경영유의사항 등 공개안

1. 금융기관명 : 롯데카드㈜

2. 제재조치일 : 2026. 7. 28.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 20건, 개선사항 34건

4. 제재대상사실

가. 경영유의사항

(1) 자본확충 등 관리 강화

회사 내규에 따르면 리스크관리부서는 관련 부서와 협력하여 전사 리스크 현황을 분석, 평가하며 이를 리스크관리위원회에 보고해야 하고, 위기상황대응 전담 부서는 위기 판단지표를 선정·관리하여야 한다.

하지만 회사는 조정자기자본비율 및 단순자기자본비율이 타사 대비 열위인데도 리스크관리위원회에서 자본적정성 관련 지표를 정기적으로 점검하지 않고 있으며, 기본자본 확충에 대한 계획 역시 세우지 않았다.

또한, 회사는 자산 증가에 따른 레버리지배율 준수 및 조정자기자본비율 관리를 위해 회사채에 비해 상대적으로 고금리인 신종자본증권을 발행하였으나,

신종자본증권의 조기상환 만기가 특정 시기에 편중되어 차환위험에 노출되어 있는데도 회사는 리스크관리부서 및 이사회에서 신종자본증권 발행 시 발생할 수 있는 리스크에 대해 논의하지 않았다.

<조치할 사항>

따라서 회사는 신종자본증권 발행을 통한 보완자본 증대 이외 자기자본 감소에 대한 대응책으로 유·무상 증자 등을 통한 기본자본 확충을 검토하는 한편,

향후 조건부자본증권 발행 시 만기구조의 적정성 및 금리리스크 등을 리스크 관리부서가 종합적으로 검토하고 관련 부서와 협의한 후 이사회에서 필히 논의할 수 있도록 관련 절차를 개선하시기 바랍니다.

(2) 이익 배당의 적정성 검토 미흡

회사는 배당 실시 前 배당 규모 등을 검토하여 이사회에 관련 안건을 상정하고, 주주총회에서 주요주주 의결을 통하여 배당을 결정하고 있다.

한편, 「여신전문금융업감독규정」 제7조의3(자기자본 대비 총자산 한도)에 따르면 총자산이 자기자본의 8배를 초과하여서는 아니 되며, 직전 회계연도 당기순이익 대비 100분의 30 이상의 이익배당을 지급한 경우에는 총자산이 자기자본의 7배 이내로 제한되는데도,

2023년을 제외한 2022 ~ 2025년 기간 중 이사회에서 배당 관련 의결 시 배당금액이 조정자기자본비율, 레버리지배율 등에 미치는 영향을 검토하지 않았으며, 배당금액 관련 구체적인 산정 근거도 보고하지 않았다.

또한, 최근 당기순이익이 감소하는 추세임에도 불구하고 배당성향이 상승하여 타사 대비 열위인 자본적정성 지표가 더욱 악화될 우려가 있다.

<조치할 사항>

따라서 회사는 향후 배당을 실시하는 경우 수익 능력을 초과하는 이익배당 여부, 레버리지배율 기준 등을 고려하여 배당 규모의 적정성 및 회사에 미치는 영향 등을 사전 검토하고 이사회 및 주주총회에서 배당 관련 의결 시 해당 내용이 보고 및 논의될 수 있도록 관련 절차를 개선하시기 바랍니다.

(3) 대주주 여신에 대한 건전성 관리 강화 등

여신금융협회의 「기업여신 심사 및 사후관리 모범규준」에 따르면 여신심사 및 승인시스템 관련 여신전문금융회사는 여신 실행 이전 신용리스크를 적절히 평가, 관리할 수 있도록 건전한 여신심사 및 승인업무에 관한 내부시스템을 운영하도록 규정하고 있으며, 회사 내규는 '여신운용의 기본원칙'으로 합리적인 의사결정을 통하여 금융 리스크를 최소화하고, 수익을 극대화하도록 운영하여야 한다고 규정하고 있으며 이를 위해 회사는 여신심의위원회를 운영하고 있다.

하지만 회사의 대주주(특수관계인 포함)에 대한 여신현황을 살펴보면, 해당 잔액은 2022년말 이후 지속 증가하였으나, 연체율이 악화되는 등 건전성에 부정적인 영향을 미치고 있다.

특히 A사에 대한 여신 심사과정에서 A사의 재무상태가 지속적으로 악화되었는데도 여신심의위원회 등에서 기업구매카드 한도 축소 등의 관리방안 마련 없이 한도를 계속 연장하여 2025년 3월에 연체 등으로 부실화되었다.

한편, 회사 내규에 의하면, 심의 대상은 "신규 취급 건에 적용되며 기존 건의 추가, 증액, 승계(차주변경), 한도 재설정(한도유지 포함)을 포함한다. 다만, 단순 만기연장, 금리변경 등의 대출조건 변동은 제외한다"고 규정하고 있는바, 대주주 관련 여신 및 요주의이하 여신에 대하여도 만기연장 건에 대하여는 심의를 생략할 수 있어 부실 가능성이 있는 여신의 경우에도 심의 없이 연장될 우려가 있다.

<조치할 사항>

따라서 회사는 대주주 대상 여신의 경우 일정 규모 이상이거나 요주의이하 여신에 대하여는 내규에 규정된 절차에 따라 심사의견서를 작성하고, 독립성을 확보할 수 있는 심사강화 방안을 마련하는 한편,

건전성이 요주의이하인 경우에는 신규 취급 제한, 만기 연장 거부 또는 향후 감액 운영 여부에 대하여 중점 검토·관리하는 기준 또는 절차를 마련하고,

대주주 여신 현황 및 관련 부실여신 정리 계획 등에 대하여 리스크관리위원회에 주기적(예 : 분기 이상)으로 보고하여 관리하는 등 대주주 여신 관련 리스크 관리를 강화하기 바랍니다.

또한, 여신심의위원회의 운영과 관련하여 만기 연장의 경우에도 심의 대상에 포함(예 : 요주의이하인 여신보유 차주의 만기연장 등)하여 심의하는 한편, 요주의 이하 여신에 대한 여신심의를 강화하는 방안을 마련하기 바랍니다.

(4) 부동산 PF대출 건전성 관리 강화

① 「부동산PF 리스크관리 모범규준」상 '책임준공확약 업무처리기준' 등 개정내용 반영 필요

여신금융협회의 「부동산PF 리스크관리 모범규준」은 2024.11.29. '부실 사업장에 대한 경공매 기준'을 정비하는 내용으로 개정되고, 2025.5.15.에는 '책임준공확약의 PF대출 관련 업무처리기준'을 신설하는 내용으로 개정되었으나, 검사 종료일 현재 회사 내규 「부동산 PF대출 취급 규정」에 이를 반영하지 않아 부동산 PF대출 관련 리스크관리에 소홀할 우려*가 있다.

* 다만, PF사업장은 모두 대리 금융기관이 타사로, 회사는 대주로서 참여

<조치할 사항>

따라서 회사는 내규에 「부동산PF 리스크관리 모범규준」의 '책임준공확약의 PF대출 관련 업무처리기준' 등 개정 내용을 반영하고, 관련 내용에 따라 PF대출 업무를 처리하도록 개선하시기 바랍니다.

② 신규 PF대출 등에 대한 리스크 관련 보고 강화

회사 내규에 따르면 회사는 리스크관리를 위해 익스포져 한도 설정과 함께 관리절차 및 정책을 마련하고, 각 사업장별 정기적 모니터링 등 사후관리를 실시하여야 하며, 리스크관리부서는 개별 자산 또는 거래가 회사에 미치는 영향을 수시로 측정하여 보고하도록 규정하고 있는데도,

2025년 중 '㉮ 개발사업 PF대출' 등 일부 사업장에 대해 신규 부동산 PF 대출을 취급하여 관련 익스포져가 증가하였으므로 사업장 현황과 향후 리스크관리 방안 등을 보고할 필요가 있으나, 이에 대한 내용을 리스크관리위원회에 별도 보고하지 않는 등 관련 리스크관리에 소홀할 우려*가 있다.

* 다만, PF대출 중 요주의이하 여신에 대한 관리방안은 위원회에 보고

<조치할 사항>

따라서 회사는 신규 부동산 PF대출에 대하여, 리스크관리위원회 등에 신규 사업장 현황, 사업성 및 건전성 등에 대한 모니터링 방안 등을 주기적(예 : 분기 이상)으로 보고하도록 개선하는 한편, 기존 PF대출의 요주의이하 사업장에 대한 관리현황 및 부실여신 정리방안을 지속적으로 관리하는 등 리스크관리를 강화하여 주시기 바랍니다.

(5) 대손충당금 적립 등을 통한 건전성 관리 강화

「여신전문금융업감독규정」 제11조(대손충당금 등 적립기준)에 따르면 여신전문금융회사는 결산시(매분기 가결산 포함) 결산일 현재 채권 및 리스자산, 카드자산, 미사용약정, 지급보증, 여신성가지급금, 미수이자, 부동산프로젝트파이낸싱 관련 채무보증에 대하여 관련 기준에 따라 충당금을 적립하여야 한다고 규정하고 있으므로, 회사는 이에 따른 적정 대손충당금을 적립하여 손실흡수능력을 유지할 필요가 있다.

하지만 회사의 '대손충당금적립비율'은 2025년 들어 6월말 및 9월말 100%에 근접하는 수준으로 하락하였는데,

이는 주로 A사에 대한 채권 및 B사 등의 장기월납채권의 부실 발생에 따라 요적립액이 증가하였는데도 실제 적립액이 요적립액 만큼 충분히 적립되지 못한데 기인한 것으로 파악된바, 회사는 부실채권 정리 및 대손충당금 적립 강화 등을 통하여 손실흡수능력을 충분히 유지하는 등 건전성 관리를 강화할 필요가 있다.

<조치할 사항>

따라서 회사는 부실채권에 대한 정리(부실채권 상각 포함) 등을 통한 여력 확보 및 추가 충당금 적립 등을 통하여 손실흡수능력이 유지될 수 있도록 '대손충당금적립비율' 관리 방안을 마련하고, 이에 대한 이행 계획 및 주기적인(예 : 분기 이상) 점검 내용을 리스크관리위원회 등에 보고하는 등 건전성 관리를 강화하시기 바랍니다.

(6) 이사회 운영 강화

「금융사지배구조법」 제13조(이사회 의장의 선임 등)에 따르면 이사회는 매년 사외이사 중에서 이사회 의장을 선임하여야 하나, 이사회는 사외이사가 아닌 자를 이사회 의장으로 선임할 수 있고 이 경우 이사회는 그 사유를 공시하고, 사외이사를 대표하는 자(이하 "선임사외이사"라 한다)를 별도로 선임하여야 한다. 한편 선임사외이사는 사외이사 전원으로 구성되는 사외이사 회의의 소집 및 주재 업무를 수행하여야 한다.

그러나 회사는 내규에 이사회 의장은 대표이사로 하며, 매년 이사회에서 선임하도록 규정하여 사외이사의 이사회 의장 선임 기회를 제한하고 있다.

또한 선임사외이사를 별도로 선임하고 있음에도 불구하고 선임사외이사가 주재하는 사외이사 전원 구성 회의를 실제로 운영하지 않아 이사회 심의 과정에서 경영진에 대한 사외이사의 견제 기능이 약화 될 우려가 있다.

<조치할 사항>

따라서 회사는 대표이사가 이사회 의장을 맡도록 한 조항으로 사외이사의 의장 선임 기회를 제한하지 않도록 관련 규정을 개선하고, 이사회의 독립성과 견제 기능을 제고할 수 있도록 선임사외이사의 사외이사회의 소집 및 주재 권한을 내부 운영지침에 구체적으로 명시하는 한편, 사외이사 간 자유로운 의견 교환을 위한 별도의 소통 채널 및 행정적 지원 체계를 마련하는 등 이사회 운영의 실효성을 강화하시기 바랍니다.

(7) 이사회 내 위원회 운영 강화

① 리스크관리위원회 운영 관련

회사는 이사회 내 위원회로 리스크관리위원회를 두고 있으며 리스크관리 위원회에서는 회사의 리스크관리 기본방침 및 전략 수립, 회사가 부담 가능한 위험 수준 결정 등의 사항을 결정하고 있으며 회사 내규로 심의·의결사항, 위원회 소집과 운영방안을 정하고 있다.

그러나 검사대상기간 중(2022.7.9.~2025.12.12.) 리스크관리위원회에서 의결 안건을 심의하였으나 일부 이사의 경우 심의를 위한 발언 빈도가 낮아 의결 논의가 심도 있게 이루어졌다고 보기 어렵다.

또한 연간 리스크관리 계획 및 리스크한도 설정과 관련된 안건에 위원들의 논의 발언이 없는 등 리스크관리위원회 위원들의 리스크관리에 대한 관심도가 낮고 연간 리스크관리 계획 및 리스크 허용한도가 매년 2월에 의결됨에 따라 시의성이 떨어지고 의결 안건도 채권 대손비용 계획에 한정되거나 자산별·업종별 한도가 설정되지 않는 등 리스크관리위원회 심의 기능이 미흡하다.

아울러 회사 내규에는 심의 안건 발생시 개최 7일전까지 각 위원에게 서면 또는 유선으로 개회 일시 및 안건을 통보하도록 되어 있으나 검사대상 기간 중 일부 안건의 경우 최소 3일~6일 전에 송부하여 검토에 충분한 시간이 주어지지 않아 위원회 운영의 실효성에 우려가 발생하고 있다.

<조치할 사항>

따라서 회사는 리스크관리계획 등 수립과 관련하여 시의성을 확보하고, 회의자료를 충실히 작성하며 안건에 대한 충분한 검토 기간을 보장하는 등 리스크관리위원회의 실효성을 제고하고 위원회 관리를 강화하시기 바랍니다.

② 내부통제위원회 운영 강화

회사는 이사회 내 위원회로 내부통제위원회를 두고 있으며 회사 내규를 통해 「금융사지배구조법」 제30조의2(임원의 내부통제등 관리의무) 등에 따른 관리 조치와 보고를 적절하게 수행하고 있는지 점검·평가하는 절차를 마련하고 있다.

하지만 내부통제위원회 중에 정보보호 또는 IT 전문가가 전무하여 기술적 리스크에 대한 실효성 있는 심의에 한계가 있는 실정이다. 실제로 2025년 상반기 내부통제위원회에 보고된 해킹사고 예방을 위한 관리체계 개선방안에 보안 취약점 관리 강화 내용이 포함되었음에도 보안 패치 업데이트가 적기에 이행되지 않아 2025년 하반기 해킹사고가 발생하였다.

이는 위원회의 이행 점검 및 보고 체계가 형식적으로 운영됨에 따라, 리스크 사전 방지 기능이 실질적으로 작동하지 못한 것으로 판단된다.

<조치할 사항>

따라서 회사는 내부통제위원회에 IT전문가를 보강하고, 위원회에 보고된 개선 방안의 실무 이행 여부를 실질적으로 점검·보고하는 체계를 마련하시기 바랍니다.

③ 임원후보추천위원회 운영 미흡

회사 내규에 따르면 임원후보추천위원회는 관련 법령 및 회사 내규에 따른 자격요건 충족 여부를 면밀히 검증한 후 후보를 추천하여야 하며, 경영승계의 적정성을 확보하기 위해 경영승계계획을 수립하고 최고경영자 후보군에 대한 상시 관리 업무를 내실있게 운영해야 한다.

하지만 회사는 사외이사 후보의 자격요건 적격 여부를 임원후보추천위원회 개최 이후에 확인하는 등 후보 검증 절차를 형식적으로 운영하고, 후보군의 전문성 등에 대한 검증 논의가 제대로 이루어지지 않고 있다.

또한 복수 후보자를 발굴·평가하도록 한 「금융사지배구조법」 취지와 달리 최고경영자 후보군을 현 대표이사 1인으로만 관리하고 있으며, 2022년 2월 임원후보추천위원회에서 후보자를 추천한 이후 최고경영자 후보군 탐색, 자격검증 및 후보군 추천 등은 전무한 상황이다.

<조치할 사항>

따라서 회사는 사외이사 후보 추천 시 임원후보추천위원회 개최 이전에 관련 법령 및 회사 내규에 따른 자격요건 검증을 완료하는 등 사전 확인 절차를 준수하고 후보자의 전문성에 대한 실질적인 논의가 이루어질 수 있도록 위원회 운영을 내실화하시기 바랍니다.

아울러 현 대표이사 1인으로만 관리 중인 최고경영자 후보군을 복수로 구성하여 관리하고, 최고경영자 후보군 탐색 및 상시 관리 업무를 실질적으로 이행하여 경영승계 계획의 실효성을 제고하시기 바랍니다.

(8) 임원 성과평가 방식 개선

임원 성과평가 체계 관련하여 아래와 같이 일부 미흡한 점이 확인되었으므로 관련 업무절차를 강화하시기 바랍니다.

① 경영진 성과평가체계 불합리

회사 내규 「성과보상체계 지침」에 따르면 회사는 높은 보상을 위한 과도한 리스크 부담행위를 제어하는 방향으로 성과보상체계를 설계하고 단기성과 중심의 인센티브 시스템을 지양하며 건전한 보상체계를 운용하여야 한다.

그러나 회사의 임원 성과평가체계 항목 대부분이 수익성·효율성 위주의 단기 실적 지표에 편중되어 있어 리스크 관리 및 내부통제 수준에 비례한 건전한 보상체계 운영이 저해될 우려가 있다.

또한 내부통제 강화를 위해 별도의 평가항목을 신설하였으나 평가항목이 추상적이고 세부 평가기준이 부재하여 경영진의 적극적인 내부통제 강화 노력을 이끌 수 있는 유인이 부족한 측면이 있다.

<조치할 사항>

따라서 회사는 전략과제·경영혁신과제 내 지표구성을 단계적으로 보완하여 리스크관리 및 신용정책 운영의 충실도 등 질적 지표 비중을 확대하고, 소비자보호 등 비재무 지표의 변별력을 제고하여 단기 실적 중심의 영업 유인을 완화하는 한편, 내부통제 미이행 및 금융사고 발생에 대한 책임경영이 정착될 수 있도록 사고의 성격과 영향도 등을 고려한 객관적인 내부통제 평가 기준을 마련하시기 바랍니다.

② 사외이사 성과 평가체계 불합리

회사 내규에 따르면 회사는 임원후보추천위원회의 후보 추천 및 연임 심사 시 주요 근거로 활용되는 사외이사의 활동내역에 대해 매년 1회 객관적이고 공정한 성과평가를 실시해야 한다.

그러나 회사의 사외이사 성과평가체계 상 자기평가 비중이 높고 상호평가 의견 기재가 생략되는 등 평가의 객관성이 미흡하다.

또한 상호평가를 받지 않는 기타비상임이사가 사외이사 평가를 수행함에 따라 사외이사 본연의 독립적인 견제 기능이 제대로 작동하지 않을 우려가 있는바, 이러한 형식적인 평가 운영은 회사 내규에서 정한 객관적인 연임 심사 및 평가 결과의 실질적인 반영이 저해될 수 있다.

<조치할 사항>

따라서 회사는 자기평가 비중을 축소하고 이사별 정성적 평가 의견 기재를 의무화하는 한편, 평가 주체에서 기타비상임이사 등을 제외하고 사외이사 간 상호평가 방식으로 전환하여 이사회의 독립적인 견제기능이 실질적으로 작동할 수 있도록 관련 프로세스를 개선하시기 바랍니다.

(9) 해외법인 내부통제 체계 강화

회사 내규에서 베트남 현지법인에 대한 업무 분장 및 리스크관리, 보고 의무 등 업무 범위를 규정하고 있다.

그러나 현지법인의 경영 현황 및 자체 감사 결과 등을 관리할 전산시스템이 구축되지 않아 보고 자료가 체계적으로 관련되지 않고 있다*. 또한 금융사고 보고에 대한 구체적인 기준이 부재하며, 현지법인에 대한 현장감사는 실시되지 않았다.

* 현재 본사와 현지법인 간 보고가 화상회의로 진행되고 회의자료를 개인이 보관

한편, 해외법인의 리스크 관련 중요한 의사결정을 위해 리스크관리부서 협조하에 리스크관리위원회를 설치하여야 하나, 회사는 리스크관리위원회를 구성하지 않고 리스크 관련 보고사항은 정기 임원회의 자료로 갈음하는 등 해외법인 운영에 대한 관리가 미흡하였다.

<조치할 사항>

따라서 회사는 현지법인 보고 전산시스템을 구축하고, 금융사고 보고 기준 마련 및 정기적인 현장감사를 실시하며 리스크관리위원회를 설치·운영하는 등 해외법인 관리 체계를 강화하시기 바랍니다.

(10) 신용정보 제공업체에 대한 관리·점검 강화

회사는 제휴업체인 C사에 법인카드 거래 관련 정보를 제공하고 있다.

그러나 법인회원으로부터 징구하는 신용정보 수집·이용 동의서 상에는 실제 제공되는 정보의 종류와 항목에 비해 현저히 적은 수준으로, 법인회원이 자신의 신용정보가 제공되는 범위를 정확히 인지하지 못할 우려가 있다.

한편, 회사는 홈페이지를 통해 제휴업체에 제공하는 신용정보 항목을 공시하고 있으나, 실제 제공되는 개별 항목들을 포괄하여 표기하고 있어 공시의 구체성이 낮고 실제 어떠한 데이터가 외부로 제공 및 활용되는 파악하기 어렵다.

아울러 외부 업체를 통해 실시한 C사의 신용정보 관리 실태 점검 결과, 다수의 미흡사항이 발견되었음에도 불구하고 회사는 별도의 추가조치 실시하지 않아 제휴사의 신용정보 보호 체계에 대한 관리 감독의무를 소홀히 하였다.

<조치할 사항>

따라서 회사는 법인회원 신용정보를 제휴사 등 제3자에게 제공하는 경우 실제 제공되는 신용정보 항목과 동의서 기재내용·홈페이지 공시내용의 일치성을 확보하여 정보 주체의 알 권리를 보장하고, 제휴사에 대한 정기적인 보안 점검 및 즉각적인 시정 조치 등 사후 관리 감독 체계를 강화하시기 바랍니다.

(11) 고객확인 업무 관련 내부통제 미흡

회사 내규에 따라 임직원은 고객과 카드발급 및 할부금융 등의 금융거래시 당해 금융거래가 자금세탁 등의 불법행위에 이용되지 않도록 고객의 신원 및 실제소유자 확인 등 고객에 대하여 합당한 주의를 기울여야 하고, 거래당사자인 본인뿐만 아니라 다른 개인 및 법인(또는 단체)을 대신하여 금융거래를 하는 대리인을 포함하여 고객확인의무를 수행하여야 한다.

또한, 자금세탁 등의 위험이 높다고 평가되는 특정고객 또는 상품 및 서비스 등을 고위험군으로 정할 수 있고, 해당 위험군에 대하여 신원확인 정보 이외 금융거래의 목적 및 자금의 원천 등 추가적인 정보를 확인하는 강화된 고객확인을 하여야 한다.

한편, 내규는 최초 금융거래를 목적으로 고객확인을 한 고객과 거래가 유지되는 동안 당해 고객에 대하여 지속적으로 고객확인을 하도록 규정하고 있다.

하지만 회사는 매월 고객확인 이행현황을 모니터링하면서 아래와 같이 강화된 고객확인 미이행 내역을 일부 발견하고 조치한 사실이 있다.

가) 2022년 12월 ~ 2023년 8월 기간 중 법인고객의 법인카드 개설 이후 대리인이 추가 또는 변경되었는데도 대리인에 대한 고객확인을 시스템상 필수 확인사항으로 운영하지 않았다.

나) 2024년 10월 ~ 2025년 3월 기간 중 재이행 주기가 도래한 고위험 개인고객에 대해 고객확인을 하면서 자금세탁 위험도에 적합하게 고객확인을 수행하지 않았다.

<조치할 사항>

따라서 회사는 고객확인 업무 수행시 유사사례가 발생하지 않도록 고객확인 및 강화된 고객확인 관련 내부통제를 강화하는 한편, 고객확인 이행현황 모니터링 관련 추출된 미이행 고객리스트, 미이행 및 보완 일자 등 상세내역도 추후 확인이 가능하도록 전산시스템상 함께 관리하는 절차를 마련하시기 바랍니다.

(12) 고객확인 장기 미이행 고객에 대한 관리 강화

내규 등에 따라 회사는 금융거래를 개시할 목적으로 고객과 계약을 체결하는 경우 고객확인을 실시하여야 하며, 기존 고객에 대해서도 거래가 유지되는 동안 자금세탁행위 등의 위험도에 따라 주기적으로 고객확인을 수행하여야 한다.

하지만 회사는 고객확인 재이행 주기가 도래한 고객에 대하여 ❶별도의 사전 안내를 하지 않고, 앱 로그인 또는 센터 내방 시 재이행을 수행하며, ❷미이행한 경우 카드 신규 또는 재발급이 불가하도록 절차를 마련하고는 있으나 2024년말 기준 고객확인 재이행률이 저조하여 카드 신규·재발급 전까지 고객확인이 장기간 재이행되지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 고객확인 재이행 주기 경과 고객에 대하여 재이행률을 주기적으로 모니터링하고, 재이행 주기 도래 전·후 안내 횟수 증대, 회사 홈페이지·앱 로그인 시 팝업 알림 등 안내 방식의 다양화 등 실효성 있는 조치를 통해 고객확인 장기 미이행 고객에 대한 관리를 강화하시기 바랍니다.

(13) 의심거래 보고(STR) 절차 강화

회사의 내규에 의하면 수사기관에 신고하거나 회사를 상대로 한 일정 금액 이상의 사기, 횡령 등의 사건을 인지한 경우 해당 거래를 의심되는 거래 보고(STR) 대상으로 분류하여 보고 책임자에게 즉시 보고하여야 한다.

하지만 회사의 STR 보고담당 부서인 준법경영팀은 2025.6월 ~ 7월 발생한 금융사고의 경우 제휴사 등의 대표이사에 대해 형사 고소 등을 검토하는 등 회사 차원에서 사건을 인지하고 있는데도 관련 내용을 감사팀으로부터 전달받지 못하였다는 사유로 의심되는 거래 보고를 현재까지 이행하지 않고 있다.

<조치할 사항>

따라서 회사는 사기, 횡령 등의 사건 인지 등 불법적인 금융거래로 의심되는 경우 유관부서 간 관련 내용을 공유하고, 담당 부서가 해당 거래가 의심거래 보고 대상에 해당되는지 여부를 검토하는 체계화된 절차를 마련하시기 바랍니다.

(14) 특정금융거래정보 관련 보안관리 강화

내규 등에 따라 회사는 자금세탁방지·테러자금조달금지 관련 정보의 안정성 확보 및 자금세탁방지방지에 관한 보안 위험 차단을 위한 지침을 마련하고, 자금세탁방지(AML) 시스템, STR·고액현금거래보고(CTR) 보고용 PC 등 보안관리 대상의 보안상 취약점 등 운영실태를 점검하고 있다.

하지만 회사가 2021년 ~ 2024년 기간 중 실시한 자금세탁방지 업무 내부 보안관리 점검에서 AML시스템 서버의 점검항목 중 특정 항목은 점검 결과가 매년 취약한 것으로 확인되고 있으며,

AML시스템 데이터베이스의 점검항목 중 일부 항목의 경우 2023년 이후 취약사항으로 지속 도출되고 있으나, 회사는 자산별 중요도 평가에 따라 중요도가 높지 않고, 단기적 개선보다는 전면 교체의 효율성 및 높은 비용 등을 고려하여 향후 AML 시스템 고도화 구축 시 병행 개선을 검토하겠다고 하여 개선조치가 지연되고 있다.

<조치할 사항>

따라서 회사는 보안관리 대상 점검 시 취약한 항목이 반복하여 도출되지 않도록 보다 근본적인 개선방안을 마련하는 한편, 자금세탁방지 업무 관련 고객확인 및 금융거래 기록, STR·CTR 보고를 위한 금융거래 자료 등이 유출 될 경우 대내외 미치는 영향 및 파급효과 등을 감안하여 중요도 평가를 실시하고, 개선조치 이행이 지나치게 장기화되지 않도록 우선순위 조정 및 지속적인 진행상황 점검 등 보안관리를 강화하시기 바랍니다.

(15) 유동성리스크 관리 강화

① 자금조달 편중도 관리 미흡

회사의 내규는 자금조달 편중 완화를 위해 조달 상대방별, 부채 만기별, 조달 수단(시장)별 편중도를 관리하도록 규정하고 있다.

그러나 실제로는 회사채 비중만 중점 관리하고 시장별 편중도는 관리하고 있지 않아 회사 내규와 실무 간 불일치로 인해 관리체계의 실효성이 저하되고 특정 조달 수단 및 시장 의존도 상승 위험을 조기에 파악하기 어려운 측면이 있다.

또한, 목표 설정, 모니터링 및 보고체계가 구체적으로 규정되지 않아 자금관리 부서에서 자체 설정한 목표를 리스크관리 부서가 점검한 후 위험관리책임자(CRO)에게 보고하는 등 표준화되지 않은 절차로 인해 관리의 일관성과 책임 소재가 불명확해질 우려가 있다.

<조치할 사항>

따라서 회사는 자금조달 편중 완화를 위한 지표가 회사 내규에 부합하도록 관리 대상을 확대하여 정합성을 확보하는 한편 시장별 편중 기준 설정 및 정기적 점검체계 마련을 통해 조달구조 변동 리스크를 체계적으로 관리하시기 바랍니다.

② 조기경보지표 기능 강화

회사는 유동성리스크 유형별 관리지표를 운영하고 매월 해당 지표를 경영진에게 보고하는 등 기본적인 유동성 모니터링 체계를 갖추고 있다.

다만, 조기경보지표의 경우 회사 내규상 제시된 지표 구성과 실제 운영방식 간 일부 괴리가 존재*하고 유동성 위기 징후를 조기에 포착하기 위한 핵심 지표 선정 기준 및 운영 원칙이 명확히 규정되어 있지 않다.

* 회사 내규에는 유동성리스크 증가 인식에 활용하기 위해 조기경보지표를 제시하고 있으나 실무적으로는 일부 지표만 핵심 조기경보지표로 활용하고 나머지는 월말 보고서 형태로 단순 모니터링

이로 인해 조기경보지표가 유동성 위기 대응 역량을 체계적으로 평가·관리하는 수단으로 기능하지 못할 우려가 있다.

<조치할 사항>

따라서 회사는 내규와 실제 운영을 일치시키는 체계를 마련하고 조기경보 지표로 활용할 지표와 단순 모니터링지표를 공식화하는 한편 핵심 지표 선정기준 및 변경 절차를 명문화하여 운영의 일관성 및 투명성을 확보하시기 바랍니다.

(16) 유동성 위기 대비 비상자금조달계획 강화

회사는 유동성 위기 단계를 구분하고 단계별 트리거(발동기준)와 대응 조치를 설정하여 비상자금조달계획을 운영하는 등 기본적인 대응 수단을 확보하고 있다.

그러나 단계별 조치가 동일한 수단을 기준으로 검토·확정·집행 등 표현만 다르게 구분되어 실제 단계에 따른 대응 수준이 달라졌다고 보기 어려우며, 트리거 설정 기준은 과거 사례를 중심으로 산정되어 최근 시장환경 및 조달 여건 변화를 반영하지 못할 소지가 있다.

<조치할 사항>

따라서 회사는 위기 단계별로 조달수단·규모·확약 수준·집행 시점을 구체화하여 실질적 단계성을 강화하고, 시장 지표를 반영한 트리거 재정비를 통해 비상자금조달계획의 실행력과 현실성을 강화하시기 바랍니다.

(17) IT운영위원회의 의사결정 실효성 제고 및 예산관리 강화 필요

회사 내규에 따라 IT부문의 효율적 운영·관리를 위해 IT운영위원회를 설치하고 주요 장·단기 IT업무계획 및 IT사업에 대한 심의·의결 절차를 마련하고 있다.

그러나, 2023년 수립한 「IT중장기 전략」은 동 위원회의 심의·의결 대상인데도 안건에 포함시키지 않아 누락되었고 동 위원회에서 결정한 IT사업이 지연*되거나 취소되는 경우 이에 대한 확인절차가 부재하여 재심의 등 후속조치가 이루어지지 않고 방치되는 등 의사결정, 심의 및 사후관리가 미흡하다.

* 2023년 '온라인결제 서버 고도화' 사업은 예산 부족으로 두 차례 연기되어 2026년 추진 예정

또한, IT예산집행률*이 크게 감소한 경우 편성의 적정성이나 집행 부진에 대한 원인분석 및 개선조치도 이루어지지 않고 있어 비효율적 예산 집행이 지속되거나 이로 인해 중요 IT사업 추진에 차질이 빚어질 우려가 있다.

* (최근 3년간 정보보호예산 집행률) 2022년(77.1%) → 2023년(92.5%) → 2024년(77.1%)

<조치할 사항>

따라서 회사는 IT운영위원회 안건의 누락방지, 심의·의결된 IT사업의 사후관리 및 IT예산 집행관리를 위한 개선 방안 등을 마련하여 동 위원회를 내실있게 운영하시기 바랍니다.

(18) 정보보호부문 투자 및 인력관리 강화 필요

회사 내규에 따라 IT부문의 보안에 필요한 인력관리 및 예산편성을 하도록 규정하고 있으며, 안정적인 IT서비스 제공을 위해 적정 수준의 투자를 유지해야 한다.

그러나, 회사의 최대 주주가 변경된 2019년을 기준으로 최근 5년간(2020~2024년) 총 예산 대비 정보보호 예산 비율 평균은 0.36%로 이전 5년(2015~2019년) 대비 0.19%p 감소하였다.

특히, IT예산 대비 정보보호예산 비율(집행액 기준)은 2015년 이후 감소 추세로 정보보호부문에 대한 투자가 위축되는 모습을 보이고 있다.

또한, 2020~2024년 기간동안 IT인력 비중은 증가(4.2%p)하고 있으나 정보보호 인력 비중은 오히려 감소(△6.1%p)하고 있어 고도화되는 사이버 위협에 대한 대응 역량이 저하되고 중요 IT사업 및 보안대책 추진에 차질이 발생할 우려가 있다.

<조치할 사항>

따라서 회사는 IT 환경 변화와 리스크를 고려하여 정보보호 예산 및 인력을 충분히 확보할 수 있도록 목표 기준을 재설정하고, 중장기적인 보안 투자 계획을 수립하여 관리체계를 강화하시기 바랍니다.

(19) 기술지원이 종료된 전산시스템에 대한 신속한 교체·업그레이드 추진

금융회사는 금융감독원 검사 지적사항 및 자체 계획에 따라 기술지원이 종료된 서버 및 소프트웨어(운영체제 등)를 적기에 교체하거나 업그레이드하여 보안 리스크를 관리해야 한다.

그러나, 회사는 2022년 금감원 지적에 따라 수립한 서버(000대) 교체 계획을 예산 부족 및 우선순위 조정 등을 사유로 수차례 연기하여 2025.9월말 기준 이행률이 약 65%(000대)에 그치고 있다.

특히, 2025년 정보유출 사고가 발생했던 온라인 결제 서버의 교체 시점을 2차례나 연기*하였음에도, 경영진 및 리스크관리위원회는 이에 따른 보안 공백이나 대체 통제수단을 면밀히 검토·승인하지 않았다.

* 온라인결제 서버 교체: 당초 2023년 목표 → 2024년 연기 → 2026년으로 재차 연기

또한, 윈도우10의 기술지원이 종료(2025.10.)되었음에도 상위 버전으로의 업그레이드가 지연되고 있으나, 이에 대한 경영진 차원의 점검 및 리스크 대응 논의가 이루어지지 않았다.

이에 따라, 기술지원 종료된 시스템이 최신 보안 패치를 제공받지 못해 해킹 등 보안 위협에 쉽게 노출되거나 침해사고가 발생할 우려가 있다.

<조치할 사항>

따라서 회사는 기술지원이 종료된 전산시스템을 계획에 따라 신속히 교체하고, 경영진은 동 계획이 특별한 사유 없이 지연·취소되지 않도록 철저히 관리하시기 바랍니다.

아울러, 동 계획이 변경되는 경우 경영진 및 IT위원회는 보안 위협 등 발생 가능한 리스크에 대해 사전에 검토하고 필요한 통제를 강구하시기 바랍니다.

(20) IT자체감사 독립성 확보 및 감사업무체계 내실화 필요

회사 내규에 따라 IT자체감사 담당자(IT실 품질관리팀 소속 2명)가 IT 관련 2개 부서(IT실, IT개발실)에 대해 정기·수시감사를 수행하고 있다.

그러나, IT실 자체감사인이 타 IT부문 임원 소관인 IT개발실에 대한 자체감사를 수행하므로 IT자체감사인의 업무범위가 적합하지 않고 인원 부족 등에 따른 업무부담으로 감사보고서가 매월 동일한 내용으로 작성되는 등 형식적인 감사가 이루어지고 있다.

또한, 지적사항 조치 여부, 이력 관리 등 사후관리가 수기로 이루어지고 있어 누락·지연 등 관리 소홀로 지적사항이 미조치 상태로 지속되거나 동일·유사사항이 재발할 우려가 있다.

<조치할 사항>

따라서 회사는 IT자체감사자의 업무 여건 보장, 독립성 및 객관성을 확보할 수 있도록 업무조정, 조직 개편 및 인력운영 개선 방안을 마련하고, 체계적이고 실효성 있는 감사 실시 및 사후관리를 위해 자체감사관리시스템을 보완하여 운영하시기 바랍니다.

나. 개선사항

(1) 신용카드 거래 시 본인확인 소홀

「여신전문금융업법」 제24조 및 「여신전문금융업감독규정」 제24조의6(가맹점 관리사항) 등에 따라 신용카드업자는 가맹점과 계약체결을 통해 해당 가맹점이 신용카드에 의한 거래를 할 때마다 본인확인*을 하도록 관리하여야 한다.

* 카드상의 서명 및 카드 비밀번호 일치여부 확인, 여신금융협회장이 정하는 기준에 적합한 인증수단을 통한 이용자의 생체정보 확인 등을 이용한 본인확인

그러나 회사는 Ⓐ 제휴카드 발급 시, 실물카드가 아직 고객에게 배송되지 않은 상태에서 고객번호만을 이용해 가맹점 판매 현장에서 고객 구매물품에 대한 결제를 승인하거나 가승인 하는 등, 신용카드가맹점이 신용카드에 의한 거래를 할 때 「여신전문금융업감독규정」상 요구되는 본인확인 인증수단 확인이 불충분한 상태에서 결제 승인이 이루어지는 시스템을 운영하였다.

<조치할 사항>

따라서 회사는 가맹점 내 신용카드 거래 진행시 해당 가맹점이 법규상 적합한 인증수단을 거쳐 본인 확인 절차가 충실하게 이행될 수 있도록, 고객이 실물 카드를 수령하기 전 결제상황에서는 앱카드 등을 등록 및 이용하여 결제절차가 진행될 수 있도록 하는 등 신용카드 거래시 본인 확인 체계를 개선하시기 바랍니다.

(2) 대주주 신용공여 취급절차 내부통제 미흡

① 대주주 신용공여 관련 이사회 운영 미흡

「여신전문금융업법」 제49조의2(대주주에 대한 신용공여한도 등)에 따르면 여신전문금융회사는 그의 대주주에게 일정금액 이상의 신용공여를 하려는 경우에는 미리 이사회의 결의를 거쳐야 하며, 이 경우 이사회는 재적이사 전원의 찬성으로 의결하여야 한다.

그러나 회사 이사회는 대주주 측 인사가 참여한 가운데 최근 수년간 대주주 등 특수관계인에 대한 대출(신용공여)을 지속적으로 승인해 왔음에도 불구하고, 이 과정에서 아래와 같이 심의 및 보고 절차가 제대로 이루어지지 않은 사실이 확인되었다.

㉮ 특수관계인 신용공여 심의의 형식적 운영

대주주 관련 안건은 이해상충 방지를 위해 사외이사의 독립적 검증이 필수적이나, 일부 의사록에서 리스크 검토 및 질의·답변 기록이 확인되지 않았다. 특히 A사 관련 안건은 '사전 설명 청취'를 이유로 본회의 내 실질적 논의 없이 의결하는 등 심의 절차를 형식적으로 운영하였다.

㉯ 이해상충 이사의 발언에 따른 심의 독립성 저해

D사 유동화대출 심의 시, 대주주 측 인사이자 차주의 이사를 겸직하여 직접적인 이해상충 관계에 있는 기타비상무이사가 차주 측에 우호적인 의견을 제시함으로써 이사회 심의의 독립성과 객관성을 저해할 소지가 있었다.

㉰ 감독당국 지적사항 이행 부실

2022년 금융감독원 종합검사 당시 E사 팩토링 대출 실행 시마다 이사회 보고를 강화하도록 요구받았음에도, 실제 의사록에는 '보고하였음' 외에 리스크 요인 및 차주 재무상태 등 의사결정에 필요한 실질적 정보 제공이 전무하여 감독 당국의 요구사항을 사실상 미이행하였다.

<조치할 사항>

따라서 회사는 대주주 관련 신용공여 심의 시 이해상충 이사의 참여 및 발언을 엄격히 제한하여 심사의 독립성을 확보하고, 리스크 검토 결과와 실질적인 질의응답 내용을 의사록에 상세히 기록함과 동시에 감독당국 지적사항에 따라 차주의 재무상태 등 의사결정에 필요한 정보를 충실히 보고하시기 바랍니다.

② 대주주 신용공여 심사 및 관리체계 미흡

㉮ 대주주 신용공여 심사 사각지대 방치

회사 내규에 따르면 심사보고서 작성 대상을 '종합금융 관련 투자·여신'으로 한정하여, 대주주 등 특수관계인 대상 거액 신용공여가 발생하는 법인카드(기업구매카드, 세금카드)에 대해서는 별도의 심사보고서 없이 신용공여가 이루어지는 구조가 형성되어 그 결과 대주주 신용공여의 상당 부분을 실질적인 내부 심사 없이 취급하는 등 관리 체계를 미흡하게 운영하였다.

㉯ 대주주 관련 차주에 대한 심사 기능의 형식적 운영

회사 내규에 따르면 법인카드 한도 부여 시 여신심의위원회 안건에 심사부서 의견을 기재하도록 하고 있으나, 실제 리스크 분석 등 심사 기능은 부실하게 운영되었다. 일례로 대주주 관련 차주인 A사의 법인카드 한도 연장 시, 차주의 재무지표가 악화되었음에도 리스크 완화 조치 없이 '연장 적정' 결론을 도출하는 등 심사 절차를 형식적으로 수행하였다.

㉰ 대주주 거래 조건의 적정성 검증 절차 미흡

대주주 관련 거래 시 '조건의 독립성' 및 '가격의 적정성'에 대한 객관적인 비교 분석이 필수적이나, 관련 검증 기록이 부재하거나 미흡하였다. 특히 대주주 관련 차주인 D사의 장래매출채권 담보대출 심의 시, 금리 및 마진 설정 과정에서 시장 수준과의 비교·검토를 누락하는 등 대주주 거래에 요구되는 내부통제 절차를 준수하지 않았다.

<조치할 사항>

따라서 회사는 대주주 관련 법인카드 등을 심사보고서 작성 대상에 포함하도록 회사 내규를 개정하여 심사 사각지대를 해소하고, 차주의 재무상태 악화 시 실질적인 리스크 관리 방안을 마련함과 동시에 시장 수준과의 객관적 비교 분석을 통한 거래 조건의 적정성 검증 절차를 강화하기 바랍니다.

③ 대주주 신용공여에 대한 여신 감리체계 운영 미흡

여신금융협회 「기업여신 심사 및 사후관리 모범규준」에 따르면, 여신금융회사는 여신심사 및 사후관리 프로세스가 적절하게 가동되고 있는지 독립적으로 점검하는 여신감리 업무를 수행하여야 한다.

그럼에도 불구하고 회사는 2023년 3월 여신 감리제도를 도입하면서 감리 대상을 부동산금융 및 특정 기업여신으로만 한정하여 운영하였다.

이로 인해 고위험군에 해당하는 대주주 관련 법인카드(기업구매카드·세금카드) 및 팩토링이 감리 범위에서 제외되었으며, 그 결과 거액 익스포저 및 차주 재무상태 악화 등 리스크 요인이 큰 대주주 신용공여가 감리 사각지대에 방치되는 결과를 초래하였다.

또한 감리 대상에 포함된 일부 대주주 기업여신의 경우에도 자산건전성 분류의 적정성만을 사후적으로 확인하는 기초적인 수준에 그침으로써 여신감리 본연의 기능을 제대로 수행하지 못한 채 형식적으로 업무를 처리하였다.

<조치할 사항>

따라서 회사는 대주주 관련 법인카드 및 팩토링을 여신 감리 대상에 명시적으로 포함하도록 관련 회사 내규를 개정하고, 단순 건전성 분류 확인을 넘어 여신 전 과정에 대한 정밀 점검 체계를 구축함으로써 감리 본연의 리스크 통제 기능을 강화하기 바랍니다.

④ 대주주 신용공여 조기경보 체계 운영 미흡

여신금융협회 「기업여신 심사 및 사후관리 모범규준」에 따르면, 여신금융회사는 여신의 잠재 부도위험을 사전에 감지할 수 있도록 조기경보시스템 전반에 대한 자체적인 내부 체계를 구축·운영해야 한다.

그럼에도 불구하고 회사는 자체 조기경보 모형 없이 외부 신용평가사의 조기경보 서비스(EW등급)를 그대로 활용하고 있어 잠재 리스크에 대한 선제적 감지 기능이 미흡한 실정이다.

실제로 A사 기업구매카드 사례에서 외부 등급이 2024년 4분기 '정상'에서 2025년 1분기 '부도'로 급변하는 등 위험 신호에 대한 예측력이 부족하고 실제 리스크를 적절히 반영하지 못하는 한계가 확인되었다.

<조치할 사항>

따라서 회사는 외부 신용평가사 등급에 의존하는 현행 방식을 개선하여 대주주 및 거액 신용공여에 특화된 자체 조기경보 모형을 구축하고, 외부 등급의 급격한 변동에 대비한 모니터링 강화 및 선제적 리스크 관리 체계를 마련하시기 바랍니다.

⑤ 대주주 관련 신용공여 공시 범위 및 절차 보완

「여신전문금융업법」 제49조의2(대주주에 대한 신용공여한도 등)에 따르면 여신전문금융회사는 그의 대주주에게 일정금액 이상의 신용공여를 한 경우에는 그 사실을 인터넷 홈페이지 등을 이용하여 공시하여야 한다.

회사는 대주주 관련 차주인 A사에 국세 카드납부 용도의 신용공여를 제공하였으나, 해당 거래가 법상 공시 대상*이 아니라고 판단하여 이를 공시에서 제외하였다.

* 기업구매전용카드, 신용카드 회원에 대한 자금의 융통, 할부금융이용액, 대출액, 지급보증액 등

그러나 2025년 초 A사의 회생절차 개시 신청에 따라 세금카드 미납분이 '회생채권'으로 신고되어 실질적으로 일반 대출과 동일한 성격을 갖게 되었는바, 투자자 보호 및 정보 제공 투명성 측면에서 해당 신용공여 현황을 대주주 거래 내역에 포함하여 공시하는 것이 타당하다고 판단된다.

<조치할 사항>

따라서 회사는 A사 회생채권을 대주주 신용공여 공시에 즉시 반영하고, 향후 법적 형식보다 경제적 실질에 따라 대주주 거래 현황을 투명하게 공개하도록 관련 내부통제 체계를 강화하시기 바랍니다.

(3) 금융사고 예방지침 운영 미흡

① 금융사고 예방지침의 내재화 미흡

회사는 2024년 4월 24일 제정된 여신금융협회의 「여신금융업권 금융사고 예방지침」을 회사 내규에 도입하면서 회사의 업무 프로세스나 조직구성 등을 반영하지 않았다.

이로 인해 실무자들이 지침의 취지와 적용 방식을 제대로 인지하지 못하여 지침이 형식적으로 운영되었고, 예방 지침이 실제 시스템과 절차에 반영되지 않아 실효성이 저하된 상태이다.

<조치할 사항>

따라서 회사는 내규 「금융사고 예방지침」의 세부 검토를 통해 주관 부서를 명확히 규정하고, 각 부서 업무 프로세스를 지침에 맞게 수정·보완하시기 바랍니다. 특히 수정된 프로세스가 안정적으로 정착될 수 있도록 상시 점검 체계를 구축하여 금융사고 예방의 실효성을 제고하시기 바랍니다.

② 고위험 직무군 선정 및 핵심 내부통제 관리 부적정

회사 내규에 따르면 금융사고 발생 위험이 높은 직무를 '고위험 직무군'으로 분류하고, 해당 직무 담당자에 대하여 직무분리, 명령휴가 등 강화된 내부통제 절차를 의무적으로 적용하여야 한다.

그럼에도 회사는 부서별 업무 위험도 파악을 소홀히 하여 최근 사고가 발생한 '장기월납서비스' 업무 등 사고 취약 직무를 고위험군에서 누락하였다. 또한 고위험 직무를 체계적으로 선별·관리하는 시스템이 미비하여, 결과적으로 직무분리 및 명령휴가 등 핵심적인 사고 예방 통제가 해당 업무에 적용되지 못하는 결과를 초래하였다.

<조치할 사항>

따라서 회사는 사고 취약 업무인 장기월납서비스 등을 포함하여 고위험 직무군을 전면 재평가하여 선정하고, 선정된 직무에 대해 직무분리 및 명령휴가 등 핵심 사고 예방 절차를 체계적으로 적용·관리하시기 바랍니다.

③ 장기근무 인력 순환배치 및 예외 관리 운영 불철저

회사 내규에 따르면 직원의 장기근무를 제한하고, 불가피하게 예외를 인정하는 경우 회사 내규에 허용 사유를 명시하고 인사담당 임원의 사전 승인 절차를 거쳐야 한다. 또한 매년 적용 배제 직원의 적정성을 평가하여 그 범위를 조정하여야 한다.

그럼에도 회사 인사팀은 2025년 4월 선정된 순환배치 대상자에 대한 구체적 기준 검토 없이 부서 요청에 따라 배제함으로써 실제 순환배치 인원을 축소 운영하였다. 이 과정에서 인사담당 임원의 사전 승인 여부나 사유 명기 등 지침상 필수 절차를 이행하지 않았으며, 회사 내규상 장기근무 허용 사유 정의 및 승인 프로세스도 미흡한 것으로 나타났다.

<조치할 사항>

따라서 회사는 순환배치 예외 인정 시 회사 내규상 구체적 근거 확인 및 인사담당 임원의 사전 승인 등 필수 절차를 엄격히 준수하고, 매년 예외 인원의 적정성을 평가하여 순환배치 제도를 실효성 있게 운영하기 바랍니다.

④ 금융사고 예방 관련 교육 운영 미흡

회사 내규에 따라 금융사고 예방을 위해 연1회 정기적으로 금융사고 예방 지침에 부합하는 업무수행 절차, 윤리의식과 올바른 직업관 등에 대해 교육을 실시해야 한다.

그러나 회사는 카드뉴스를 내부 포탈에 게시하는 것만으로 교육을 종료하여 고위험 직무 담당의 이수 및 법령 숙지 여부에 대한 확인이 곤란하다.

<조치할 사항>

따라서 회사는 금융사고 예방 교육의 실효성을 높이기 위해 교육 이수 현황을 인사 관리 체계와 연계하고, 미이수자에 대한 관리 등 실질적인 사후 관리 조치 방안을 수립 운영하시기 바랍니다.

(4) 리스크관리 관련 내부규정 마련 소홀

회사 내규에 따르면 리스크관리위원회 및 리스크관리협의회는 리스크 관리 관련 내부 규정의 제·개정을 담당하며, 관리 대상 리스크를 정의하고 매년 신용·시장·금리·운영리스크별 한도를 설정하고 있다.

그러나 시장 및 운영 리스크의 인식·측정·관리 방법에 관한 내부 규정 부재로 관리 근거가 미비하고, 위원회와 협의회 간 의결 사항 중복*으로 각 회의체의 역할과 책임이 불분명하며, 운영지침상 개정 권한의 혼재**로 규정 개정 주체가 불일치한다.

* '리스크관리 계획 및 리스크한도 설정' 등 「금융사지배구조법」상 리스크관리위원회의 역할에 대해 리스크관리협의회에서 의결하고 동일한 안건을 리스크관리위원회에서도 의결

** 리스크 관련 운영지침 개정 권한
「리스크관리위원회 운영지침」 : 이사회, 리스크관리위원회
「리스크관리협의회 운영지침」 : 리스크관리위원회, 리스크관리협의회

<조치할 사항>

따라서 회사는 시장 및 운영 리스크의 구체적인 관리 기준을 회사 내규에 명시하여 관리 체계를 보완하고, 각 회의체 간 의결 권한 및 지침 개정 주체를 일원화하여 의사결정 체계의 정합성을 확보하시기 바랍니다.

(5) 법인회원에 대한 경제적 이익제공 금지 관련 관리 미흡

「여신전문금융업법 시행령」 제7조의3(신용카드업자의 금지행위)에 따른 법인회원에 대한 과도한 경제적 이익 제공 제한 규제*를 준수하여야 함에 따라 관련 모니터링 시스템을 마련·운영하고 있다

* (규제1) 총비용의 총수익 초과 금지(「여신전문금융감독규정」 제25조 제8항)
(규제2) 경제적 이익 합산액이 신용카드 연간 이용총액의 0.5% 초과 금지(「여신전문금융감독규정」 제25조 제10항)

그러나 회사는 법인회원에 대한 과도한 경제적 이익제공 금지 규제 관련 회사 내규*를 마련하지 않았고 연중 3회 모니터링 및 1회 사후관리만을 실시하는 등 관리체계가 미흡하며,

* 법인회원에 대한 경제적 이익 제공 기준, 기준 초과여부 점검 방법, 소기업 확인절차 등 구체적인 업무절차를 포괄한 회사 내규 미마련

또한 법인회원에 대한 영업전략 부서가 경제적 이익 모니터링 및 사후관리를 병행하여 이해상충 문제 발생할 소지가 있다.

<조치할 사항>

따라서 회사는 법인회원에 대한 과도한 경제적 이익제공 금지 규제 관련 회사 내규를 마련하고 이에 대한 모니터링·사후점검 주기 확대를 통해 관리체계를 강화하는 한편, 이해상충 방지를 위해 법인카드사업기획팀의 모니터링 결과에 대한 내부통제를 강화하시기 바랍니다.

(6) 불법모집 영업점 점검 및 징계 절차 미흡

① 불법모집 발생영업점의 관리자에 대한 패널티 부과방안 미흡

회사 내규에 따라 불법모집이 발생한 영업점에 인사, 평가상 불이익을 부여하는 등 모집인 관리책임자의 관리·감독 책임을 부과하고, 불법모집 누적 발생건수에 따라 해당 영업점의 관리자에 대한 제재기준을 마련하고 있다.

그러나 불법모집 누적 벌점을 연초마다 초기화하여, 인사상 '주의' 조치가 이뤄져야 함에도 경고장 발송 등 '경징계'로 조치하는 경우가 발생하고 있다.

<조치할 사항>

따라서 회사는 내부제재기준 적용시, 모집인 관리책임자가 책임 있는 감독을 수행할 수 있도록 평가기간을 합리적으로 조정하거나 제재기준을 강화하는 방안을 마련하시기 바랍니다.

② 불법모집 점검부실

회사 내규에 따라 신용카드회원 불법모집에 대한 현장점검을 실시하여야 하고, 이에 따라 회사는 현장점검반을 운영하여 연 1회 이상 영업점포(지점·센터) 및 현장에 대한 점검을 실시하고 있다.

하지만 회사가 점포 및 현장점검 때 활용하는 점검표가 부실*하여 점검의 실효성을 강화할 필요성이 있다.

* ❶전문모집인들이 고객모집에 활용하는 태블릿에 대한 점검기준 미마련, ❷법인회원 모집인·법인 에이전트들에 대한 점검항목 미마련, ❸과다경품 관련 「여신전문금융업법 시행령」 개정사항(2024.5.22. 개정) 미반영 등

<조치할 사항>

따라서 회사는 점포 및 현장점검 시 활용하는 점검표를 연 1회씩 주기적으로 검토하고, 필요시 개선*하여 불법모집 점검의 실효성을 제고하시기 바랍니다.

* ❶전문모집인의 태블릿을 점검하는 항목 신설(고객 개인신용정보 포함 여부 확인 등), ❷법인카드 모집인·에이전트들을 위한 방문판매 관련 점검표 신설, ❸관련 법령 개정사항 반영 등

(7) 전문모집인에 대한 교육훈련 미흡

회사 내규에 따라 모집인을 대상으로 매 분기마다 모집인 교육을 실시하여야 하고, 이에 따라 회사는 센터·지역·법인카드 지점 모집인들을 대상으로 매 분기별 정도영업 준수교육을 실시하고 있다.

하지만 회사는 본사 법인모집인에 대한 교육을 미실시하고 있으며, 전문모집인 교육자료가 미흡하여 이에 대해 개선할 부분*이 있다.

* ❶모집인 위탁계약서 상 명시된 자금세탁방지 교육 미실시, ❷교육자료에 「여신전문금융업법 시행령」 개정사항(과다경품 관련, 2024.5.21. 개정) 미반영 등

<조치할 사항>

따라서 회사는 본사 법인모집인에 대한 교육을 실시하고, 주기적으로 법인모집인 교육자료를 점검·개선하여 전문모집인 교육을 강화하시기 바랍니다.

(8) 카드대출 금리산정 관련 검토 미흡

회사 내규 등에 따라 카드 대출상품에 대한 기준금리*를 분기별로 산정하고, 그 합리성 및 타당성을 가격결정위원회에서 심사하여야 한다.

* 신용·자본·업무·조달원가 및 목표이익률로 구성

그러나 회사는 기준금리의 주요 구성항목인 목표이익률을 산정함에 있어 기본목표이익률 및 조정목표이익률, 등급 차등화 요소를 고려하고 있음에도, 가격결정위원회 안건에서는 조정목표이익률 산출 근거만 별첨으로 포함하고 있을 뿐, 기본목표이익률 및 등급 차등화 요소에 대해서는 산출 근거를 별도로 기재하지 않고 있어 목표이익률 적정성에 대한 충분한 심의가 제한되고 있다.

또한, 가격결정위원회 안건상 당분기 기준금리의 전분기 대비 증감 내역을 기재하고 있으나, 단순 수치를 비교하는 수준에 불과할 뿐 금리 변동에 영향을 미치는 주요 항목 및 증감 사유 등에 대한 내용이 포함되어 있지 아니하여 위원회 차원에서 기준금리 증감 원인 분석 등을 통한 기준금리의 타당성* 등에 대한 관련 충실한 논의가 이루어지기 어려운 측면이 있다.

* 전분기와의 대사를 통하여 구성 항목에 대한 자의적 조정 여부 및 기준금리 변동이 내·외부 환경 변화 중 어디에서 기인하는지 등에 대한 내용 파악 가능

<조치할 사항>

따라서 회사는 가격결정위원회 안건에 목표이익률 산정 근거 및 기준금리 증감 원인 등을 충실히 기재하여 위원회 차원에서 기준금리의 적정성 및 합리성 등에 대하여 충실히 의논할 수 있도록 금리산정 관련 업무 절차를 개선하시기 바랍니다.

(9) 카드대출 등 신용리스크 관리 미흡

회사 내규에서는 개인회원 카드대출 및 신용카드 관련 신용관리 정책 의사결정*을 신용관리위원회에서 수행하도록 정하고 있다.

* 고위험 취약차주에 대한 카드론 한도기준 변경, 특별한도 심사기준 강화 등

그러나 회사는 현재 운영 중인 신용관리 정책의 적정성을 동 위원회 차원에서 주기적으로 점검하는 절차를 마련하고 있지 않아 신용리스크 관련 의사결정사항에 대한 사후관리*가 미흡한 측면이 있다.

* 예를 들어 신용관리위원회가 수립한 '카드대출 취급 거절 기준'(필터링 기준)에 대해 소관 부서에서 실효성 점검을 수행하고 있으나, 점검 결과가 신용관리위원회에 보고되지 않음

<조치할 사항>

따라서 회사는 카드한도 및 카드대출 관련 신용정책이 적정히 운영되고 있는지 신용관리위원회에 차원에서 주기적으로 점검하는 등 신용리스크 관리 절차를 개선하시기 바랍니다.

(10) 집합투자증권 관련 회계처리 검토 미흡

회사 내규에서는 회계담당자가 관계법령 및 회사 사규에서 정하는 바에 따라 신의성실 원칙을 준수하여 그 직분에 따른 회계처리를 적정하게 하여야 한다고 정하고 있다.

그러나 회사는 2025년 중 기관 전용 Ⓑ 사모펀드에 유한책임사원으로 출자하면서, 유한책임사원이 업무집행사원의 투자의사결정 업무에 관여할 수 없도록 정하고 있는 「자본시장과 금융투자업에 관한 법률」상 규제사항*이 지배력 판단에 미치는 영향에 대하여 충분하게 검토하지 않은 채 펀드에 대한 출자지분율만을 기준으로 지배력 보유 여부를 판단**한 사실이 있다.

* 제249조의11(사원 및 출자) ④ 유한책임사원은 기관전용 사모집합투자기구의 집합투자재산인 주식 또는 지분의 의결권 행사 및 대통령령으로 정하는 업무집행사원의 업무에 관여해서는 아니 된다.

** 지배력 검토 관련 자체 점검표상 실무부서(종합금융3팀)에서는 출자 약정서상 회사의 지배력 행사가 제약될 수 있는 고려 사항을 기재하였으나, 검토부서(회계팀)는 해당 내용에 대한 충분한 검토 없이 90% 이상의 지분율을 사유로 지배력을 보유한 것으로 결론

<조치할 사항>

따라서 회사는 집합투자증권에 대한 지배력 보유 여부 판단시 출자지분율 등 양적기준뿐만 아니라 유관 법령에서 정하고 있는 규제사항 등 질적기준까지 충실히 검토할 수 있도록 회계처리 관련 업무 절차를 개선하시기 바랍니다.

(11) 마케팅 행사 관련 수익성 분석 및 내부통제 강화

회사 내규에 의하면 판촉행사 또는 全 회원 대상 이용 증대 캠페인 행사를 실시하는 경우 기대되는 추가 영업수익이 예상되는 비용 이상이어야 실행하는 것을 원칙으로 하고 예외적으로 '경영목적상 필요할 경우' 손익관리위원회에서 달리 정할 수 있다.

하지만 회사는 ㈜ 프로모션을 진행하면서 마케팅 행사로 추가된 영업수익을 계산하는 것이 곤란하다는 사유로 회사 내규에 근거하지 않고 별도의 기준으로 수익성 분석을 실시하였으며, 예외내용과 관련하여 손익관리위원회에서 심의한 내역이 없다.

한편, 내규는 일부 예외를 제외하고 마케팅 행사 실시 前 손익관리위원회의 심의를 거치고, 마케팅 행사의 사후 수익성 분석자료를 손익관리위원회에 보고하도록 규정하고 있으나,

예상 또는 집행비용에 예산 내·외 금액이 혼재되어 있는 경우에 대해서는 규정하고 있지 않아 예산 내·외 금액을 혼용하여 마케팅 비용을 지출한 경우 손익관리위원회 심의 및 보고가 생략되는 건이 있어, 예산 외 금액을 집행하는 마케팅 행사에 대한 손익관리위원회의 내부통제가 미흡할 우려가 있다.

<조치할 사항>

따라서 회사는 마케팅 행사 실시 판단 기준, 손익관리위원회 심의 및 보고 기준을 보완하는 등 회사 내규를 현실화하여 마케팅 행사 관련 수익성 분석 및 내부통제를 강화하시기 바랍니다.

(12) 자금조달 및 운용에 관한 독립적 기준 마련

회사 내규는 유동성리스크 인식·측정·모니터링·보고체계 및 리스크관리 부서의 역할 등을 규정하면서 자금조달 전략 수립 관련 사항은 자금관리 부서와 협업한다고 명시하고 있다.

또한, 재무위원회가 연간 자금조달 및 운용계획의 적정성, 분기별 자금조달 실적 및 시장동향 분석에 대해 심의·의결하도록 역할을 부여하고 있다.

그러나 회사의 내규는 리스크 관점의 관리체계만 규정하고 있어 자금조달 원칙, 거래상대방 관리, 유동성관리 기준, 자금관리 부서의 역할과 책임 등 실무적 조달·운용 기준을 구체화하고 있지 않으며,

자금 운용과 관련해서도 운용기관 선정기준, 한도, 수단 등 핵심 정책이 명문화되어 있지 않아 실무 수행 과정에서 재량이 과도하게 작용할 우려가 있으며, 재무위원회의 심의·의결 사항을 실제 자금조달 및 운용에 일관되게 반영할 수 있는 세부 기준의 부재로 전략과 실무 간 연계성이 미흡하다.

<조치할 사항>

따라서 회사는 현재의 리스크 중심 지침과 별도로 자금조달 및 운용 기준을 독립적으로 제정하여 실무 기준을 명확히 하고, 자금조달·운용의 예측 가능성과 일관성, 책임성을 제고하여 재무위원회의 심의·의결 사항이 실무부서 운영기준까지 유기적으로 연계되도록 관련 프로세스를 정비하시기 바랍니다.

(13) 자금세탁방지 전산시스템 설계·운영 미흡

회사는 내규 등에 따라 금융거래 등을 이용한 자금세탁행위 및 공중협박자금조달행위를 방지하기 위하여 고객에 대해 합당한 주의를 기울여야 하며, 자금세탁행위 등을 할 우려가 있는 경우에는 더욱 엄격한 고객확인을 하여야 한다.

또한, 자금세탁행위 등과 관련된 위험을 식별하고 평가하여 고객확인에 활용하여야 하며, 관련 위험 식별 및 평가 시 국가위험, 고객유형, 상품 및 서비스 위험 등을 반영하고, 해당 고객의 자금세탁행위 등의 위험도가 적정하게 반영되도록 위험 평가요소 및 중요도를 정하여 위험을 평가하여야 한다.

현재 회사는 위험기반접근(RBA) 자금세탁방지 시스템을 구축하여 운영 중으로 고객, 국가, 상품 및 서비스로 구성된 위험 카테고리별 평가와 함께 기존고객에 대해서는 행동위험 정보를 추가로 인식하여 위험을 평가하고, 각 카테고리별 가중치 적용을 통해 종합위험평가점수를 도출하여 이에 따라 고위험·중위험·저위험으로 위험등급을 산정하고 있다. 이렇게 산정한 위험등급에 따라 고위험 고객에 대하여 강화된 고객확인(EDD)을 수행하고 있으며, 위험등급별로 고객확인의 재이행 주기를 설정·운용하고 있다.

하지만 회사가 2019년 8월 신규 구축한 자금세탁방지 시스템은 모든 고객의 위험을 고·중·저로 분류하고 있으나, 계정계(고객정보관리) 시스템에서는 고·저위험으로만 분류하는 등 이원화하여 운영되고 있다. 특히, 자금세탁방지 시스템에서 위험평가 실시 결과 고위험에서 저위험으로 변경된 경우에는 계정계로 데이터를 전송하지 않음에 따라 계정계와 자금세탁방지 시스템간 고객위험평가 결과값이 불일치하는 상황이다.

<조치할 사항>

따라서 회사는 계정계 시스템과 자금세탁방지 시스템간 연계성을 보완하여 동일 고객에 대해 동일한 위험평가가 적용되고 이를 기반으로 고객확인 재이행, 의심거래 보고 등 자금세탁방지 업무가 운용될 수 있도록 전산시스템을 개선하시기 바랍니다.

(14) 강화된 고객확인 업무 운영 부실

회사는 내규 등에 따라 자금세탁행위 등을 할 우려가 있는 경우 더욱 엄격한 고객확인, 즉 실제 당사자 여부 및 금융거래 목적과 거래자금의 원천 등을 확인하는 강화된 고객확인(EDD)을 수행하여야 하는데도 회사는 아래와 같이 강화된 고객확인 운영이 미흡한 사례가 있다.

① 회사는 강화된 고객확인 수행 시 고객의 거래목적 및 자금원천 등 추가 정보를 확인하고 있으나 거래목적을 '기타'로 선택하는 경우 세부 내용을 기재하지 않거나, 자금원천을 '기타'로 선택한 경우 세부 내용을 기재하지 않은 사례가 확인되었다.

② 또한, 직업 정보를 '무직'으로 기재한 개인고객에 대하여 자금원천을 '급여·근로소득 또는 '사업소득'으로 입력한 사례도 있었다.

<조치할 사항>

따라서 회사는 고객확인 수행 시 추가 정보를 '기타'로 선택한 경우 세부 내용을 필수로 입력하도록 회사 내규 및 전산시스템을 개선하고, 고객확인 업무 운영의 적정성을 주기적으로 점검하는 한편, 세부 내용의 충실한 기재를 위해 관련 임직원 교육 및 연수 실시 등 자금세탁방지 업무 관련 내부통제를 강화하시기 바랍니다.

(15) 전화권유판매(TM)를 통한 강화된 고객확인 절차 관련 내규 등 미흡

회사는 자금세탁 위험도가 고위험인 개인 고객을 대상으로 강화된 고객확인을 위해 카드 신규 발급 또는 교체·추가 시 거래목적 및 자금원천을 확인하고 있으나, 회사 내규는 TM 상담과정에서 거래목적이 신용카드 개설로 명확하다는 사유로 TM상담원이 별도 질문 없이 거래목적을 '개인카드 개설' 코드로 입력·유지토록 하고, 자금원천 또한 '직업정보'를 참조하여 TM상담원이 별도 질문 없이 자금원천 코드를 직접 선택·입력하도록 잘못 안내하고 있어 정확한 고객확인이 이루어지지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 TM상담원이 거래목적 및 자금원천을 임의로 입력하지 않고 고객 문의를 통해 이를 확인하도록 강화된 고객확인의 취지에 부합하게 회사 내규를 개정하고 관련 내용에 대한 직원 및 TM상담원 교육을 강화하시기 바랍니다.

(16) 고객확인 업무 소홀

① 기존고객의 국적 변경 시 고객확인 부실

회사는 내규 등에 따라 고객이 계좌를 신규로 개설하거나 일회성 금융거래 등을 하는 경우 고객의 신원에 관한 사항을 확인하여야 하며,

회사가 확인하여야 하는 개인고객의 신원정보를 성명, 생년월일 및 성별(외국인 비거주자의 경우에 한함), 실명번호, 국적, 주소 및 연락처(단, 외국인 비거주자의 경우에는 실제 거소 또는 연락처) 등으로 정하고 있다.

한편, 내규에 의하면 회사는 고객확인을 한 고객과 거래가 유지되는 동안 당해 고객에 대하여 지속적으로 고객확인을 하여야 함에 따라 내국인이 한국 국적을 포기하거나 외국인이 한국 국적을 취득하는 등 기존고객이 국적 변동으로 정보 변경을 요청하는 경우 변경된 국적을 기준으로 실지명의, 주소 및 연락처 등을 확인해야 한다.

하지만 회사는 2022.1.2. ~ 2025.9.30. 기간 중 기존고객이 국적 변동으로 정보 변경을 요청하는 경우 증빙자료 요청 및 확인은 하였으나, 전산시스템상 고객확인 정보(실지명의, 국적, 주소, 연락처)를 변경하지 않은 사례가 있다.

<조치할 사항>

따라서 회사는 중요 고객확인정보 변경 즉시 전산시스템상 등록하도록 절차를 개선하고, 고객확인정보 관리의 적정성을 주기적으로 점검하는 등 관련 내부통제를 강화하시기 바랍니다.

② 법인 고객의 실제 소유자 확인 업무 소홀

회사는 내규 등에 따라 법인 고객의 실제 소유자를 확인하여야 하고, 법인 고객의 실제 소유자에 해당하는 사람을 지정하여 성명, 생년월일 및 국적 등을 확인하여야 하는데, 3단계 절차*를 통해 단계별로 실제 소유자를 파악해야 하고, 단계별 확인절차를 생략한 채 곧바로 3단계인 '법인 또는 단체의 대표자'로 실제 소유자를 지정할 수는 없다.

* 1단계 : 25% 이상의 지분증권을 소유한 사람
2단계 : ①, ②, ③ 중 택일(① 최대 지분증권을 소유한 자, ② 대표자 또는 임원 등의 과반수를 선임한 주주, ③ ①~② 외에 법인·단체를 사실상 지배하는 사람)
3단계 : 법인 또는 단체의 대표자

하지만 회사는 법인 고객의 실제 소유자에 해당하는 사람 중 1단계에 해당하는 '25% 이상 지분증권 소유자'에 해당하는 사람이 있어 관련 자료를 징구하였으면서도 이를 입력하지 않고, 3단계에 해당하는 '법인의 대표자'로 오입력하였다.

<조치할 사항>

따라서 회사는 법인 고객의 실제 소유자 확인 및 근거자료가 일치하도록 관리할 수 있는 절차를 마련하고, 동 절차에 대한 담당 직원 교육을 강화하시기 바랍니다.

(17) 해외 현지법인의 의심스러운 거래 보고 추출기준 관리 미흡

회사는 내규 등에 따라 해외에 소재하는 자신의 지점 또는 자회사의 자금세탁방지 등의 의무이행 여부를 관리하여야 한다.

회사는 현재 베트남에 현지법인 1개(롯데 파이낸스 베트남)가 진출해 있는바, 동 법인은 현지 법령 및 회사 내규 등에 따라 고객확인, 직원알기제도, 직원 교육 및 연수 등 자금세탁방지 업무를 수행하고 있으며,

매월 자금세탁방지업무 활동 현황에 대해 'Monthly AML Report'를 작성하여 본점에 보고하면, 회사 내규에 따라 준법경영팀은 현지법인의 AML 의무 이행 여부를 점검하고 그 결과를 매분기 준법감시인에게 보고 및 관리하고 있다.

한편, 내규 등에 따라 의심스러운 거래의 보고(STR)를 위해 전산시스템을 개발하고 전자금융거래에 대해 주의를 기울여 금융거래 등이 STR 대상인지 효율적으로 확인할 수 있는 방안을 강구하도록 노력하여야 한다.

하지만 베트남 현지법인은 현재 수 개의 STR 추출기준을 마련하여 운영 중으로, 2021.1.1.~ 2024.12.31. 기간 중 일부 추출기준은 STR 경보(alert)가 발생하였으나 거래내역 등 적정성 확인을 통해 베트남 중앙은행(SBV) 보고 대상에서 모두 제외되었고, 일부는 경보가 발생한 적이 한 차례도 없는 등 추출기준의 실효성이 낮은데도 해당 기간 중 추출기준의 임계치 조정 등 적정성 검토가 전혀 이루어지지 않았다.

<조치할 사항>

따라서 회사는 해외 현지법인의 STR 추출기준의 유효성 제고를 위해 신규 추출기준의 도입을 검토하고, 임계치 조정 등 적정성 점검을 강화하는 등 관리·감독을 강화하시기 바랍니다.

(18) 고가의 귀금속 판매상 관련 업종 분류 미흡

내규에 따라 회사는 자금세탁 등과 관련된 고객의 위험을 국가위험, 고객 유형, 상품 및 서비스 위험 등으로 식별, 분류, 평가, 측정하는 체계를 수립·운영하여야 한다.

또한, 고가의 귀금속 판매상 등의 고객은 자금세탁 등의 위험이 높은 고객으로 고려하여 추가정보 확인이 필요한 고객으로 고려하여야 하며, 고위험군에 대하여 강화된 고객확인을 수행하여야 한다.

하지만 회사가 고위험으로 분류한 국내법인 고객 중 일부는 업종이 고가의 귀금속 판매상으로 분류되었으나 실제로는 이와 무관한 의류 제조·판매업 등을 영위하는 것으로 확인되었다. 이는 회사가 한국표준산업분류상 '의복, 의복 액세서리 및 모피제품 제조업(C14)'을 고가의 귀금속 판매상으로 일괄 분류하도록 자금세탁방지 시스템을 구축하고, 이를 운영하면서 실제 영위 업종을 추가적으로 확인하지 않은 데 기인한다.

또한, 회사의 現 업종 분류 기준에서는 고가의 귀금속 판매상에 해당하는 한국표준산업분류상 '시계 및 귀금속 소매업(G4783)' 등이 회사 자금세탁방지 시스템상 고가의 귀금속 판매상(환금성판매상)에 포함되지 않아 고위험군에서 누락될 우려도 있다.

<조치할 사항>

따라서 회사는 한국표준산업분류 내 하위 분류항목을 참고하여 고위험군에 속하는 업종의 세분화 및 추가 자료 징구 등을 통한 실제 영위 업종 확인 등 고객유형 평가가 자금세탁행위 위험도를 충실히 반영할 수 있도록 관련 시스템을 개선하시기 바랍니다.

(19) 정보보호 체계 및 보안인력 관리 미흡

회사 내규에 따라 정보처리시스템의 최신 정보보호 이슈를 지속적으로 수집하고, 주요 보안 취약성에 대한 영향평가 및 보정(패치)작업 등을 수행하기 보안 취약점 관리체계를 마련·운용하고 있다.

그러나, 외부 기관(금융보안원, 제조사 등)의 보안 권고에 대한 구체적인 위험도 분석 기준이나 조치 기한 설정 기준을 마련하지 않았으며, 취약점 조치 이력을 엑셀 등으로 수기 관리하여 누락이나 검증이 제대로 이루어지지 않는 등 관리체계가 다소 미흡*하다.

* 2023.1월~2025.6월 중 발견된 보안 취약점의 전체 건수를 산정할 수 없으며 시스템 미구축으로 추적 관리 곤란

또한, 담당자 퇴직 등에 따른 핵심업무의 공백에 대비한 인력확보·운용 방안을 마련하지 않아 신규 담당자에게 충분한 업무 인수인계 및 관련 직무 전문화 교육이 실시되지 않고 있다.

이에 따라, 보안 취약점이 적시에 조치되지 않아 해킹 등 전자적 침해사고에 노출되거나 미숙한 인력 운용으로 정보보호업무에 차질을 빚을 우려가 있다.

<조치할 사항>

따라서 회사는 보안 취약점의 인지부터 조치까지 전 과정을 체계적으로 관리·추적할 수 있는 정보보호 관리체계(관련 위험도 분석 기준 등 포함)와 업무 인수인계 절차, 교육방안 등을 포함한 인력운용절차를 수립하여 철저히 운영하시기 바랍니다.

또한, 보안 인력의 업무 연속성을 보장할 수 있는 구체적인 인수인계 및 교육 프로그램을 제도화하시기 바랍니다.

(20) 정보자산 통제·관리 체계 미흡

① IT자산 현행화 및 취약점 점검 대상 관리 미흡

회사 내규에 따라 정기적인 실사를 통해 서버 등 IT자산 도입·운용 현황을 파악하고 이를 대상으로 보안 취약점을 점검하고 있다.

그러나, 다량의 IT자산목록이 자산관리시스템 등 전산시스템 아닌 엑셀 파일로 수기 관리되고 있어 기재 누락·오류가 발생하고 있고 취약점 점검 대상 목록이 IT자산대장과 연동되지 않고 별도 관리되고 있어 자산 변동 내역이 적시에 반영되지 않아 취약점 점검 시 중요 서버가 누락될 우려가 있다.

* 2024.8월 기준 IT자산대장 대비 취약점 분석용 목록에서 000대 누락

<조치할 사항>

따라서 회사는 취약점 점검 대상 누락 방지를 위해 IT자산이 적시에 현행화되고 관련 부서에 통지될 수 있도록 방안을 마련하시기 바랍니다.

② IT자산 유지보수 및 보정작업(패치) 관리 미흡

회사 내규에 따라 외부 업체에 위탁하여 전산장비, 프로그램 등 IT자산을 유지보수하고 해당 제조사가 발표하는 성능(기능) 또는 보안 관련 보정작업의 필요 여부를 수시로 검토하고 있다.

그러나, 회사는 정당한 사유 없이 침해사고가 발생한 웹로직 서버 등 전산시스템을 유지보수하지 않거나, 권고되는 보정 작업에 대해 '추후 검토'로만 처리 후 장기간 방치하는 등 관리가 다소 미흡하다.

이에 따라, IT자산이 적정히 관리되지 않고 취약한 상태로 운영되다가 대규모 장애를 유발하거나 정보보안 사고에 쉽게 노출될 우려가 있다.

<조치할 사항>

따라서 회사는 운용 중인 IT자산이 최적의 성능을 발휘할 수 있도록 유지보수 및 보정작업이 이루어지도록 관련 업무절차를 개선하시기 바랍니다.

③ 취약점 점검 결과 검토 및 이행조치 관리 미흡

회사는 내규에 따라 정기적으로 정보시스템의 취약점을 분석하고, 이행조치 계획을 수립하여 최고경영자에게 승인을 받는 등 체계적으로 관리 절차를 운영해야 한다.

그러나, 회사는 외주업체를 통해 취약점 점검을 하는데 동 업체의 결과보고서에 대해 적정성 여부를 검토하지 않아 2024년 하반기 전자금융기반시설 점검에서 온라인결제서버의 '주기적인 보안패치 및 벤더 권고사항 미적용' 항목에 대한 취약점 점검이 실시되지 않았는데도 '양호'로 평가된 사실을 인지하지 못하는 등 취약점 점검을 미흡하게 수행하고 있고

당해 연도에 조치되지 않은 취약점은 이행계획을 수립*하여 차년도로 이월하고 있으나 해당 계획이 지연되더라도 그 사유를 확인하거나 이행계획을 재수립하는 등 보완절차가 미비하다.

* 위험도 및 영향도를 고려하여 단기(2개월), 중기(3개월), 장기(6개월)로 조치기간을 구분

또한, '23년부터 점검 확대로 취약점 조치 대상 건수가 급증*하였는데도 경영진의 관심 및 지원 부족으로 우선순위에 밀려 적시에 조치되지 못한 채 장기간 방치되고 있다.

* (2022년) 0,000개 → (2023년) 0,000개 → (2024년) 00,000개

이와 같이 취약점 점검 및 조치 절차가 전반적으로 미흡하여 정보보안 사고 예방 및 대응이 적정하게 이루어지지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 취약점 점검 결과 보고서의 적정성 검토, 취약점 조치 여부 추적관리 절차를 마련하여 회사 내규에 반영하고 이의 이행실태에 대해 정기적으로 점검하여 경영진에게 보고하는 방안을 마련하여 철저히 시행하시기 바랍니다.

(21) 침해징후 상시 감시 및 접근제어시스템 운영 미흡

정보보안 사고 및 이상징후 등을 탐지, 분석하기 위해 전산자원 모니터링 및 보안관제 체계를 운영하고 있다.

그러나, 회사는 웹방화벽 보안정책 누락으로 웹방화벽의 공격탐지 로그가 보안관제시스템으로 전송되지 않도록 하였고 대용량 트래픽 공격 관련 이상징후를 식별할 수 있는 탐지 규칙을 미설정하여 이상징후 등을 실시간으로 인지하기 어려운 실정이다.

또한, 서버·DB 접근통제시스템은 인가된 PC에 에이전트를 설치하는 방식으로만 구성하여 비인가 단말기를 통해 우회*할 수 있는 등 보안에 취약하고, 일부 명령어 실행 이력 및 결과 내역**을 기록·유지하지 않고 있어 사고 발생 시 원인 규명을 위한 정밀한 사후 분석이 어렵다.

* 접근통제 에이전트가 설치되지 않은 PC의 서버·DB의 접근기록은 기록되지 않음

** 주요 조회 명령어(cat, vi 등) 이외 일부 명령어(tail, ls 등)는 미기록

<조치할 사항>

따라서 회사는 웹방화벽 등 정보보호시스템에서 수집되는 주요 로그는 즉시 탐지 및 통합 분석을 위해 보안관제시스템에 전송되도록 웹방화벽 보안정책을 누락없이 관리하고, 접근통제시스템은 우회 접속이 되지 않도록 개선하며 각종 명령어 실행내역은 모두 기록·유지하는 등 정보보호체계를 개선 및 강화하시기 바랍니다.

(22) 정보보안 운영체제(Secure OS) 적용 및 운영 미흡

주요 정보가 저장된 서버 등 전산시스템에 대해 해킹 방지 및 접근 통제 강화를 위해 정보보안 운영체제(Secure OS)를 설치·운영하고 있다.

그러나, 온라인 결제 웹어플리케이션 서버(WAS) 등 일부 중요 서버는 상기 운영체제 설치가 필요한데도 적용 기준 미비로 누락 되어 정보보안 사고, 비인가자의 접근, 권한 탈취 시도 등 불법행위에 노출될 우려가 있다.

<조치할 사항>

따라서 회사는 중요 서버에 정보보안 운영체제 설치가 누락되지 않도록 적용 기준을 마련하여 철저히 운영하시기 바랍니다.

(23) 정보보호시스템 보안정책 변경 이력 관리 미흡

방화벽 등 정보보호시스템의 보안정책 변경 및 전산자료 복호화 시 그룹웨어(전자결재시스템) 및 작업관리시스템을 통해 신청·승인 절차를 운영하고 처리 이력을 기록·관리하고 있다.

그러나 처리 이력이 항목·유형별로 체계적으로 관리되지 않고 기록의 구체성과 검색 기능 또한 미흡하여 사후 추적성과 업무 효율성이 저하되어 있다.

또한, 그룹웨어에 보관 중인 처리 이력은 중요도를 고려하지 않고 일괄적으로 보존기한(5년)이 설정되어 있어 중요 이력이 파기될 가능성이 있으며, 이로 인해 보안 사고 발생 시 원인 분석 및 책임소재 규명이 곤란해질 우려가 있다.

<조치할 사항>

따라서 회사는 정보보호시스템 보안정책의 처리 이력이 항목·유형·중요도별로 체계적으로 관리되고 중요 이력이 임의 파기되지 않도록 관련 기준 및 절차를 마련하고 전산시스템을 개선하시기 바랍니다.

(24) 고객정보 보관실태 점검 미흡

회사 내규에 따라 지정된 '정보보안점검의 날'에 서버, DB 등 전산시스템을 대상으로 개인신용정보 등 고객정보 보관 현황 및 적정성을 점검하고 있다.

그러나, 외부 인터넷과 접점하는 중간보안구간(DMZ) 내 전산시스템에 한정하여 점검하고 내부망 내 전산시스템은 점검하지 않고 있으며 점검 이력 및 결과를 체계적으로 보관하지 않고 있다.

또한, 담당 부서장(정보보호센터장)에게는 예외 처리내역, 암호화 누락 여부 등 법규 및 회사 내규 준수와 관련된 주요 사항이 아닌 단순 현황만 보고하는데 그치는 등 점검이 형식적으로 운영되고 있다.

<조치할 사항>

따라서 회사는 고객정보를 보관하는 전산시스템을 파악하고 이를 대상으로 주기적으로 실효성 있게 점검*하며 추세 분석이 가능한 기간을 설정하여 점검 이력 및 결과(상세내역 포함)를 보관하시기 바랍니다.

* 대상이 다수일 경우 순환 점검 등 방안 마련

아울러, 점검 결과를 법규 준수 및 리스크 관점에서 분석하여 부서장 등 책임자에게 보고함으로써 내실있는 점검이 수행되도록 개선하시기 바랍니다.

(25) 서버 접속로그 등 가동기록 백업 관리 미흡

회사는 내규에 따라 정보보안 사고 발생 시 사후 추적성을 확보하기 위해 서버 등 전산시스템의 접속내역 등 로그를 자동으로 기록하여 1년 이상 보관하고 있다.

그러나, 담당 부서 중 일부는 로그를 개별 보관하는 등 통합로그시스템에 연동하지 않아 일관성 및 통합성이 확보되지 않고 있으며* 온라인결제 등 일부 대고객 서비스**의 경우 가동기록 등 로그를 별도로 백업하지 않고 있어 해킹 등 보안사고 발생 시 로그가 무단 삭제되어 원인 분석 및 책임소재 규명이 곤란해질 우려가 있다.

* 통합로그시스템에 연동을 요청한 시스템 로그만 보안기술팀에서 관리

** 온라인결제, 기프티샷, DigiLOCA, 커머스 등

또한, 데이터 복구에 필요한 서버 설정 파일, 시스템 파일 등은 소산하지 않고 있고 복구훈련 대상에도 포함하지 않고 있어 실제 재해 발생 시 복구에 차질을 빚을 우려가 있다.

<조치할 사항>

따라서 회사는 각 정보처리시스템의 주요 로그는 통합하여 관리하고 데이터 복구에 필요한 설정 파일 등은 데이터와 함께 별도로 백업하며, 재해복구훈련 시 복구 가능 여부를 검증하는 등 전산자료 백업·복구체계를 개선하시기 바랍니다.

(26) 정보보호부문 자체감사 실효성 미흡

회사 내규에 따라 정보보호 자체감사인(1명)을 지정·운영하고 자체감사를 통해 정보보호업무 적정성 점검을 위해 체크리스트*를 마련하고 있으나, 점검 항목의 열거에 그치고 점검 범위·방법 등에 대한 구체적인 기준이 마련되어 있지 않다.

* (정보보호 점검리스트) 보안기획, 보안교육, 취약점 분석 등 19개 항목

또한, 자체감사인은 미조치 취약점이 조치 완료 시까지 추적·관리되지 않는데도 개선 요구를 하지 않는 등 정보보호업무 수행의 적정성에 대한 검토가 충분히 이루어지지 않고 있다.

<조치할 사항>

따라서 회사는 정보보호 자체감사의 실효성을 제고하고 정보보호업무의 적정성을 종합적으로 검토할 수 있도록 '정보보호 점검리스트'에 점검 범위·방법·기준 등을 구체적으로 명시하며 이를 토대로 자체감사가 일관되게 수행되도록 관련 업무절차를 개선하시기 바랍니다.

(27) 원격접속 승인 절차 및 운영 통제 미흡

회사 내규에 따라 재택근무 및 긴급 사용 등 필요시 소속 부서장의 승인을 받아 원격접속시스템에 접속을 허용하고 일정시간 사용하지 않는 경우 접속이 강제 종료되도록 하는 등 보안통제*를 운영하고 있다.

* 백신 프로그램 설치, 원격접속 기록 및 저장, 원격접속자에 대한 보안서약서 징구, 원격 접속 후 일정 유휴시간 경과 시 네트워크 연결 차단 등

그러나, 부서장 이외에도 팀원도 승인이 가능하고 특히, 외주직원의 경우 내부 직원이 아닌 외주업체 팀장이 승인하도록 운영하는 등 메뉴얼과 다르게 운영되고 있으며

시스템에 오류*로 인해 원격접속 종료시간이 부정확하게 기록되고 있는데도 이에 대한 적정성 점검을 실시하지 않아 해당 오류를 인지하지 못하는 등 취약하게 운영하고 있다.

* 실제로 원격 세션은 끊어졌으나 종료 시간이 업데이트되지 않음

이에 따라, 비인가 또는 불필요한 원격접속이 허용될 가능성이 있으며 보안사고로 이어질 우려가 있다.

<조치할 사항>

따라서 회사는 원격접속 승인 절차 등을 회사 내규로 정비하고 관련 신청·승인 및 접속내역의 적정성에 대해 정기적으로 점검*하시기 바랍니다.

* 전산시스템 장애 및 오류 조치, 프로그램 변경 등 중요 작업의 경우 해당 작업 내역까지 연계하여 전반적으로 이상 여부를 확인

(28) 퇴직자의 전산시스템 접근권한 삭제 관리 미흡

회사 내규에 따라 퇴직자의 전산시스템 접근권한이 즉시 자동 삭제되도록 계정관리시스템을 구축하고 인사정보와 전산시스템을 연동하여 운용하고 있다.

그러나, 계정관리시스템은 퇴직 발생 시 사용자 권한을 회수하고 계정 삭제 명령을 연동된 전산시스템에 전송하고 있으나 삭제 결과는 회신받지 않고 있어 실제 삭제 여부를 쉽게 확인할 수 없고 자체 감사자도 사후 점검 시 삭제 여부에 대한 확인을 별도로 하지 않고 있다.

이로 인해, 일부 퇴직자 계정은 사용 권한이 모두 회수되어 시스템 접근은 불가하나 계정 자체는 시스템에 잔존한 사례가 있었으므로 계정 삭제 처리 결과에 대한 사후 검증체계가 미흡하였다.

<조치할 사항>

따라서 회사는 퇴직자의 접근권한 삭제 요청·결과·내역 등을 체계적으로 확인할 수 있도록 계정관리시스템을 개선하고 자체감사 시 이에 대한 적정성을 정기적으로 점검하시기 바랍니다.

(29) 오픈소스 소프트웨어 관리체계 미흡

회사 내규에 따라 오픈소스 소프트웨어(이하 '오픈소스') 0,000종을 도입·운용하고 있고 각 부서는 사용하는 오픈소스의 버전, 라이선스 등 명세를 작성하여 정기적으로 현행화하여 관리하고 있다.

그러나, 회사는 오픈소스 관리를 위한 총괄부서를 지정하지 않고 있고 부서별 담당자가 일부 지정되지 않은 상태로 운영하고 있으며 오픈소스 도입시 법률 검토, 제조사 기술지원 여부 및 보안 취약점에 대해서도 관리하지 않는 등 오픈소스 도입·운용 전반에 대한 관리가 미흡하다.

이에 따라, 사용 중인 오픈소스가 알려진 취약점을 이용한 보안사고에 노출되거나 라이선스 위반에 따른 법적 분쟁이 발생할 우려가 있다.

<조치할 사항>

따라서 회사는 오픈소스 총괄부서 및 부서별 담당자를 지정하여 정기적인 점검을 통해 전사적인 사용 현황과 취약점 등을 체계적으로 파악하고 회사 내규에 점검 대상 및 주기, 법률 검토 요건 및 취약점 심각도별 조치 방법 등 관리에 필요한 절차를 명확히 규정하는 등 오픈소스 관리체계를 개선하시기 바랍니다.

(30) 전산시스템 성능관리 미흡

회사 내규에 따라 사내 클라우드시스템(AAA)* 등 전산시스템의 자원별(CPU, 메모리 등) 임계치를 설정하여 사용 현황을 성능모니터링시스템(BBB)을 통해 실시간 확인하고 있다.

* 2018년 구축, 계정계(00개) 및 채널계(00개) 업무 전반에 사용 중

그러나, 임계치가 추이 등 현황 분석 없이 권고치보다 높게 설정*되어 이상징후를 조기에 파악하기 어렵고 클라우드시스템에 대해서는 임계치나 성능 단계별 대응방안을 마련하지 않고 있다.

* (여신금융협회 가이드라인) 정상 : 70% 미만, 주의 : 70～75%, 경계 : 75～80%, 심각 : 80% 초과
(롯데카드) 정상 : 80% 미만, 주의 : 80～90%, 경고 : 90～95%, 심각 : 95% 초과

또한, 경계(90% 초과) 또는 심각(95% 초과) 단계가 '10초 이상' 유지되는 경우 담당자에게 문자메시지(SMS)로 통보되고 담당자는 이를 최고정보책임자(CIO)에게 보고하도록 운영하고 있는데 '10초 미만'의 상태가 반복되면 이상징후를 인지하기 어려운 한계가 있으며

네트워크 장비는 사용률(회선 등)이 경계(90% 초과) 또는 심각(95% 초과) 단계에 도달해도 문자메시지(SMS) 통보 대상에서 제외되어 담당자가 이를 인지하지 못해 최고정보책임자(CIO)에게도 보고 되지 않고 있다.

이용자가 급증하는 대형 이벤트에 대비한 협의 및 사전 테스트 절차가 부재하고 기간별 사용량 추이 분석도 체계적으로 실시되지 않는 등 성능관리 체계가 미흡하다.

이에 따라, 전산 자원의 용량 부족 등으로 주요 정보처리시스템에 장애가 발생하거나 신속한 장애 대응을 하지 못할 우려가 있다.

<조치할 사항>

따라서 회사는 모든 전산시스템에 대해 업무 특성을 고려하여 적정한 임계치를 설정하고 임계치가 경계·심각단계에 도달하는 경우 예외 없이 담당자에게 통보하며 경영진 보고, 전산 자원 증설 등 각 임계치 단계별 대응방안을 철저히 이행하시기 바랍니다.

(31) 위탁, 제휴 외주업체 리스크 관리 미흡

회사는 내규에 따라 전자금융업자 등 외부업체에 위탁·제휴하여 운영 중인 간편결제, AI 상담 챗봇 등 대고객 서비스 관련 업무를 포함하여 비상계획을 수립·운영하고 있다.

그러나, 비상계획 수립을 위한 핵심업무 선정 과정에서 핵심업무와 연계된 해당 외부업체의 폐업, 전산시스템 장애 등 운영리스크로 인한 업무 영향도를 분석하지 않고 있고 비상시 서비스 복구를 위한 비상연락망, 관련 시스템의 구성도 관리 및 복구절차 마련 등 대응체계 마련이 미흡하다.

이로 인해 해당 업체의 서비스 장애 시 주요 서비스를 신속히 복구하지 못할 우려가 있다.

<조치할 사항>

따라서 회사는 핵심업무에 영향을 주는 위탁·제휴 서비스를 식별하고 장애 발생 시 신속한 복구를 위해 대체 수단 유무를 고려하여 비상복구대책을 마련(관련 시스템·네트워크 구성도, 비상연락망 포함)하여 정기적으로 현행화하는 등 위탁·제휴 외주업체에 대한 리스크 관리방안을 마련하여 시행하시기 바랍니다.

(32) 프로그램 검증 조직 및 테스트 결과 관리 미흡

여신금융협회의 「프로그램 통제 공통 가이드라인」에 따르면 프로그램 검증 조직은 IT개발 경력이 10년 이상인 인력으로 구성하되 해당 인력이 부족한 경우 최고정보책임자(CIO) 등 개발 담당 임원의 승인하에 조정할 수 있으며 프로그램 테스트 시 결과서를 작성하도록 권고하고 있다.

그러나, 프로그램 검증조직 중 일부(0명)는 경력 10년 미만의 인력으로 구성되었는데도 담당 임원은 이를 인지하지 못하고 있으며 프로그램 테스트 결과를 작업관리시스템에 등록 시 테스트 결과서 및 관련 증빙을 누락하는 등 관리가 미흡하다.

이에 따라, 프로그램 검증의 실효성이 저하되어 오류 및 취약점이 충분히 식별되지 못해 장애 예방 및 사후 검증이 곤란할 우려가 있다.

<조치할 사항>

회사는 프로그램 검증 조직에 대한 인력 자격 요건, 업무 범위·방법 등 운영·관리절차를 마련하여 회사 내규에 반영하고 테스트 관련 증빙, 결과서 등 중요 자료가 누락되지 않도록 철저히 관리하시기 바랍니다.

(33) 전산센터 저장매체 반입·반출 통제 미흡

회사 내규에 따라 하드디스크 등 저장매체는 반출할 경우 주요 정보를 복구할 수 없도록 삭제·폐기하고 반입 시에는 바이러스·악성코드를 검사하는 등 보안조치를 이행하여야 한다.

그러나, 하드디스크 등 저장장치의 전산자료 완전 삭제 여부를 확인하지 않고 외부로 반출하거나 서버 운영체제 보정작업 등을 위해 반입하는 USB 등 이동형 저장장치에 대해 악성코드 검사를 실시하지 않는 등 관리·통제가 미흡하다.

이에 따라, 하드디스크, USB메모리 등 저장매체를 통한 중요 정보의 유출이나 악성코드 감염 등으로 이어지는 보안사고가 발생할 우려가 있다,

<조치할 사항>

따라서 회사는 전산센터의 저장매체 반출·반입과 관련한 전산자료 삭제 확인 및 악성코드 검사 절차가 철저히 이행되도록 관련 보안통제를 강화하시기 바랍니다.

(34) 정보보호실무위원회 운영 미흡

회사 내규에 따라 정보보호위원회 안건을 사전에 검토하고 주요 실무사항을 협의하기 위해 '정보보호위원회에 상정 안건 및 기술에 관한 사항' 등 업무에 대해 정보보호실무위원회(위원장 1인 포함 총 5명)를 통해 심의·의결토록 하고 있다.

그러나 회사는 검사대상기간 중 정보보호위원회를 32회 개최하여 동 위원회에 상정된 안건 80건 중 75건이 실무안건에 해당하는데도 동 실무위원회를 개최하지 않는 등 운영이 미흡하였다.

이에 따라, 정보보호 관련 실무부서의 충분한 사전 검토와 의견 수렴이 이루어지지 않아 관련 리스크 및 보완 필요사항이 반영되지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 정보보호실무위원회를 통한 안건 사전 검토 및 의견 수렴 절차를 정착시킬 수 있도록 방안을 마련하여 정보보호 관련 의사결정의 실효성을 제고하시기 바랍니다.