제재내용 공개안

1. 금융기관명 : 삼성생명보험(주)

2. 제재조치일 : 2026. 1. 13.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 13건, 개선 6건

4. 제재대상사실

가. 경영유의사항

(1) 보수위원회 운영 강화 필요

회사는 내규「보수위원회규정」등에 따라 임직원의 보수와 관련한 사항을 심의·의결하기 위해 보수위원회를 운영하고 있으며, 해당 내규는 보수의 결정 및 지급방식에 관한 사항, 보수지급에 관한 연차보고서의 작성 및 공시에 관한 사항, 보수정책에 대한 의사결정 절차와 관련된 사항을 각각 심의·의결하도록 정하고 있으나,

회사는 보수위원회 심의·의결 사항에 대하여 안건을 상정할 때 보수정책, 보수체계의 설계 및 운영, 보수지급에 관한 연차보고서 등 각각의 안건으로 의사결정이 필요한 사항을 매년 2월 '보수체계 평가의 건'이라는 하나의 안건으로 통합하여 의결하고, 약 20페이지로 구성된 보수체계 연차보고서를 슬라이드 한 장으로 요약하여 보수정책, 보수체계 운영 등 안건과 일괄 심의·의결하고 있으며,

보수위원회 위원이 관련 안건을 충분히 검토한 후 의사결정할 수 있도록 사전에 충분한 시간을 두고 안건을 미리 통지해야 하는데도, 내규상 보수위원회 개최 24시간 전에 통지하도록 규정하고 있어 보수위원회 개최에 임박하여 안건을 통지함으로써 위원들이 안건내용을 충분히 검토하지 못하고 안건을 심의·의결할 우려가 있고,

한편 2019～2023년 사내이사가 보수위원회 위원으로 포함되어 운영되면서 사내이사가 본인의 성과평가 및 보수책정에 대하여 의결권을 행사한 사례가 있어 보수위원회의 객관성 및 공정성이 훼손되어 운영된 사실이 있으므로,

회사는 보수위원회 심의·의결 사항에 대하여 위원들이 충분히 검토한 후 의사결정할 수 있도록 각 사안별로 구체적인 정보를 제공하고, 보수위원회 개최 전 충분한 시간을 두고 안건을 통지하여 보수위원회 운영이 객관성 및 공정성을 확보할 수 있도록 업무절차를 강화하시기 바람

(2) 차익거래 계약 관련 내부통제 철저 필요

회사는 차익거래를 위한 허위·가공계약을 방지하기 위해 2023. 7월 차익거래* 방지시스템을 도입하여 상품출시 이전 과도한 수수료 및 시책 지급에 따른 차액발생 여부를 보험계약의 전 기간 보험료 납입 회차별로 점검하고 있으나,

* 과도한 수수료 및 시책 지급으로 계약해지시 이익(수수료+시책+해지환급금-납입보험료-환수금>0)이 발생하는 계약

일부 상품의 경우 높은 시책을 책정하여 보험료 납입 25회차(제3보험상품) 또는 37회차(생명보험상품) 이후 차액이 일부 발생할 수 있는데도 구체적인 대응방안을 마련하지 않았고,

또한 회사는 차익거래가 의심되는 계약의 모집설계사에 대한 사후적인 내부통제*를 정하고 있으나 검사대상기간 중 차액거래가 11,929건(자기계약 1,214건)이나 발생하였는데도 실제 차익거래 현황에 대한 모니터링 및 제재조치 등이 부족한 상황이므로,

* 자기계약을 반복해지한 설계사가 신계약(자기계약) 모집시 지점장 승인 후 접수 및 월말 3일 이내에는 청약접수 불가

회사는 보험계약 전 회차에 걸쳐 실제 차익거래가 발생하지 않도록 차익거래 방지 시스템을 보완하고, 차익거래 방지를 위한 내부통제가 실효성 있게 운영되도록 업무절차를 강화하시기 바람

(3) 자회사GA 물품구입 비용 지급 관련 통제절차 강화 필요

회사는 마케팅 운영(안)*에 따라 자회사인 A 보험대리점 소속 보험설계사들이 보유·관리 중인 고객을 대상으로 2019.11.1.~2024.5.31. 중 모집업무 위탁계약서 등에 정해진 수수료 외에 신상품 마케팅 업무수행 등을 위한 고객제공 물품구입 비용 중 일부인 총 12.5억원을 지원한 사실이 있고,

* 프리미엄 고객사랑서비스 : 회사 전속 및 A사 소속 보험설계사 등을 대상으로 이들이 모집·수금 관리 중인 보유고객을 유형화하여 보험설계사들로부터 방문 및 물품 전달 고객을 신청받고 물품 구입비용의 일부(건별 5천원)를 회사가 판매업체에 직접 지급하는 방식으로 비용 지원 (차액은 해당 보험대리점 소속 보험설계사가 부담 (수수료에서 공제))

한편 회사는 프리미엄 고객사랑서비스 제공으로 인한 해당 고객의 유지율 개선 등 성과에 대한 적절한 검토를 수행하지 않은 채, 보험대리점 중 자회사 GA만을 대상으로 동 서비스를 운영하고 있어 보험대리점 간의 공정한 경쟁 질서를 저해할 우려가 있으므로,

회사는 프리미엄 고객사랑서비스를 운영함에 있어 유지율을 포함한 성과분석을 주기적으로 실시하는 등 서비스 운영에 대한 내부통제를 강화하시기 바람

(4) 불건전한 영업행위에 대한 사전 통제절차 미흡

회사 내규「금융소비자보호기준」등에 따르면 금융소비자 담당부서는 소비자 불만을 근본적으로 해소하기 위해 민원예방 및 해소방안을 수립하여 정기적으로 경영진에게 보고하여야 하고, 민원·분쟁이 빈번하게 발생하는 주요 원인을 파악하여 제도개선 사항을 도출하고 관련 부서장에게 제도개선을 요청하여 개선 여부를 관리하여야 하며, 주요 민원·분쟁에 대한 대응결과를 금융소비자보호 내부통제위원회에 상정하여야 하나,

2020~2023년 중 전체 보험상품의 평균 불완전판매비율은 0.11%로 생명보험회사 전체 평균(0.OO%)보다 높은 수준이어서 그 원인을 파악하고 개선방안을 마련하는 등 불완전 판매를 차단하기 위한 노력이 필요한 상황인데도 금융소비자보호 내부통제위원회 보고 사항에 대한 구체적인 기준이 없어 원인 및 개선방안 등을 동 위원회에 보고하지 않았고,

특히 경영인정기보험의 불완전판매비율*은 2023년 1.37% 등으로 수년간 전체 보험 상품의 평균 불완전판매비율 보다 ○○배 이상 높은데도 관련 사항만 2022.1월 소비자 보호 내부통제 임원실무위원회, 2022.4월 금융소비자보호 내부통제위원회에서 각각 1회씩

논의하는데 그쳤고 이후 관련 부서에 제도개선을 요청하거나 민원 및 불완전판매율의 개선상황을 관리하는 등의 조치가 없었음

* (2020년) 1.47% → (2021년) 1.18% → (2022년) 1.40% → (2023년) 1.37%

또한 경영인정기보험은 타 상품 대비 과다한 차익거래가 발생할 수 있도록 수수료 체계가 구성되어 있어 수수료를 노린 허위·작성계약과 불완전판매계약이 다수 발생할 가능성이 있으므로 판매 전후 지속적으로 주의를 기울일 필요가 있는데도 2024.4월 이후에야 일부 보험대리점만을 상대로 프로모션 지급을 감액하는 등 적극적인 조치를 취하지 않았으므로,

회사는 불완전판매비율이 생명보험회사 전체 평균보다 높은 이유를 분석하고 이에 대한 개선방안을 마련할 필요가 있으며, 특정 보험상품 등에 불완전판매비율이 높거나 민원발생이 많은 경우 그 원인을 파악하고 적극적인 대책을 마련하여 경영진에 보고하는 등 업무절차를 강화하시기 바람

(5) 최적가정 설정 업무 운영 강화 필요

회사는 내규「가정 산출매뉴얼」및「회계정책서」에 따라 보험부채를 평가할 때 편의 없는 최적가정을 설정해야 하며 개별 보험계약을 적절한 보험포트폴리오에 귀속시켜야 하나

보험부채 평가 시 사용하는 계리적 가정 중 해지율 및 갱신율은 보험계약자의 계약자행동(탈퇴)과 관련한 현금흐름 추정 시 사용되므로 동일한 개념을 바탕으로 산출식을 설정하는 것이 합리적인데도, 해지율은 응당유지보험료[1]를, 갱신율은 계약건수를 기반으로 각각 산출[2]하고 있으며, 또한 응당유지보험료는 동일한 보험가입금액일지라도 보험료 납입기간에 따라 상이하게 계산되므로 실제 계약자 탈퇴와 관련된 현금흐름을 합리적으로 반영하지 못할 가능성이 있고,

1) 보험계약이 해지되지 않을 경우 회사 내로 유입 예정인 영업보험료

2) 해지율 = $\frac{\text{해지보험료}}{\text{응당유지보험료}}$, 갱신율 = $\frac{\text{갱신건수}}{\text{갱신대상건수}}$

보험상품 포트폴리오 구분은 상품 단위로 수행하며 주된 위험을 기준으로 개별 보험계약을 포트폴리오(사망, 건강, 금융)에 귀속시키고 있으나, 사망위험을 주로 담보하는 일부 유배당 보험상품을 사망 포트폴리오가 아닌 건강 포트폴리오로 잘못 귀속시켜 공시자료 및 업무보고서 상에서 보험회사별 비교가능성을 저해하는 측면이 있으므로,

회사는 내규에 근거하여 최적가정에 대한 가정산출방법론을 검토하고 현금흐름 산출모델을 개선하고, 주된 위험을 기준으로 개별 보험계약을 적절한 포트폴리오에 귀속시켜 공시자료 및 업무보고서를 정확히 작성할 수 있도록 업무절차를 강화하시기 바람

(6) 금리인하 요구권에 대한 소비자 안내 강화 필요

회사는 대출을 받은 고객이 금리인하를 요구하는 경우 고객의 신용상태 개선 여부를 점검하여 기존 대출금리를 인하하고 있으며, 전 차주에 대하여 금리인하 요구권을 정기적(연 2회)으로 안내하는 한편 신용도가 높아진 차주 등 금리인하 대상고객을 선별하여 반기 1회 이상 선제적으로 추가 안내하고 있으나,

회사가 금리인하 대상고객에게 선별적으로 안내하고 있는 내용이 정기안내와 유사한 문구*를 사용하고 있어 고객이 스스로 금리인하대상자임을 인지하기 어려운 측면이 있으므로

* **(정기안내)** 삼성생명에 금리인하를 요청하실 수 있어요. 신용평점을 올릴 수 있는 제도도 같이 확인해 보세요
(선별안내) 삼성생명에 금리인하를 요청하실 수 있어요. 신용평점 개선은 요구권 수용의 주요항목으로, 신용평점 개선이 있을 경우 신청을 권해드려요

회사는 금리인하가 가능한 고객에게 선별적으로 안내할 때 고객이 금리인하 대상자라고 인식할 수 있도록 안내문구를 개선하시기 바람

(7) 상장주식 자산운용 절차 관리 강화 필요

회사는 보유자산의 효율적인 운용을 통한 장기적·안정적 자산 가치 향상을 위해 국내외 채권, 외환파생상품 등의 보유자산 대부분을 자산운용사에 위탁하여 운용하고 있으며 일부 상장주식만 직접 운용하고 있고

회사가 직접 운용하는 상장주식의 경우 개별주식 운용계획 또는 신규투자 대상 선정(안) 등을 문서로 작성하여 담당 임원에게 보고한 후 이를 근거로 보유하고 있는 상장주식을 매각하거나 신규 매수하고 있는데

문서 상 자산운용계획과 실제 자산운용내역에 차이가 있는데도 검사대상기간 중 작성된 상장주식 관련 검토문서 20건 중 문서관리대장에 등록된 것은 3건으로, 등록되지 않은 17건의 문서는 전결권자의 최종 승인 여부를 확인할 수 없고

동 문서에 의해 개별주식을 매각하거나 매수를 추진하는 과정에서 의사결정이 변경된 사례가 다수 존재하나, 이에 대한 변경사유 및 최종 의사결정자 등에 대해서는 기록·관리하지 않고 있으므로

회사는 효율적인 자산운용을 위해 상장주식의 평가, 보유, 매각 등 사후관리 업무에 대한 의사결정이 합리적이고 투명하게 이루어질 수 있도록 의사결정에 대한 이력관리 등을 강화하시기 바람

(8) 수익증권 자산건전성 분류 기준 강화 필요

회사는 내규 「자산건전성 분류 및 대손충당금적립 기준」 및 「자산건전성 분류 및 대손충당금적립 지침」에 따라 회사가 보유한 투자자산에 대해 자산건전성을 5단계로 분류하고 있는데, 자산건전성 분류는 기준일에 회사가 보유한 정보를 최대한 반영하여 분류할 필요가 있음에도

회사는 수익증권의 자산건전성 분류와 관련하여 2023년 말까지는 정량적 기준인 수익증권의 순자산가치(NAV) 하락기준만을 반영하고 있어, 경제적 실질을 반영할 시 고정 이하로 분류할 필요가 있는 수익증권이 정상 또는 요주의로 분류되었다가 부실이 현실화되었을 때는 장부에서 제거되는 현상이 발생하는 등 투자자산의 건전성 분류가 적시에 이루어지지 않았고

또한 회사는 2024.3월말 부터는 대체자산 자산건전성 분류시 정성적 기준*도 반영하도록 내규를 개정하였으나, 개정 이후에도 정성적 위험 요인을 인지한 수익증권을 '정상'으로 분류하는 등 자산건전성 분류업무에 미흡한 부분이 있으므로

* 지속적인 이자 배당 중단 등 연체 여부, 부도 발생 여부, 수익증권 기초자산의 부실화 여부 등

회사는 수익증권 자산건전성 분류 시 투자자산의 부실 여부를 판단할 수 있는 정성적 요소를 적시에 반영하여 자산건전성 분류가 정확히 이루어질 수 있도록 관련 업무절차를 강화하시기 바람

(9) 외부 위탁운용사 평가체계 강화 필요

회사는 내규「일반계정 아웃소싱 운용사 선정 및 관리지침」등에 따라 투자일임 계약을 체결한 외부 위탁운용사에 대해 연 1회 정기평가를 실시하고 있으며, 동 평가 점수를 바탕으로 매년 외부 위탁운용사를 선정하고 있고, 또한 정기평가 점수가 2회 연속 70점을 하회하거나 운용사의 핵심 역량이 현저히 저하되는 경우 등을 제외하면 별도의 외부 위탁운용사 선정 과정 없이 기존 계약을 유지 및 연장하고 있음

이러한 평가체계가 효과적으로 작동하기 위해서는 평가항목별로 구체적인 기준이 마련되어야 하고 평가근거를 철저히 기록·관리하여야 하며, 손실이 발생하는 등 운용성과가 미흡한 경우 이를 점수에 반영하는 것이 바람직하나

회사는 정량평가의 기준이 되는 벤치마크 수익률 산출기준을 규정화하지 않았고, 정량평가 시 국내채권 및 주식 운용에 손실이 발생해도 일정한 점수를 부여①하고 있으며, 또한 정성평가 시 구체적인 평가근거 없이 단 한 줄의 평가의견으로 높은 점수②를 부여하고 있어 평가가 관대화되어 신뢰성을 해칠 우려가 있으므로

① 성과를 금리차로만 평가하고, 손실에도 기본 점수(일반계정 : 4.5점, 특별계정 8점)를 부여
② 2023년 B사의 일반계정 정성평가 점수(40점 만점)는 국내채권 38.0점, 해외채권 36.3점, 주식 36.6점, PE 37.9점

회사는 외부 위탁운용사 평가 시 객관성 및 공정성을 확보하기 위해 벤치마크 수익률 산출기준을 규정화하고 철저히 기록·관리하는 한편, 운용상 발생한 손실을 평가항목에 반영하는 등 정량평가의 기준을 합리화하고 정성평가 시 평가 근거를 구체화하는 등 평가체계를 강화하시기 바람

(10) 심사역협의회 운영 철저 필요

회사는 내규「융자운용지침」등에 따라 여신심사위원회의 예외 승인이 필요한 주택담보대출에 대한 승인 업무를 수행하기 위해 심사역협의회를 설치·운영하고 있고

심사역협의회의 예외 승인 업무가 철저하게 이루어지기 위해서는 구체적인 협의회 구성 및 운영 기준이 마련되어야 하고, 예외 승인이 필요한 대출은 심사역협의회 구성원의 충분한 논의를 거쳐 결정하는 것이 바람직하나

동 내규에서 심사역협의회는 심사부서장 외 전문심사역 2인으로 구성한다고 정했을 뿐 구체적인 구성원 자격기준을 마련하지 않은 채 심사부서장이 임의로 지정한 직원을 전문심사역으로 선정하여 예외 승인 업무를 수행하고 있으며, 심사역협의회를 대면 개최하지 않고 전산시스템을 통해 심사서류 및 증빙을 확인하고 결재하는 형태로 동 협의회를 운영하면서 한 줄의 심사역 의견을 근거로 구성원 합의를 득하여 예외 승인을 결정한 사례가 있어 합리적 심사근거를 확인하기가 어려운 실정이므로

회사는 심사역협의회 구성 및 운영 기준을 마련하는 한편, 대면 회의를 개최하고 안건을 문서화하는 등 심사역협의회 운영 관련 업무절차를 강화하시기 바람

(11) 지급여력비율(K-ICS) 산출·검증 업무 강화 필요

회사는 「보험업감독업무시행세칙」 [별표22]에서 정한 방법에 따라 K-ICS비율, 시장·신용위험액을 산출해야 하는데

회사는 2023.3월말~2024.3월말 시장위험액 중 주식위험액을 산출하면서 '주식형 레버리지 펀드 또는 레버리지 전략 추구 헤지펀드'에 대해서는 별도의 산식*에 따른 충격수준을 적용해야 하는데도 기타주식에 대한 충격수준(49%)을 적용하여 시장위험액을 과소 산출하였고

* Max{Min(약관상 최대레버리지비율 ×35%, 100%}, 49%} 또는 100%

같은 기간 신용위험액 산출 시 부동산PF 익스포져 등급을 잘못 분류하여 신용위험액을 과소산출하였으며, 최신 통계가 반영되지 않은 신용위험계수를 적용하는 등으로 LTV 등이 산출 가능한 담보부자산(기업담보대출)의 신용위험액을 과대 산출하여

종합하면 회사는 2023.3월말~2024.3월말 시장위험액을 2,396~5,911억원 과소 산출, 신용위험액을 50~81억원 과대 산출하였으며, K-ICS비율을 0.89~2.89%p 과대 산출하였으므로

회사는 시행세칙에 정해진 바에 따라 정확하게 시장·신용위험액 및 K-ICS비율 등을 산출할 수 있도록 정합성 검증 관련 업무절차를 강화하시기 바람

(12) 대고객서비스 관련 프로그램 관리 강화 필요

회사는 내규 「변경관리지침」에 따라 프로그램 개발 시 단위테스트, 통합테스트 및 인수테스트 절차를 거치도록 하고, 내규 「장애대응 관리지침」에 따라 발생한 전산장애의 원인, 등급 및 귀책, 재발방지대책 등을 장애관리시스템에 등록·관리하고 있으나

「금융IT 안전성 강화 가이드라인」*에서 대고객서비스 관련 프로그램 개발 시 사전 영향도 분석을 실시하고 그 결과에 따른 리스크를 테스트 시 반영하는 절차를 운영하도록 권고하고 있으나 동 절차를 운영하지 않고 있고

* 2023년 11월 금융감독원에서 전산사고의 주요 원인인 프로그램 오류, 비상대책, 성능관리에 대한 최소한의 기준을 제시하고자 IT검사 및 모범사례 등을 기반으로 마련한 권고사항

또한, 현업부서의 프로그램 개발 요청내용이 부실하거나 현업부서와 IT부서 간 협의 미흡 등으로 인한 대고객서비스 프로그램 장애가 다수 발생하였으나, IT부서는 현업부서 귀책이라는 이유로 이에 대한 재발방지대책 수립을 미흡하게 실시하고 있으며

회사는 프로그램 변경 통제를 강화하기 위해 정보전략팀 내 변경승인위원회(CAB : Change Advisory Board)[1]를 운영 중이나, 금전 관련 프로그램 개발 건에 대해 변경승인위원회 운영을 검토를 누락한 사례[2]가 있으므로

1) 핵심·중요 업무시스템에 대한 프로그램 개발 및 변경 중 개발 시간이 크거나, 타 시스템 연계 필요 등 영향도가 크거나, 금전, 고객정보 관련이 있는 프로그램에 대해 검토
2) 금전 관련 프로그램 장애 발생 25건은 변경승인위원회 검토 누락

회사는 대고객서비스 관련 프로그램 개발 시 사전 영향도 분석을 실시하고, 분석 결과에 따른 리스크 등을 프로그램 테스트 시 반영하는 등 전산장애 예방을 위한 테스트 강화 방안을 마련·운영하시기 바람

또한, 현업 업무요건 및 현업부서와 IT부서 간 협의 미흡으로 발생하는 전산장애 예방을 위해 개발요청 전 협의 및 심의 등을 강화하고, 변경승인위원회(CAB) 검토 대상 프로그램 개발 시에 동 위원회의 검토 절차가 누락되지 않도록 철저히 운영하는 등 대고객서비스 관련 전산 프로그램 장애 최소화를 위한 대책을 마련·운영하시기 바람

(13) 외부연계서비스 관리 강화 필요

회사는 금융계열사와 2021년 4월 '금융플랫폼 공동 구축 협약서'를 체결하여 계열사 공동 모바일앱 '모니모'*를 구축·운영하고 있으나

* 4개 금융계열사(삼성생명·C사·D사·E사)가 공동 개발하여 2022년 4월 출시, 고객이 하나의 앱으로 4개 금융계열사 서비스를 모두 이용 가능하도록 구축한 시스템

2024년 1/4분기 기준 모니모의 활용 비중은 보험료 입금 76.0%, 보험금 청구 84.7%에 달하고 있음에도, 전자금융거래 실적 등 이용자 통계현황 관리가 미흡하고,

모니모 장애로 인한 전자금융 사고사례[1]가 있는데도 별도의 재발방지 대책을 마련하지 않는 등 모니모 장애 시 비상대응체계[2]가 미흡하므로

1) 2022. 8. 22. 모니모 앱에서 160분간 삼성생명 계약·서비스 조회 불가
2) 모니모 앱 장애가 발생할 경우 대체수단(삼성생명앱, 모바일웹, PC) 활용하도록 안내하고 있으나, 모니모 앱 자체가 접속 불가할 경우에 대한 대비책 미비

회사는 모니모의 업무지속성 유지를 위하여 이용자 통계 현황관리 및 비상대응체계를 마련·강화하시기 바람

나. 개선사항

(1) 문서관리 업무 미흡

회사는 내규 「문서지침」에 따라 문서관리 담당자가 해당 부서의 문서분류체계에 근거하여 문서의 생성 및 폐기 목록을 작성하고 문서관리 책임자는 해당 부서의 문서목록을 관리하도록 규정하고 있으며, 문서관리 총괄부서에서는 정기적으로 문서분류체계, 문서목록 및 문서보관 등의 적정성을 확인해야 하나

회사는 문서결재를 위한 시스템으로 「전자결재·보고 시스템」과 「Knox Potal-결재 시스템」을 이원화하여 운영하면서 각 시스템별 이용 기준을 정하지 않아 이용자 편의에 따라 결재 시스템을 각각 이용하고 있으며, 「Knox Potal-결재 시스템」의 경우 결재 60일 후 전산상 문서가 삭제되도록 구현되어 있어 내규 상 문서보존기한을 준수하지 못하고 중요 결재자료가 소실될 가능성이 있고

각 부서가 엑셀파일로 관리하는 문서목록에는 문서번호, 담당부서, 보관위치 등 정보가 구분되어 관리되고 있지 않으며, 서면결재 문서를 문서목록에 기재하지 않은 사례가 발생하는 등 문서목록을 통한 문서의 체계적인 유지·관리가 다소 미흡한 것으로 확인되었으므로

회사는 체계적인 문서관리를 위해 결재시스템을 일원화하여 운영하거나 명확한 기준에 따라 결재시스템을 구분하여 사용함으로써 문서보존기한을 준수할 필요가 있으며, 서면결재 문서의 경우에도 전자적으로 등록·관리하여 문서의 생성부터 폐기까지 체계적으로 관리할 필요가 있음. 또한 문서목록에는 문서번호, 담당부서, 보관위치 등 충분한 정보를 기재한 후 중요 문서가 누락되지 않도록 시스템으로 관리하고 주기적인 점검을 실시할 필요가 있음

(2) 오픈소스 소프트웨어 관리 미흡

회사는 프로그램 개발 시 효율성 및 비용절감 등을 위해 다수의 오픈소스 소프트웨어*(Open Source Software, 이하 '오픈소스')를 도입·운영 중에 있으나

* 누구나 자유롭게 확인·수정·배포할 수 있는 소프트웨어로서 다수의 협업을 통해 개발·관리되며 운영체제, 응용 프로그램, 미들웨어 등 그 유형이나 이용 방식이 다양

검사착수일(2024.6.13.) 현재 홈페이지에 대해서만 오픈소스 도입 및 사용현황을 파일로 관리 중에 있고, 오픈소스 도입부터 사용 및 사후관리 등 오픈소스 관리체계를 마련·운영하지 않고 있어 오픈소스 사용현황 파악, 기술지원 종료 대응, 취약점 조치 등 오픈소스 관리를 소홀히 할 우려가 있고

또한 삼성생명 모바일앱 등 오픈소스를 포함하여 재배포하는 애플리케이션에 대해 오픈소스 라이선스 고지 필요성에 대한 검토 절차를 마련·운영하지 않고 있어 오픈소스 라이선스 미준수로 인한 법적 문제 발생 소지가 있으므로

회사에서 현재 사용 중이거나 도입하는 모든 오픈소스에 대한 관리체계를 마련·운영하고, 오픈소스를 포함하여 재배포하는 모든 애플리케이션의 오픈소스 라이선스를 확인 후 필요시 저작권 표시 및 라이선스 고지 등 라이선스별 의무사항을 준수하여 법적 분쟁이 발생하지 않도록 운영하시기 바람

※ 검사기간 중 삼성생명 모바일앱에서 사용 중인 오픈소스(Apache 2.0, MIT License)에 대해 법무실 검토 후 라이선스 고지 실시(2024.6.25.)

(3) 일괄작업 영향도 검토 미흡

회사는 내부 업무매뉴얼 「성능관리 가이드라인」에서 신상품 출시, 신규 서비스 오픈 등 대형이벤트가 예정된 경우 사전적으로 관련 시스템에 대한 부하테스트 등 성능관리 절차를 거치도록 정하고 있으나

대형이벤트와 연관된 전산작업(일괄작업 등)의 지연·부하 등으로 인해서도 고객서비스가 영향을 받을 수 있는데도, 이에 대한 별도의 검토 절차는 마련하지 않고 있어 대형이벤트로 인해 일괄작업이 지연되어 고객서비스가 지연된 사례*가 확인되었으므로

* (2021.4.13.) 암보험 신상품 출시로 보험가입 설계가 급증하였고 이로 인해 관련 일괄작업이 지연(시스템 자원점유)되면서 고객 서비스(가입 설계 및 청약) 지연

회사는 대형이벤트 등에 따라 시스템에 부하를 주거나 장시간 소요 가능성이 큰 일괄작업의 실행 전 영향도 검토 절차를 마련하여 일괄작업에 따른 전산시스템 장애가 발생하지 않도록 운영하시기 바람

(4) 정보처리시스템 성능 관리 소홀

회사는 내규 「가용성관리지침」, 「용량관리지침」, 「네트워크 운영지침」 및 「성능관리가이드라인」에 따라 전산시스템별 임계치 기준을 설정하고, 주요 시스템의 CPU, 메모리, 스토리지 등 성능을 모니터링하며, 임계치 초과 시스템에 대한 조치 등을 하고 있으나

회사 전산시스템별 특성을 고려하지 않고 기본적인 자원 사용률이 높은 시스템(ERP시스템) 기준으로 임계치를 일률적으로 설정하였고, 「금융IT 안전성 강화 가이드라인」의 전산자원별 임계치 기준[1]을 크게 상회하는 수준으로 전체 전산시스템의 임계치를 설정·운영[2]하고 있어 ERP시스템을 제외한 시스템의 경우 임계치 기준이 높아 용량 초과 시 적시 대응이 미흡할 우려가 있음

1) [금융IT 안전성 강화 가이드라인] CPU 및 메모리 임계치 기준

전산 자원	정상	주의	경계	심각
CPU	60% 미만	60% ~ 65%	65% ~ 70%	70% 초과
메모리	70% 미만	70% ~ 75%	75% ~ 80%	80% 초과

2) CPU/메모리 : 주의 90%, 경계 95%, 심각 99%

또한, 성능 모니터링 대상을 핵심 시스템(52개) 중 일부 시스템(12개)으로 한정하고 있고, 임계치 초과 시 용량 증설 등 조치에 장기간 소요*되고 있어 용량 초과로 인한 장애 발생 우려가 있으므로

* 3개월 이상 장기간 임계치 초과 CPU·메모리의 추가증설에 6개월 이상 소요

「금융IT 안전성 강화 가이드라인」 및 전산시스템별 자원 사용량을 고려하여 전산자원별 임계치 기준을 재검토하고, 전체 핵심시스템으로 성능 모니터링 범위를 확대하며, 일정 기간 이상 임계치가 초과된 시스템은 용량 증설 등 조치를 적시에 수행하여 장애 발생 가능성을 최소화하시기 바람

(5) 데이터베이스 접근통제 미흡

회사는 데이터베이스(DB) 접근통제를 위해 DB접근제어시스템(DB Safer)을 운영하고, DB에 직접 접근 가능한 접속 명령어는 중요 명령어로 지정하여 사전 권한 신청, 사후 모니터링 및 사용내역 소명 절차를 통해 관리하고 있으나

모니터링 시 DB관리자의 DB데이터조작명령어(DML : Data Manipulation Language) 수행내역 모니터링 범위를 개인정보 데이터 조회로만 한정하고 있어 임의로 데이터를 변경, 삭제한 내역은 모니터링을 누락할 우려가 있고

DB테이블 및 컬럼 등을 변경할 수 있는 DB데이터정의명령어(DDL : Data Definition Language) 수행 내역은 모니터링 대상으로 지정하고 있지 않아, DB관리자가 임의로 테이블을 변경, 삭제하는 경우 수행 내역에 대한 적정성 확인 및 적기 대응이 어려우므로

회사는 DB관리자에 의한 개인정보 데이터 조회 외에도 DB테이블, 컬럼 및 데이터 등을 변경하는 DB명령어(DDL, DML) 수행내역을 모니터링하고, 수행의 적정성을 소명·검증하는 절차를 마련·운영하시기 바람

(6) 홈페이지 및 앱 소스코드 취약점 관리 불합리

회사는 내규「취약점분석평가관리지침」에 따라 전자금융기반시설의 취약점 분석평가를 연 1회 이상(홈페이지는 6개월에 1회 이상) 실시하고, 내규「응용시스템보안지침」에서 보안성 검토 대상인 경우 프로그램 개발·변경 시 자체 보안성 심의 후 취약점을 확인 및 조치하도록 지침 및 절차를 마련하고 있으나

홈페이지(삼성생명, 다이렉트) 및 모바일앱 개발 시 소스코드 취약점 점검 및 보안담당자 확인·조치 후 운영시스템에 이관토록 하였음에도, 2023.9월 형상관리시스템을 변경하면서 소스코드 취약점 점검 후 보안담당자의 확인절차를 누락한 채 이관하고 있으며

모바일앱의 경우 앱 취약점 점검은 실시하고 있으나, 소스코드에 대한 취약점은 점검 주기를 마련하지 않고 장기간 점검을 실시하지 않아* 취약점이 포함된 소스 코드가 운영 시스템으로 이관될 우려가 있으므로

* 2018년, 2020년 2회 수행

회사는 홈페이지 및 모바일앱 개발 시 소스코드 취약점 점검결과에 대해 보안담당자 승인 후 이관하는 절차를 형상관리시스템에 마련·운영하고, 모바일앱 취약점 점검 시 소스코드 취약점에 대해서도 정기적으로 취약점을 점검하도록 점검 주기를 설정하여 운영하시기 바람