산자료 백업·복구 검증 불합리

회사 내규 「F규정」에 따르면 회사는 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 주요 백업 전산자료에 대해서는 검증하여야 한다. 따라서 회사는 백업·소산 중인 DB데이터와 파일시스템 운영체제, 시스템 로그 등에 대해 정기적으로 복구검증을 수행할 필요가 있다.

하지만 회사는 백업·소산한 전산자료 중 DB데이터에 대한 복구 훈련만 수행하고 파일시스템과 운영체제, 시스템 로그 등에 대한 복구훈련은 수행하지 않고 있다.

이에 따라, 백업·소산된 운영체제 설정정보, 시스템 파일 및 프로그램 파일, 시스템 로그 등에 대한 무결성 검증이 미흡할 우려가 있다.

<조치할 사항>

회사는 파일시스템과 운영체제, 시스템 로그 등 백업·소산된 전산자료 전반에 관한 복구검증을 정기적으로 수행할 수 있도록 업무절차를 마련·운영하시기 바랍니다.

(19) 정보처리시스템 접근통제 불합리

회사 내규 「G규정」은 시스템 자원을 사용할 수 있는 범위와 수준을 제한하는 등 시스템 접근 통제를 통해 시스템을 안정적으로 유지하고 전산사고를 방지하도록 정하고 있다. 따라서 회사는 명령어 실행 제한 등을 통해 인가받지 않은 사용자가 서버에 접속하거나 작업을 수행하는 것을 방지할 필요가 있다.

하지만 검사착수일 현재 사용자가 특정 서버에 접속한 후 서버 간 원격 접속 명령어를 통해 접근 권한이 없는 다른 서버로 접속할 수 있어 비인가자가 서버접근통제 정책을 우회하여 중요 서버에 접근할 위험이 있다.

또한, 일반계정으로 접속한 사용자가 계정전환 명령어를 통해 서버 관리자 계정으로 전환할 수 있어 계정의 비밀번호가 노출·공유되는 경우 관리자 계정이 오남용될 우려가 있다.

<조치할 사항>

회사는 서버접근통제 정책을 거치지 않고 서버 간 원격 접속이 가능한 명령어를 차단하고 관리자 계정으로 전환할 수 있는 사용자 계정을 제한하는 등 정보처리시스템 접근통제 정책을 강화하시기 바랍니다.

(20) 정보처리시스템 감리체계 미흡

회사 내규 「H 지침」은 정보처리시스템 구축사업의 개발예산이 자본금의 0.0%를 초과하는 경우, 감리 적용대상으로 정하고 있다.

하지만 정보처리시스템 구축사업에 대한 감리 적용 기준금액이 지나치게 높게 설정되어있어 검사대상기간 중 감리실적이 OO건(0.0%)에 불과하다.

또한, 시스템 구축사업에 대한 감리 적용기준을 사업비 규모로만 판단하고 있어 기준 금액 이하의 대고객 및 내부 핵심업무 관련 정보시스템 구축사업은 감리를 수행하고 있지 않는데, 사업관리 소홀로 심각한 오류 및 일정 지연 등의 문제가 발생할 우려가 있으므로 개선이 필요하다.

<조치할 사항>

회사는 정보처리시스템 감리 기준금액을 하향 조정하고 대고객 및 내부 핵심업무와 관련된 정보화 사업을 감리대상에 포함하도록 관련 내규 및 업무 절차를 개선하시기 바랍니다.

(21) 프로그램 변경관리 및 테스트 미흡

회사는 내규 「I지침」, 「J지침」 등에 프로그램 변경관리에 대한 업무절차를 마련하여 운영하고 있으나 아래와 같이 프로그램 통제가 다소 미흡하므로 이를 개선할 필요가 있다.

㈎ 테스트 수행 절차 부적정

회사는 프로그램 변경통제에 대한 업무절차를 마련하고 프로그램 개발·변경 시 서비스요청관리시스템을 통해 개발자, 동료 테스트 및 인수(현업) 테스트를 거쳐 책임자(C부 RM) 승인 후 운영하고 있다.

하지만 검사대상기간 중 수행한 프로그램 개발·변경 건 중 개발자 테스트와 동료테스트 수행자가 동일한 사례가 있으며

인수(현업)테스트 결과 등록 시 개발자가 작성한 테스트 결과를 그대로 등록하거나 정상여부만 기록하는 등 테스트 결과를 상세하게 작성하지 않은 사례가 있다.

또한 정보시스템 개발 프로젝트에 관한 테스트(단위·통합·인수) 수행 시에도 테스트 결과서에 테스트 수행자를 명시하지 않거나 관련 증빙자료

(캡쳐화면 등)을 보관하지 않는 사례가 있어 테스트의 적정성에 대한 확인이 곤란하다.

㈏ 자체 프로그램 개선 시 검토 절차 미비

회사는 프로그램 개발·변경내용을 운영시스템에 적용하면 현업담당자가 정상 반영 여부를 확인하는 '서비스 요청 관리 절차'를 운영하고 있다.

하지만 프로그램 변경사항을 운영시스템에 반영 후 현업담당자가 확인하기까지 평균 OO일 이상 소요되고 있으며

프로그램을 자체 개선*하는 경우 운영시스템 적용 후 정상 반영 여부를 검증하는 절차가 없어 프로그램 변경으로 인한 운영시스템 장애 발생 시 확인이 늦어져 신속한 대응이 어려울 우려가 있다.

* 배치수행 시간 개선, 프로그램 조회 쿼리 성능 개선 등

<조치할 사항>

회사는 일일 IT자체감사 수행 시 프로그램 개발·변경 건에 대한 샘플링 점검을 추가 확대하여 테스트 적정성 및 운영시스템 적용 후 책임자 확인 등 점검을 강화하고, 운영시스템 적용 후 책임자 확인이 지연되지 않도록 관련 업무절차를 개선하시기 바랍니다.

또한, 프로그램 자체 개선 건에 대하여 운영시스템 반영 후 책임자 확인 절차를 추가하여 운영하고, 정보시스템 개발 프로젝트 수행 시 테스트 결과서에 테스트 수행자, 결과 증빙자료 등을 체계적으로 관리할 수 있도록 관련 절차를 강화하시기 바랍니다.

(22) IT프로젝트 관리 불합리

회사는 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 내규 「K지침」을 마련하고 있으나 아래와 같이 IT프로젝트 관리 절차가 다소 미흡하므로 이를 개선할 필요가 있다.

㈎ 표준 필수 산출물 관리 미흡

회사는 정보처리시스템 개발 프로젝트에 대한 담당자별 책임 및 역할, 진척관리, 산출물 관리 등 관련 업무절차를 마련하고 사업 착수 시 사업수행계획서를 통해 산출물을 정의하고 사업 종료 시 프로젝트담당자(PM)가 최종 산출물을 산출물관리시스템에 등록하고 있다.

하지만 표준 필수 산출물이 정의되어 있지 않아 운영자매뉴얼 등 시스템 운영에 필요한 산출물이 누락될 우려가 있고, 일부 프로젝트의 경우 최종 산출물의 일부를 산출물관리시스템에 등록하지 않고 개인 PC에서 관리하는 등 산출물의 등록·관리가 미흡하다.

㈏ 프로젝트 관리 기준 및 인력 부족

회사는 품질관리담당자가 품질관리 계획 수립 및 점검 수행 등 IT프로젝트의 품질관리 업무를 수행하도록 정하고 있다.

하지만 현재 회사는 C부 내 프로젝트 품질관리를 담당할 인력이 없고 품질관리 대상 및 점검 방법 등 프로젝트 품질관리에 관한 세부 기준도 마련되어 있지 않다.

이에 따라, IT프로젝트 추진 과정에서 코드 리뷰, 정적 분석 등 표준화된 품질보증 활동이 이루어지지 않아 프로그램의 안정성과 신뢰성이 저하될 우려가 있다.

<조치할 사항>

회사는 내규에 표준 필수 산출물을 정의하고 프로젝트 최종 검수 시 검수자가 필수 산출물 제출 여부 및 산출물관리시스템 내 등록 여부를 확인하도록 하여 IT프로젝트에 대한 산출물 관리가 체계적으로 이루어질 수 있도록 개선하시기 바랍니다.

또한, IT프로젝트에 대한 품질관리 업무를 수행할 수 있도록 인력을 보강하여 품질관리업무를 개선하고 IT프로젝트에 대한 자체 감사 수행 주기를 확대하여 프로젝트 산출물에 대한 적정성 점검을 강화하시기 바랍니다.

(23) 이용자 정보 관리 미흡

회사는 비인가자에 의한 중요정보 유출, 파괴 등의 피해를 방지하기 위해 회사 내규 「L지침」 제24조의2 등을 마련하고 정보보호 시스템을 운영하고 있으나, 아래와 같이 이용자 정보 보호 대책이 다소 미흡하므로 이를 개선할 필요가 있다.

㈎ 프로그램 테스트 시 이용자 정보 변환관리 미흡

회사는 내규 「M지침」 제12조에 따라 프로그램 테스트를 위한 이용자 정보 필요 시 IT담당 부서장의 결재를 득하고 데이터를 변환하여 사용하도록 정하고 있다.

하지만 데이터 변환 솔루션에 결재 기능이 없어* 담당 부서장의 결재 없이 데이터를 변환하고 있고, 정보보안점검의날 사후 점검 시에도 변환 정책의 적용 여부만 점검하여 데이터 변환의 정당성 등에 대한 검토가 수행되지 않아 이용자정보 관리가 미흡할 우려가 있다.

* 솔루션을 도입하면서 요구사항에 결재 기능을 포함하지 않음

㈏ 개인정보 비식별화(마스킹) 처리 절차 미흡

개인정보 조회·출력 시 개인정보를 비식별(마스킹)처리하여 보안 조치를 수행하고, 마스킹 예외가 필요한 화면의 항목은 P부 합의를 받고 시스템 담당 외주 업체에 공문을 발송해 비식별 해제(마스킹 해제) 처리하고 있다.

하지만 내규에 화면 마스킹 대상에 대한 기준이 없고 예외처리 및 사후 점검 등에 대한 절차를 정하지 않아 마스킹이 누락되거나 과도하게 예외허용이 될 우려가 있다.

<조치할 사항>

회사는 이용자 정보 사용 시 부서장 결재 후 변환이 수행될 수 있도록 솔루션을 개선하고, 내규에 마스킹 관련 지침 및 마스킹 예외처리 절차와 사후 점검에 대한 사항을 명시하여 개인정보에 대한 관리·통제를 강화하시기 바랍니다.

(24) 취약점 분석·평가 불합리

회사는 전자금융기반시설에 대한 취약점 분석·평가를 정기적으로 실시하고 취약점 이행조치 결과를 정보보호위원회의 심의·의결을 거쳐 최고경영자에게 보고하고 있다.

하지만 불가피한 경우가 아닌데도* 기술적으로 조치가 가능한 일부 취약점을 위험수용 사항으로 분류하고 있다.

* 다수 서버 적용 어려움, 시스템 교체 후 조치 예정 등

또한, 위험수용 대상을 정보보호위원회 심의·의결 안건에 포함하여 최고경영자에게 전부 일괄하여 보고·승인하고 있으므로, 취약점을 제거하지 않아 발생 가능한 문제점을 최고경영자가 명확하게 인지하지 못할 우려가 있다.

<조치할 사항>

회사는 추후 조치가 가능할 것으로 판단되는 취약점은 위험수용이 아닌 조치예정 취약점으로 분류하여 이행점검 및 관리토록 하고, 위험수용 취약점에 대해 보고 시 최고경영자가 위험수용하는 취약점의 문제점을 명확히 파악할 수 있도록 분리하여 보고하시기 바랍니다.

(25) 침해사고 대응체계 미흡

회사는 전자금융기반시설에 불법적인 침투나 권한취득 방지를 위해 내규 「N지침」 제5조, 제7조 제1항 등을 마련하여 훈련을 수행하고 관련 시스템을 운영하고 있으나, 아래와 같이 침해사고 대응이 다소 미흡하므로 이를 개선할 필요가 있다.

㈎ 웹방화벽(WAF) 운영 정책 미흡

회사는 내규 「N지침」에 따라 해킹 등 전자적 침해행위를 방지하기 위해 웹방화벽(WAF)을 도입하여 운영하고 있다.

하지만 방화벽 관리의 어려움을 이유로 웹방화벽의 운영정책을 탐지모드*로 운영하여 침해 공격시도에 대한 즉각적인 대응이 어려울 우려가 있다.

* 공격시도를 탐지만 하고 차단하지 않는 등 방화벽 정책 적용 미흡

㈏ 비상대응 훈련 미흡

회사는 침해사고 대응능력 확보를 위해 침해사고 대응훈련 등 비상대응 훈련을 연 O회 실시하고 사후 결과에 대해 필요한 조치를 이행하고 있다.

하지만 침해사고 대응 훈련을 홈페이지에만 수행하고 있어 ㉮, ㉯ 등 모바일 앱과 승인계에 대한 공격에는 대응이 어려울 우려가 있다.

<조치할 사항>

따라서 회사는 웹방화벽 정책 전반에 대한 검토 후 운영에 영향도가 낮은 운영정책은 즉시 차단 조치하고 나머지 사항에 대해서도 영향도 확인 후 조치하시기 바랍니다.

또한, 서버해킹·디도스 훈련 시 홈페이지뿐만 아니라 모바일 앱 등에 대한 훈련도 함께 실시하시길 바랍니다.