

## 경영유의 및 개선사항 공개

1. 금융기관명 : KB라이프생명보험(주)

2. 제재조치일 : 2026. 7. 22.

3. 제재조치내용

| 제재대상 | 제재내용             |
|------|------------------|
| 기 관  | 경영유의 12건, 개선 13건 |

4. 제재대상사실

가. 경영유의사항

### (1) 소비자보호부문 성과평가 체계 강화 필요

회사는 내규 『금융소비자보호 내부통제기준』에 금융소비자보호 총괄책임자·업무담당자에게 재무적 경영성과를 중심으로 업무평가기준을 마련해서는 아니되며 공정한 업무평가기준 및 급여복지기준을 마련해야 함을 명시하고 있으나,

2023년 소비자보호부 성과계약서\*에 보험손익, 신계약 환산월납보험료 등 재무적 경영성과\*\*를 연계하여 소비자보호 부서장·부서원에게 성과급을 지급한 사실이 있다.

\* 부서의 성과지표를 담고 있으며 각 부서에서 성과평가 항목을 선정하고 재무기획부의 검토를 거친 뒤 부서장과 본부장이 서명하는 과정을 거쳐 확정

\*\* 소비자보호부 성과지표 배점 중 10% 차지

### <조치할 사항>

회사는 금융소비자 권익 보호를 위한 공정한 업무수행이 이루어질 수 있도록 소비자보호부 성과계약서 작성 시 「금융소비자보호 내부통제기준」을 준수하여 재무적 경영성과가 연계되지 않도록 주의하시기 바랍니다.

## (2) 경영인정기보험 관련 내부통제 미흡

회사는 경영인정기보험과 관련하여 아래 (가)~(라)와 같이 미흡한 점이 있으므로 이를 개선할 필요가 있다.

### (가) 금융소비자보호 내부통제에 관한 사항

회사는 금융소비자보호법 등에서 정하는 바에 따라 금융상품 판매 과정에서 불완전판매가 발생하지 않도록 적절한 조치를 이행하여야 한다.

2020년~2023년 기간 중 회사 전체 보험상품의 평균 불완전판매비율\*(0.17%)은 생보사 평균(0.07%)의 2.4배에 달하며, 특히 경영인정기보험의 불완전판매비율은 0.65%로 매우 높아 불완전판매율을 낮추기 위한 적극적인 조치가 필요한 상황이다.

\* 민원해지, 품질보증해지, 무효

이에 따라 금융소비자보호부는 불완전판매 현황 및 관리 방안을 금융소비자보호 내부통제위원회에 보고하는 등 소비자보호 관련 업무를 수행하고 있으나, 불완전판매율 개선을 위한 실효성 있는 관리 조치가 이행되지 않고 있다.

회사는 2024년 14회 상품심의회(2024.7.18.)를 통해 경영인정기보험 상품 개정\*을 심의하며 불완전판매 예방을 위한 소비자보호방안으로 유지율 부진 및 불완전판매·민원 과다 GA에 대해 시책 패널티를 부과하는 안을 마련하였으나 현재까지도 패널티 부과 기준 등 시행 방안을 구체화하지 않고,

오히려 제휴GA 추가시책(파트너십 프로모션) 지급기준에 경영인정기보험 판매실적을 반영하고 경영인정기보험 한정 파트너십 GA를 신규 선정하는 등 판매 촉진을 유인하는 정책을 실시(2024.7.30.)하였으며,

\* 장기유지보너스 변경으로 5년 시점 환급률이 86.4%에서 95.5%로 상향되어 저축성 상품으로의 불완전판매 가능성을 더욱 증대

그 과정에서 금융소비자보호부는 동 시책 및 프로모션 제·개정 사전협의시 소비자보호 불이익 및 특이사항이 없다고 검토하는 등 금융소비자 보호 관점에서 일관되고 충실한 검토를 진행하지 아니하였다.

## <조치할 사항>

회사는 금융상품 판매과정에서 불완전판매가 발생하지 않도록 상품심의회에서 논의된 소비자보호방안 이행 방안을 적기에 시행·점검하고, 시책 및 프로모션 제·개정 시에도 상품의 불완전판매율 및 민원 현황 등을 반영하는 등 실질적인 내부통제 조치를 이행하시기 바랍니다.

### (나) 모집종사자 내부통제에 관한 사항

경영인정기보험을 법인세 절세 상품으로 설명해 모집하는 등 불건전영업행위가 확대됨에 따라 생명보험협회는 신인설계사(등록 3개월 미만)의 경영인정기보험 판매를 제한\*하고 보험회사가 GA 소속 설계사를 대상으로 불완전판매방지 및 세법 교육을 강화 실시하도록 하는 등의 내부통제 강화방안을 업계에 전파하였다.

- \* ① 경영인정기보험의 완전판매를 위해서는 세법 관련 전문지식(납입보험료의 손금 산입 요건, 해약보험금 수령 시 과세 여부 등)이 요구되고, ② 타 상품군 대비 월납보험료가 높으며, ③ 영업 난도가 높은 법인을 대상으로 한 상품인 점을 고려

그러나 회사는 신인설계사 판매 제한을 이로부터 4개월이 경과한 뒤에서야 시행(2024.8.23.)하였고 그 결과 2024.4.17.~2024.8.22. 기간 동안 총 94건의 신인설계사 청약이 접수되었으며, GA 소속 설계사를 대상으로 한 세법 교육 또한 일체 실시하지 않았다.

## <조치할 사항>

회사는 상품특성에 따라 모집조직(GA 및 보험설계사 등)에 적절한 교육 방안을 마련하고, 경영인정기보험과 관련하여, GA 소속 설계사를 대상으로도 불완전 판매방지 및 세법 교육 등을 실시하시기 바랍니다.

### (다) 보험계약 인수심사에 관한 사항

보험회사는 건전한 보험계약 인수를 위하여 보험계약자 및 피보험자의 가입 취지, 보험료 납입능력 등을 충분히 고려해 심사를 수행하여야 한다. 그러나 회사의 경영인정기보험 계약 인수심사 업무수행에서 다음과 같은 문제점이 발견되었다.

① 동 상품은 법인의 최고경영인을 피보험자로 하여 최고경영인의 유고 시 발생할 수 있는 재무적 위험을 보장하는 상품이나,

회사는 계약자 및 피보험자가 법인이 아닌 개인\*·개인사업자인 경우에도 청약을 승낙하였으며, 계약자가 법인인 경우에도 피보험자가 법인 경영에 영향력을 행사하는 최고경영인 및登記임원에 해당하는지 확인하지 않고\*\* 청약을 승낙하였다.

\* 피보험자가 보험설계사 본인인 자기계약(102건), 비경제활동인구(주부, 학생) 계약(582건) 등

\*\* 내규에 따라 보험가입금액 15억 초과건(51건)에 대해서만 최고경영인,登記임원 여부를 확인

| 피보험자별 판매 현황 ('24년 1~8월 청약건, 단위: 건) |         |           |         |          |
|------------------------------------|---------|-----------|---------|----------|
| 구 분                                | 개 인     | 개 인 사 업 자 | 법 인     | 합 계      |
| 피 보험 자                             | 3,750   | 14        | 1,543   | 5,307    |
|                                    | (70.7%) | (0.3%)    | (29.1%) | (100.0%) |

② 회사는 상품의 보험료 월납액이 타 보험상품보다 크고\* 납입기간이 전기납입을 감안하여 계약자 및 피보험자의 계약유지능력을 심사하여야 하나,

\* 월납초회보험료 2백만원 초과건이 전체계약의 12% ('24년 1~8월 청약 전체 5,307건 중 637건)

내규 「고액계약 기준 및 구비서류 매뉴얼」에 재정심사 대상을 보험가입금액 15억 초과 건으로 한정하고 있어 2024년 전체 청약의 0.96%(전체 5,307건 중 51건)에 대해서만 재정심사를 실시하는 등 대부분의 청약에 대해 재정심사를 실시하지 않았다.

\* 고액계약 기준 및 구비서류 관련 매뉴얼

한편, 내규에 따라 재정심사를 실시한 청약(51건) 중에서도 연환산 보험료가 법인의 2년 평균 당기순이익을 초과하는 등 법인의 납입 능력 대비 보험료가 과다하여 이상 계약으로 의심되는 청약(9건), 내규 상 가입한도\*를 초과하는 청약(15건)을 반송하지 않고 승낙하는 등 관련 내부통제가 미흡하다.

\* <sup>1)</sup> 피보험자 지분율이 있는 경우 최근 3개년 평균 당기순이익\*최대15배\*피보험자 지분율(%),

<sup>2)</sup> 피보험자 지분율 없는 경우는 개인연소득\*10배 이내, <sup>3)</sup> 설립 후 3년 미만인 경우는 평균 당기순이익\*10배

### <조치할 사항>

① 회사는 경영인정기보험이 상품 취지에 부합하게 운영될 수 있도록 계약 관계자(보험계약자 및 피보험자 등)를 제한하시기 바랍니다.

② 상품특성에 따라 실질적인 재정심사가 될 수 있도록 관련 심사기준을 강화하는 등 계약유지능력을 면밀히 심사하시기 바랍니다.

### (라) 가상계좌를 통한 계속유지보험료 수납에 관한 사항

가상계좌를 통한 보험료 수납이 보험료 대납 및 허위·가공계약의 수단으로 악용되는 등 부당모집행위를 방지하기 위하여 우리원은 보험회사가 가상계좌 입금 건의 실입금자 정보를 확인하도록 업계에 지도(2020.7월)하였으며,

이에 따라 회사는 모집설계사가 가상계좌를 통해 보험료를 입금하는 경우 상세 사유를 소명토록 하고, 대납으로 확인되는 경우 징계위원회에 부의하여 처벌하는 내용의 내부통제 체계를 마련하였다. 특히 경영인정기보험은 영업 현장에서 거액의 수수료 등을 제시하며 과도한 보험료를 납입하도록 유인하는 편법이 만연한 점, 납입보험료의 손금산입을 통한 법인세 절세 효과 등을 강조하는 점\*을 고려해 볼 때, 가상계좌를 통한 보험료 수납을 보다 철저히 관리할 필요가 있다.

\* 납입보험료의 손금 산입을 위해서는 법인 계좌에서 보험료를 직접 납입할 필요

그러나 회사의 모니터링 체계는 실입금자와 해당 계약의 모집설계사 일치 여부만을 확인하는 수준에 그치고 있어, 모집설계사와 동일 GA에 소속된 설계사가 가상계좌를 통해 계속보험료를 3회 이상 지속 납부하는 등 우회적인 보험료 대납이 의심되는 사례에 대해서는 모니터링 및 관리가 이루어지지 않고 있다.

### <조치할 사항>

회사는 모집설계사 외 모집설계사와 동일GA 소속 모집설계사가 납입하거나 일정 기간 지속적으로 가상계좌 납입이 진행되는 경우 등에 대해 모니터링을 추가 실시하시기 바랍니다.

### (3) 모바일 청약 및 해피콜의 보안 강화 필요

회사는 대면 방식의 상품권유 이후, 계약자에게 청약화면 접속을 위한 웹주소 (이하 'URL')가 담긴 알림톡을 발송하여 계약자의 본인인증 후 계약조건, 중요사항 등을 직접 확인 및 자필서명하는 모바일 청약\*을 실시하고 있다.

\* 검사대상기간 중 총 136,506건 청약

또한, 전자적 방식의 해피콜에 동의한 계약자를 대상으로 URL이 담긴 알림톡을 발송하여 계약자가 본인의 휴대폰을 통해 본인인증 후 보험계약의 중요사항 이해 여부 등을 확인하는 모바일 해피콜\*을 실시하고 있다.

\* 검사대상기간 중 총 324,205건 실시

하지만 ①모집설계사 등 제3자가 계약자에게 전송된 알림톡을 전달받으면 모바일 청약 및 해피콜 관련 URL에 접속할 수 있고, ②본인인증번호를 전달받으면 제3자의 휴대폰으로 청약 및 해피콜을 실시할 수 있음에도, 대리실시를 방지하는 내부통제 방안을 마련하지 않은 사실이 있다.

#### <조치할 사항>

회사는 모집설계사 등 당사에 등록된 설계사 번호로 모바일 청약 및 해피콜 관련 알림톡(URL)을 발송하지 않도록 전산시스템을 개선하고, 계약자가 아닌 제3자에게 URL 전송시 청약 및 해피콜의 대리실시가 진행될 수 없도록 접속을 차단하는 등 관련 업무를 개선할 필요가 있다.

#### (4) 책임준비금 산출 관련 업무절차 강화 필요

회사는 한국채택국제회계기준과 이에 따라 회사가 마련한 회계정책서 등에 따라 최선추정부채(BEL), 위험조정(RA), 보험계약마진(CSM) 등 책임준비금을 합리적으로 산출하고 오류를 방지하여 객관성·정합성을 제고하여야 하나, 2023년말 책임준비금 산출 과정 중 다음과 같이 미흡한 점이 있다.

##### ① 최선추정부채(BEL) 산출에 관한 사항

보험계약대출 평가 시 미래현금흐름은 회사의 경험통계, 상품별 보험계약대출 한도 등이 고려된 합리적인 가정을 적용하여 산출하는 것이 타당하나, 회사는 전산 오류 등으로 탑클래스 종신보험 등 4,984건의 보험계약에 대해 보험계약대출 잔액이 있음에도 미래현금흐름을 누락하는 등 현금흐름을 잘못 계산하여 최선추정부채(BEL)를 산출한 사실이 있다.

또한, 2024년도 최적가정(사업비율) 산출 시 사업비정책 상 차세대사업 관련 실제 비용발생 금액 48.7억원의 10%인 4.9억원을 기간인식하기로 최적가정모델협의회에서 결정하였음에도, 회사는 10%가 아닌 90%에 해당하는 43.8억원으로 잘못 적용하여 최선추정부채(BEL)를 산출한 사실이 있다.

##### ② 보험계약마진(CSM) 산출에 관한 사항

보험계약마진(CSM) 산출시 회사 계리방법서에서 정한 기준\*에 따라 보험계약 집합을 '이익계약', '기타계약', '손실계약'으로 분류하여야 하나, 회사는 전환시점("22.1.1.) 보험계약마진(CSM)을 산출하는 과정에서 보험계약집합 분류 시 121,743건의 보험계약을 기준과 다르게 분류하여 845억원의 보험계약마진을 830억원으로 산출한 사실이 있다.

\* 이익계약:  $CSM > RA$ , 기타계약:  $RA \geq CSM \geq 0$ , 손실계약:  $CSM < 0$

#### <조치할 사항>

회사는 최선추정부채(BEL) 산출시 보험계약대출 현금흐름 생성 과정에서 발생한

오류를 수정하고, 최적가정 산출시 최적가정모델협의회에서 결정한 사항이 정확하게 적용될 수 있도록 하며, 보험계약마진(CSM) 산출시 보험계약집합 분류를 내규에 맞게 수정하는 한편, 오류사항을 조기에 발견할 수 있도록 책임준비금 산출 및 검증 업무를 강화할 필요가 있습니다.

#### (5) 파생결합증권(ELS)을 편입한 펀드에 대한 위험관리 강화 필요

회사는 운용 중인 변액펀드에 편입되는 주가지수 파생결합증권(ELS)에 대해 ELS-VaR\*을 리스크관리지표로 설정하고 있으며 동 지표의 관리 기준을 30% 초과로 설정하고 있으나, ELS를 편입한 펀드의 위험관리 업무절차에 아래와 같이 미흡한 사실이 있다.

\* ELS-VaR = (손실발생확률)×(손실 발생 시 투자금액 대비 기대손실금액의 비율)

① ELS 편입 시에만 ELS-VaR를 측정하고 이후에는 지표의 측정 및 관리를 수행하지 않아 고위험 투자자산인 ELS의 사후적인 리스크관리를 실시하지 않았다.

② 발행 시장에서 ELS 종목의 ELS-VaR이 관리 기준(30%)을 초과할 가능성이 현저히 낮고\*, 회사는 2014년에 기준을 설정한 이후 적정성 검증을 실시하지 않는 등 리스크관리지표를 미흡하게 운영하였다.

\* ELS-VaR값이 기준을 상회하는 경우에 해당되기 위해서는 손실확률이 30%이고, 손실 시 기대손실금액이 투자금액 대비 100% 이어야 하는데 이는 발생가능성이 극히 드물어 보임

#### <조치할 사항>

회사는 편입한 ELS에 대한 주기적인 리스크관리지표 측정을 실시하여 투자 이후 사후적인 리스크를 관리하고, 리스크관리지표 기준에 대한 적정성을 검증하고 결과를 기록·보관하여 ELS를 편입한 펀드에 대한 위험관리를 강화하시기 바랍니다.



## (6) 특별계정 외부 위탁운용사 평가체계 강화 필요

회사는 내규 「자산운용규정」 및 「자산운용사 선정 및 평가 세칙」 등에 따라 투자일임계약을 체결하고 특별계정(변액) 운용 업무를 외부 자산운용사에 위탁하여 정기적으로 위탁운용사에 대한 평가를 실시하고 있다.

하지만 ELS펀드에 대해서는 투자가 집행된 2014년 이후부터 현재까지 성과 평가를 실시하지 않았고, 2023.1.1. 「자산운용사 선정 및 평가 세칙」을 개정하여 ELS 등 구조화펀드를 평가 대상 자산에서 제외한다는 문구\*를 추가하였으며, 이후 동 자산에 대해 별도의 평가체계를 마련하지 않은 사실이 있다.

\* 「자산운용사 선정 및 평가 세칙」 제12조(성과평가 대상) ① 담당부서는 자산운용의 적정성을 모니터링함으로써 효과적인 자산운용이 지속적으 가능토록 하기 위하여 모든 펀드에 대하여 주기적으로 성과평가를 하는 것을 원칙으로 한다. 단, 다음 각호의 경우는 성과평가 대상에서 제외한다.

5. ELS펀드등과 같은 구조화펀드로서 정해진 펀드구조에 따라 수익률이 결정되는 경우

이에 따라 평가체계상 산출된 점수가 운용성과를 제대로 반영하지 못하여 자산운용사 선정이 불합리하게 이루어질 우려가 있다.

### <조치할 사항>

회사는 평가에서 제외되는 자산 항목을 최소화하고 평가 제외 근거에 대한 합리적이고 명확한 사유를 기재할 필요가 있으며, 특히 합리적인 사유 없이 평가를 실시하지 않은 ELS 등 구조화펀드의 경우 벤치마크 또는 대안지표를 설정하여 성과평가를 실시하고 손실 및 컴플라이언스 등을 반영한 평가체계를 마련하시기 바랍니다.

## (7) 외화보험 보험계약대출 제도 및 운영 강화 필요

보험회사는 한국은행이 제정한 「외화대출 취급지침」에 따라 해외 실수요 용도의 자금에 한해서만 외화보험상품의 보험계약대출 취급이 가능\*하다. 이와 관련하여 회사는 외화보험 보험계약대출 제도 및 운영에 대해 다음과 같이 미흡한 점이 있다.

\* 회사는 한국은행으로부터 “보험계약대출은 외화대출 용도제한 적용 범위에 포함되어 해외 실수요인 경우에 한해 외화대출 취급이 가능”하다는 통보를 받음(2021.8.27.)

① 회사는 2021.8.27. 이후부터 검사종료일 현재까지 외화표시보험 4건을 판매하면서 외화표시보험 보험약관 등\*에 “외국환거래법에 따라 보험약관대출이 제한될 수 있다”는 내용을 반영하지 않았다.

\* 회사는 2022.7.1. 이후부터는 상품설명서에 “한국은행 외화대출 취급지침에 따라 보험계약대출이 제한됩니다”라는 내용의 계약자확인서를 징구 중

② 또한 회사는 외화표시보험의 보험료를 연체하는 경우 보험계약대출 성격의 ‘보험료자동대출납입’ 약정을 운영할 수 없음에도, 검사종료일 현재 ‘무배당 달러 종신보험’의 보유계약 중 42건이 보험료의 자동대출납입 약정을 유지하고 있다.

### <조치할 사항>

회사는 외화표시보험 보험약관에도 보험계약 대출이 제한됨을 명시하는 등 관련 업무를 개선하고, 위 약정을 유지하는 보험계약자에게 보험료의 자동대출납입이 제한됨을 상세하게 안내하여 관련 위규사항 및 계약자에 불이익 발생하지 않도록 관리하시기 바랍니다.

## (8) 지급여력비율(K-ICS) 산출 관련 업무절차 강화 필요

회사는 K-ICS 비율(자본적정성비율)을 「보험업감독업무시행세칙」[별표22](이하 ‘기준서’)에서 정한 방법에 따라 K-ICS비율, 시장·신용위험액을 산출해야 한다.

그러나 2023.6월 ~ 2024.6월(5개 분기) 동안 다음의 내용과 같이 K-ICS 비율, 시장·신용위험액을 오산출한 사실이 있다.

① (시장위험액) 회사는 기준서 4.3.다.⑥.ㄱ.에 따라 “주식형 레버리지 펀드 또는 레버리지 전략 추구 헤지펀드”에 대해서는 익스포저에 기타주식에 적용하는 충격수준(49%)이 아닌, 아래와 같이 별도로 정해진 산식에 따른 충격수준을 적용하여 위험액을 계산해야 한다.

**< 레버리지 펀드 적용 충격계수 산식 >**

$$\text{Max}\{\text{Min}(\text{약관상 최대레버리지비율} \times 35\%, 100\%), 49\%\} \text{ 또는 } 100\%^*$$

\* 약관 상 최대레버리지 비율이 확인되지 않을 경우 100%의 충격수준을 적용

그러나 회사는 보유하고 있는 PEF펀드에 대해 상기 산식율을 적용하지 않고, 기타주식에 적용하는 충격수준(49%)을 적용하여 시장리스크를 산출하여 시장위험액을 과소산출한 사실이 있다.

② (신용위험액) 회사는 기준서 <표30>5-2.가.에 따라 거래자산별 익스포저에 “라.위험계수 산출기준”에 따라 산출한 위험계수를 곱한 후 합산하여 산출해야 한다.

회사는 “라. 위험계수 산출기준” 상 보험회사가 1순위로 저당권을 설정하고 지급여력비율산출 기준일 현재 분양률 또는 사전 임대계약률이 100%인 계약에 대해서만 우량 부동산PF 신용위험계수를 적용하여 신용위험액을 산출해야 한다.

**부동산PF 익스포저 위험계수**

(단위 : %)

| K-ICS<br>신용등급 |               | 유효만기 |     |     |      |      |      |      |      |      |      |       |       |       |       |      |
|---------------|---------------|------|-----|-----|------|------|------|------|------|------|------|-------|-------|-------|-------|------|
|               |               | 0-1  | 1-2 | 2-3 | 3-4  | 4-5  | 5-6  | 6-7  | 7-8  | 8-9  | 9-10 | 10-11 | 11-12 | 12-13 | 13-14 | 14+  |
| 무<br>등<br>급   | 부동산PF<br>(우량) | 2.9  | 5.6 | 6.6 | 7.2  | 7.5  | 7.8  | 8.0  | 8.0  | 8.1  | 8.1  | 8.2   | 8.2   | 8.2   | 8.2   | 8.2  |
|               | 부동산PF<br>(일반) | 4.3  | 8.4 | 9.9 | 10.9 | 11.3 | 11.7 | 12.0 | 12.0 | 12.1 | 12.1 | 12.3  | 12.3  | 12.3  | 12.3  | 12.3 |

※ 「보험업 감독업무 시행세칙」[별표22]<표30>

그러나 회사는 기준서 상 우량 부동산PF 익스포저 임에도 일반 부동산PF 익스포저로 분류하여 시장위험액을 오산출한 사실이 있다.

### K-ICS 비율 오산출 내역(2023.6월말~2024.6월말)

(단위 : 억원, %p)

| 구 분         |           | 2023.6월말 | 2023.9월말 | 2023.12월말 | 2024.3월말 | 2024.6월말 |
|-------------|-----------|----------|----------|-----------|----------|----------|
| 시장<br>위험액   | 레버리지 펀드   | 16       | (379)    | (627)     | (225)    | (238)    |
| 신용<br>위험액   | 부동산PF 오적용 | 0        | 0        | 0         | 8        | 0        |
| K-ICS<br>비율 | 수정 前(a)   | 270.7    | 277.0    | 329.8     | 303.8    | 299.2    |
|             | 수정 後(b)   | 270.8    | 275.2    | 325.7     | 302.5    | 297.4    |
|             | 차이(b-a)   | 0.1      | △1.8     | △4.1      | △1.3     | △1.8     |

#### <조치할 사항>

앞으로는 기준서에 정해진 바에 따라 정확하게 K-ICS비율, 시장위험액, 신용위험액을 계산할 수 있도록 관련 업무에 유의하시기 바랍니다.

### (9) IT감사업무 강화 필요

감사부는 내규 「감사위원회규정」, 「감사위원회직무규정」, 「감사업무세칙」에 따라 IT부서를 대상으로 2020년~2023년 기간 중 총 8회(정기감사 2회, 특별감사 6회)에 걸쳐 감사를 수행하였다.

그러나 IT업무 전반을 대상으로 한 감사가 아닌, 보안 등 일부 IT업무에 편중된 감사가 수행<sup>1)</sup>되었고, 감사 지적사항에 대한 개선계획(미정리보고서 등)이 기한 내 제출되지 않는 등 감사 결과에 따른 사후 조치를 적절하게 관리하지 않은 사례<sup>2)</sup>가 존재한다.

1) 업무유형별 감사 횟수('20~'23) : IT보안 6회, IT서비스 5회, 시스템 개발 2회, IT경영 2회

2) 감사 지적사항에 대한 개선계획을 지연 제출한 사례(아래 표 참고)

### 감사 결과에 따른 사후 조치 미흡사례(3건)

| 감사 시작일자       | 지적사항                                       | 정리기한         | 미정리보고서 제출일자  |
|---------------|--------------------------------------------|--------------|--------------|
| 2021. 1. 18.  | 사용자 계정 및 권한 관리 강화                          | 2021. 6. 5.  | 2021. 6. 17. |
| 2021. 10. 18. | 청약서 발송 누락 등 완전판매 관리 부적정                    | 2022. 5. 14. | 2022. 6. 23. |
| 2023. 5. 17.  | LOS 사업 수행사 사업수행범위 변경에 따른 계약 내용 변경 여부 검토 필요 | 2023. 9. 27. | 2024. 5. 13. |

또한 IT부서는 내규 「IT자체감사세칙」에 따라 IT자체감사인을 지정하여 자체감사 절차대로 감사를 수행해야 하나 IT자체감사인을 지정하지 않고, 세부적인 자체감사 절차\*가 없고 자체감사도 수행하지 않고 있다.

\* 자체감사의 계획수립, 대상업무 선정, 수행주기, 결과보고, 후속조치 등

#### <조치할 사항>

회사는 IT감사가 특정 업무에 편중되지 않고 IT업무 전반에 대해 이루어질 수 있도록 IT감사 대상·범위를 조정하고, 감사결과에 따른 사후 조치가 적절하게 이뤄지도록 관리를 강화하는 한편, 자체감사인이 절차에 따라 IT자체감사를 수행할 수 있도록 자체감사업무를 개선하시기 바랍니다.

### (10) 오픈소스 소프트웨어 관리 강화 필요

회사는 정보처리시스템의 개발·운영 시 생산성 향상 및 비용 절감 등을 위해 오픈소스 소프트웨어\*(이하 “오픈소스SW”) 21종과 이를 효율적으로 관리하기 위한 오픈소스SW 관리 솔루션(Black Duck)을 도입하여 활용하고 있다.

\* 오픈소스 소프트웨어 : 저작권이 존재하지만, 저작권자가 소스코드를 공개하여 누구나 자유롭게 사용, 복제, 배포, 수정, 활용할 수 있는 소프트웨어

이러한 오픈소스SW는 저작권 및 라이선스 정보의 고지, 소스코드 공개 등 라이선스 의무사항을 준수해야 하고, 이를 위반하는 경우 법적 분쟁이 발생할 수

있으며, 적시 보안패치 등 보안관리가 취약할 경우 해킹 등 사이버공격의 주요 대상이 될 수 있다.

따라서 소프트웨어 구성요소 분석(SCA, Software Composition Analysis) 등을 통해 오픈소스SW의 라이선스를 식별하여 의무사항을 준수하고, 보안 취약점을 주기적으로 점검 및 조치하는 등 활용주기\*에 따라 오픈소스SW를 체계적으로 관리하는 것이 중요하다.

\* 오픈소스SW 식별 → 라이선스 및 보안 관련 이슈 파악·해결 → 승인 → 사용·관리

하지만 회사는 오픈소스SW 관리와 관련한 업무분장을 「직제규정」 등 관련 내규에 반영하지 않아 관리주체(부서)를 불명확하게 운영하고 있다.

또한 전체 업무시스템(59개) 및 관련 애플리케이션에 적용하여 활용 중인 오픈소스SW의 종류·버전·라이선스 등 정보를 식별하지 않고 운영하는 등 현황관리가 미흡하고, 라이선스 의무사항을 준수하지 않고 보안패치를 적용하지 않고 있어 발생할 수 있는 이슈를 파악하지 못하고 있으며, 공식적인 승인 절차 없이 사용하는 등 오픈소스SW 활용주기에 따른 관리가 미흡하므로 라이선스 위반이나 보안 취약점 등으로 인한 법률·보안 리스크가 큰 상태이다.

#### <조치할 사항>

따라서 회사는 오픈소스SW 관리주체 및 활용주기 전반에 걸친 관리체계를 내규에 반영하고, 활용 중인 오픈소스SW를 체계적으로 관리·운영하시기 바랍니다.

## (11) 노후화된 정보처리시스템 관리 강화 필요

회사는 내규 「정보보호규정」에 따라 모든 서버 및 인프라에 대해 주기적으로 패치와 업그레이드를 수행하고 있다.

하지만 회사는 운영 중인 서버 1,115대 중 366대<sup>1~2)</sup>(32.8%), 데이터베이스서버 103대 중 20대<sup>3)</sup>(19.4%)에 제조사의 기술지원이 종료된 소프트웨어(운영체제<sup>1)</sup>, 하이퍼바이저<sup>2)</sup>, 데이터베이스관리시스템<sup>3)</sup>)를 사용하고 있어 적시에 업그레이드, 보안 패치 등의 기술지원을 받지 못해 장애가 발생하면 신속·정확한 대응이 어렵고, 보안취약점을 이용한 침해사고의 우려가 있다.

1) AIX 6.1/7.1/7.2(75대), CentOS 4.8/5.x/6.x/7.x/8(47대), HP-UX 11i(2대), RHEL 5.x/6.x/7.x(70대), RockyOS 8.7(1대), SUSE 11(2대), Windows Server 2012(117대)

2) VIOS 2.2.6.10/3.1.1.21(30대), VMware ESXi 6.7.0/Photon(22대)

3) Oracle 11g/12/18.5(5대), Postgresql 11(3대), MS-SQL 2012(12대)

### <조치할 사항>

따라서 회사는 노후화된 정보처리시스템에 대한 교체 또는 기술지원 연장 계약 등 조치 계획을 수립하고, 동 계획에 따른 소요 비용을 정보기술부문의 예산에 반영하는 한편, 조치 전의 노후화된 정보처리시스템은 업무 중요도·영향도에 따라 네트워크 격리, 주기적인 보안취약점 점검 등의 보안대책을 마련하여 운영하는 등 노후화된 정보처리시스템의 관리를 강화하시기 바랍니다.

## (12) 전산장애 관리 강화 필요

회사는 내규 「시스템장애 및 문제관리세칙」, 「인프라 운영 업무매뉴얼」 등에 따라 전산장애가 발생하면 장애 내용의 심각도, 대고객 영향 등을 고려하여 장애등급을 분류하고 관련 내용을 장애관리시스템에 등록하여 관리하고 있다.

하지만 장애관리시스템에 장애 시점, 원인 및 영향 등 세부 내용을 잘못 등록한 사례\*가 확인되고, 이러한 사례로 인해 발생한 장애를 신속하게 해결하지 못하거나 유사한 장애가 반복될 우려가 있다.

\* ① 장애 발생, 인지 및 복구시점을 동일한 시간으로 등록

② 발생 원인이 '미상(알 수 없음)'인 장애를 '근본원인 해소된 장애'로 분류하여 등록

### <조치할 사항>

따라서 회사는 장애관리시스템에 전산장애의 원인 및 재발방지 대책 등이 정확히 기록·관리되는지의 여부에 대해 주기적인 점검을 수행하고, 동 점검 절차를 내규에 반영하는 등 전산장애 관리를 강화하시기 바랍니다.



## 나. 개선사항

### (1) 차익거래 계약관련 내부통제 미흡

회사는 2023.7월부터 상품출시 이전 과도한 수수료 및 시책 지급에 따른 차익거래\*계약 발생 여부를 점검하고 있다.

\* 과도한 수수료 등의 지급으로 이익(수수료+시책+해지환급금-납입보험료-환수금>0)이 발생

하지만 회사는 차익거래 점검 대상을 ①GA채널, ②보험료납입 36회차 이내로 한정함에 따라, 전속채널 판매 상품 및 37회차 이후 발생 여부 등 현황을 검토한 사실이 없다\*.

\* (사례) KB종신보험 무배당(간편심사형, GA채널) : 보험료납입 36회차에 수수료를 18% 지급(월납보험료 대비)하고, 37회차에 331% 지급한 결과 310%의 차액 발생

또한, 차익거래를 유발할 수 있는 수수료(보험료납입 17회차) 및 시책(4회차)의 환수정책구조\*를 채택·운용한 결과, 'KB 종신보험 무배당' 등 일부 상품(24개)은 보험료납입 37회차 시점에 평균 162%의 차액이 발생함에도 이에 대한 상시적인 점검방법 및 구체적인 대응방안을 마련하지 않은 사실이 있다.

\* 수수료의 경우 보험료납입 17회차까지, 시책의 경우 보험료납입 4회차까지만 환수를 실시

또한, 검사대상기간 중 차액이 발생한 계약 총 19,566건(자기계약 326건)과 관련하여 차익거래 계약이 반복적으로 발생하는 보험대리점 또는 설계사별 차익거래 계약현황에 대한 모니터링 및 제재조치 등 내부통제가 부족한 사실이 있다.

#### <조치할 사항>

회사는 차익거래 방지시스템을 도입하여 전체 모집채널 및 전 회차(보험료 납입)의 차액여부를 점검하고, 수수료 및 시책의 환수 기간을 강화하며, 차익거래 계약이 반복적으로 발생하는 보험대리점 또는 설계사별 계약 해지 현황을 모니터링하고, 제재조치하는 등 내부통제를 강화하여 차익거래 계약이 발생하지 않도록 관리할 필요가 있다.

## (2) 자금세탁방지 운영체계 미흡

회사는 자금세탁방지와 관련하여 아래 (가), (나)와 같이 미흡한 점이 있으므로 이를 개선할 필요가 있다.

### (가) 고객확인업무 운영체계 미흡

회사는 내규인 「자금세탁방지업무규정」 제23조 및 제27조에 따라 금융거래를 이용한 자금세탁 등 불법행위를 방지하기 위해 법인고객인 경우 실제 소유자\*의 성명, 생년월일, 국적 등을 고객으로부터 제출받아 고객확인 의무를 수행하고 있다.

\* ① 의결권 있는 발행주식총수 25%이상의 주식·출자지분을 소유한 자 → ② 주식·출자지분 수가 가장 많은 주주 등 → ③ 법인대표자의 순서로 단계별로 실제 소유자를 확인

하지만 업무처리담당자가 법인의 실제소유자를 확인하고도 자금세탁방지 시스템에는 확인단계를 법인대표자로 입력하거나, 대표자를 실제 소유자로 등록하는 등 고객확인 정보가 일부 오기재하였고 주기적인 사후점검을 통해 확인하지 않는 등 일부 고객검증 관련 미흡한 사례가 있다.

### (나) 의심스러운 거래 운영 미흡

회사는 내규인 「자금세탁방지업무세칙」 제9조에 따라 의심스러운 거래 검토 시 현업부서 보고담당자는 10일이내에 자금세탁방지업무담당자에게 보고하여야 하고, 의심스러운 거래 검토시작일로부터 최종 검토 완료까지 30일을 넘지 않아야 한다.

하지만 검사대상기간 동안 총 13,846건의 의심스러운 거래에 대해 검토하면서 237건은 10일을 초과하여 자금세탁방지업무 담당자에게 보고하였고, 126건은 30일을 초과하여 검토 완료하였다.

\* 의심스러운 보고 검토 완료 후 FIU에 3일이내 보고하였음

### <조치할 사항>

회사는 고객확인 정보의 전산 오기재를 방지하기 위해 관련 서류 확인 및

준법감시 재검증 절차를 철저히 하고 의심스러운 거래 검토시 정해진 기한 내에 검토 및 사후검증 등 관련 내부통제를 강화하시기 바랍니다.

### (3) 집행임원 성과보수 환수체계 미흡

회사는 내규 「집행임원운영규정」에 따라 집행임원에게 부여된 장·단기 성과급의 전부 또는 일부를 사유\*에 따라 보상위원회 및 이사회 결의로 환수할 수 있다.

\* 감독기관 문책요구, 내부통제 관련 규정 위반 등

하지만 내규 등에 성과급 환수사유별 환수 비율에 대한 가이드라인이 없어 소관 위원회의 결정에 따라 환수 비율과 금액이 결정되는 등 일관된 기준이 적용되지 않을 우려가 있다.

#### <조치할 사항>

회사는 환수비율 등을 합리적으로 운영할 수 있도록 상세 가이드라인을 내규에 마련하여 환수비율에 대한 기준을 명확히 하시길 바랍니다.

### (4) 외화보험 환율적용 업무절차 미흡

회사는 외화보험을 판매하고 있으며, 외화 보험료 및 보험금을 원화로 환산\* 하는 경우에는 약관상 정해진 환율로 정확하게 계산하여야 한다.

\* 보험계약자가 원화환산납입서비스특약, 원화환산지급서비스특약에 가입한 경우

동 특약에서 원화 환산에 적용되는 환율은 환산기준일의 일정 범위\* 내에서 정하도록 하고 있으며, 내부 상품심의위원회 의결을 통해 특약에 명시된 일정 범위를 보험료 등은 매매기준율에 +2원, 보험금 등은 매매기준율에 -2원으로 일괄 적용하고 환산하고 있다.

\* 보험료 등의 금액을 납입할 때에는 전신환매도율과 매매기준율 사이의 범위,

보험금 등의 금액을 지급할 때에는 전신회매입률과 매매기준율 사이의 범위

또한, 회사는 보험료 등을 원화로 환산하기 위해 주거래은행으로부터 환율 정보를 제공받고 있으며, 매일 23시 30분 기준으로 제공받는 환율을 약관상 환산 기준일의 최종으로 고시하는 매매기준율로 판단하고 있다.

그러나 회사가 환율을 제공 받는 23시 30분 이후에도 주거래은행에서 고시하는 환율이 계속해서 변동하는 사례가 발생하고 있어 23시 30분 이후 환율이 급격하게 변동하는 경우 특약에서 정한 일정 범위를 벗어난 환율로 보험료 등을 환산하게 되는 상황이 발생할 수 있다.

#### <조치할 사항>

회사는 환율변동 내역을 23시 30분 이후에도 확인할 수 있도록 전산시스템을 개선할 필요가 있고, 주기적으로 환율적용이 올바르게 적용되었는지 사후검증을 수행할 수 있도록 관련 업무절차를 개선하시기 바랍니다.

### (5) 보험금 지급누락방지 시스템 운영 미흡

회사는 보험수익자가 정당하게 지급받아야 할 보험금이 누락되지 않도록 보험금 청구시 제출된 증빙서류의 기재내용을 기초로 관련 보장금부의 지급여부에 대한 주기적인 사후검증 등 보험금 지급누락방지 업무를 수행하고 있으나, 매월 사후검증을 위해 지급누락 점검대상을 산출하는 과정에서 점검대상이 일부만 산출되거나 특정 담보에 대한 산출로직이 없어 사후검증이 일부 이루어지지 않은 사실이 있다.

또한, 사후검증 결과 미지급 보험금을 사후 지급하는데 그치지 않고 점검결과를 토대로 산출로직의 적정성과 점검대상의 정합성을 주기적으로 확인하고, 반복적인 유형의 지급누락 건 발생 방지를 위해 원인파악 및 개선방안을 마련하고 추진하여야 하나, 그동안 지급누락방지 전담 인력 없이 사후검증과 보험금 심사 및 조사 등의 업무를 병행함에 따라 실효성 있는 점검과 지속적인 개선 및 후속조치가 이루어지지 않은 사실이 있다.

## <조치할 사항>

회사는 지급누락방지 전담인력을 지정하고, 사후검증 요건과 매뉴얼 정비, 반복적인 누락 유형에 대한 개선방안 마련 등을 수행하여 실효성 있는 사후검증과 후속조치가 지속적으로 이루어질 수 있도록 지급누락 방지 업무 체계를 보완하시기 바랍니다.

### (6) 재무제표 주석사항 오기재에 관한 사항

회사는 내규 「회계규정」 및 「회계업무처리세칙」에 따라 재무제표를 명확하게 작성해야 하는데도 FY'23 재무제표 내 주석 사항 작성 및 공시할 때 아래 ①~②와 같이 업무절차에 미흡한 점이 있으므로 동 절차를 개선할 필요가 있다.

- ① 2023년 시행된 기업회계기준서 제1117호('이하 기업회계기준서')에 따르면 보험회사는 “보험서비스를 제공하고 그러한 서비스에 대한 교환으로 받을 것으로 기대하는 대가를 반영한 금액을 보험수익”으로 인식한다. 그러나 회사는 이러한 사항을 반영하지 않고 2022년 이전까지 적용된 제1104호(보험계약)에 따른 수익 인식 기준을 재무제표 주석으로 기재\*하였다.

\* “회사는 보험료 회수기일이 도래되어 납입된 보험료를 수익으로 인식하며...(생략)”

또한, 변동수수료접근법(VFA)을 적용한 보험계약에 대해 기업회계기준서에 따른 위험경감수단을 사용하지 않는에도 재무제표 주석 상 위험경감수단을 사용한다고 잘못 기재\*하였다.

\* “회사는 위험경감수단을 사용하여 화폐의 시간가치 및 금융위험이...(생략)”

- ② 회사는 외환위험을 “환율변동으로 인해 회사의 순자산가치가 하락할 위험”으로 정의하며 환율변동에 직·간접적인 영향을 받는 모든 자산과 부채를 측정 대상(exposure)으로 분류한다. 그러나 회사는 재무제표 주석상 외화보험계약과 관련된 보험계약마진\*(CSM)을 제외하고 외환위험 익스포저를 기재하였다.

\* “기업회계기준서 제1021호 ‘환율변동효과’를 적용하는 경우에는 보험계약마진을 포함하여 계약집합을 화폐성 항목으로 회계처리한다.”(문단 30)

이와 같은 질적 및 양적 주석사항 오기제는 재무정보 이용자의 이해가능성을 저해할 수 있다.

#### <조치할 사항>

회사는 내규 「회계규정」 및 「회계업무처리세칙」에 근거하여 재무제표 구성항목인 질적, 양적 주석 관련 작성 업무 및 검증 절차를 개선하시기 바랍니다.

### (7) 정보처리시스템 성능관리 불합리

회사는 내규 「IT관리규정」, 「인프라 운영 업무매뉴얼」 등에 따라 CPU, 메모리, 디스크 등 전산자원의 성능을 수집·분석한 보고서를 매월 작성하여 추이 분석을 수행하고 성능관리 대상 및 임계치 기준을 설정하여 운영하고 있다.

하지만 전산자원의 단계별(정상, 주의, 경계, 심각) 임계치 기준을 2023년 12월 생명보험협회에서 배포한 「전산시스템 성능관리 가이드라인」 기준보다 높게 수립<sup>1)</sup>하여 운영하고 있고, 각 임계치 단계별 대응 방안을 수립하지 않아 임계치 수준을 초과하는데도 적절한 조치를 취하지 않는 사례가 존재<sup>2)</sup>하는 등 성능관리 미흡으로 인한 전산장애 발생이 우려된다.

1) 회사 기준(주의: 85%, 경계: 90%, 심각: 95%)은 동 가이드라인보다 10%~15% 상향하여 운영

2) (예시) 계정계 주요 운영시스템(pd-los-was-01~08)의 평균 메모리 사용률이 96%를 초과

또한 동 가이드라인에서 요구하는 장애 사전 예방조치를 적기에 수행하기 위한 성능관리 조직 및 긴급증설 절차를 마련하지 않고 있다.

#### <조치할 사항>

회사는 동 가이드라인 및 정보시스템 성능분석 결과 등을 고려하여 전산자원의 사용 임계치를 합리적인 수준으로 설정하고 단계별 대응 방안을 구체적으로 수립하는 한편, 장애 예방조치를 위한 성능관리 조직 및 긴급 증설 절차 등을 마련하시기 바랍니다.

## (8) 전산자료 보안관리 미흡

회사는 전산자료의 유출, 파괴 등을 방지하기 위하여 전산자료 보호대책을 수립·운영하고 있으나, 아래 (가) 및 (나)와 같이 전산자료 보안관리에 미흡한 사항이 있으므로 이를 개선할 필요가 있다.

### (가) 외주인력의 자료 반출 시 보안정책 개선 필요

「IT보안세칙」에 따라 외주인력이 생산한 자료는 내부망에 저장하되 외부로 반출하는 경우 사전에 정보보호책임자의 승인이 필요하다.

하지만 회사는 외주인력이 망간자료전송시스템을 이용하여 내부망에 있는 자료를 외부로 반출 시 정보보호책임자의 승인 없이 반출\*할 수 있도록 운영하여 중요한 자료가 외부로 유출될 우려가 있다.

\* 검사대상기간 중 외주인력이 자료 반출을 신청한 106건 중 현장대리인(외주업체 소속 관리자)의 승인으로 50건이 반출(반출자료는 일반문서 서식 및 본사 보고용 서류 등)

### (나) 이용자 정보를 활용한 테스트 시 통제 강화 필요

「정보보호규정」에 따라 테스트 시 이용자 정보가 불가피하게 필요한 경우 변환하여 사용하고, 테스트 데이터의 사용기간이 종료되면 즉시 삭제하되 주요 정보가 포함된 테스트 데이터에 대해서는 사용기간과 관계없이 매월 일괄 삭제하고 있다.

하지만 회사는 이용자 정보의 변환작업 실패로 재작업하는 경우 별도의 승인 절차 없이 데이터베이스관리자(DBA, Database Administrator)가 직접 변환 신청·승인할 수 있도록 운영\*하였으며, 사용기한을 초과한 테스트 데이터의 삭제 여부를 확인하는 절차를 마련하지 않아 이로 인한 데이터의 남용 및 잔존 우려가 있다.

\* 검사대상기간 중 책임자 승인을 통해 실행 완료한 변환작업 20,059건 중 데이터베이스 문제로 변환 실패하여 데이터베이스관리자가 책임자 승인 없이 재실행한 작업은 1,268건

### < 조치할 사항 >

회사는 외주인력이 자료를 반출하는 경우 정보보호책임자의 승인을 거치도록 하는 등 자료의 반출입 보안정책 및 절차를 개선하시기 바랍니다.

또한 이용자 정보의 변환작업이 실패한 경우에도 책임자의 승인을 거치도록 하고, 승인 내역 및 사용이 종료된 테스트 데이터의 삭제 여부 등을 주기적으로 점검하는 방안을 마련하는 등 전산자료의 보안관리를 개선하시기 바랍니다.



## (9) 제3자 연계 서비스 재해복구훈련 미흡

회사는 내규 「IT업무위수탁에관한지침」 및 「업무지속성계획(BCP)관리규정」에 따라 통합인증, OpenAPI 조회 등 제3자 정보처리 위탁 및 연계 서비스(25개)를 제공하고, 이 중 업무영향분석<sup>1)</sup>(BIA, Business Impact Analysis)을 통해 선정된 16개 연계 서비스<sup>2)</sup>에 대해서는 재해·재난 등으로 인한 업무 중단에 대응하기 위해 연 1회 이상 모의훈련(재해복구훈련)을 수행하고 있다.

- 1) 업무 중단 시에도 수행되어야 할 주요 업무(핵심업무)를 정의하는 절차
- 2) OpenAPI 조회, 신계약 심사, 약관 발송, 펌뱅킹, 자동이체/금융거래정보, 고객정보 조회, 카드납입, 전자세금계산서, 세금우대/모집조직/보험가입내역/변사자 조회, SAP 채권/거래소별 정보 수신, 개인정보노출자 조회, 공전소, SMS/알림톡, KB FCC, MSP 서비스, 연금포털/실손보험 청구

하지만 업무영향분석을 통해 재해복구훈련 대상으로 선정한 일부 서비스(방카 영업 관련 서비스 등)에 대한 재해복구훈련을 수행하지 않았고, 재해복구훈련시 2개 이상의 외부기관과 연계가 필요한 업무\*에 대한 파악이 미흡하여 외부기관과 연계한 재해복구 훈련이 제대로 이루어지지 않아 훈련 완성도가 저하되었으며, 이로 인해 동 서비스의 장애·중단 시 외부 리스크가 내부로 전이될 우려가 있다.

\* 보험금 수금 업무(금융결제원, KSNET), DM 청약 업무(트랜스코스모스, KB국민카드) 등

### < 조치할 사항 >

회사는 업무영향분석을 통해 선정된 핵심업무 관련 연계 서비스가 재해복구 훈련 대상에서 누락되지 않도록 업무영향분석 결과와 재해복구훈련 계획 간의 연계 및 식별·대조 절차를 강화하고, 2개 이상의 기관과 연계가 필요한 핵심업무의 식별 및 관련 기관과의 협조체계 구축 등을 통해 재해복구훈련을 내실화하는 등 제3자 연계 서비스의 비상대응체계를 개선하시기 바랍니다.

## (10) 암호 관리체계 운영 미흡

회사는 내규 「암호화세칙」에 따라 암호키 및 암호 알고리즘의 관리 절차와 기준을 마련하고, 암호화 관리 준수 여부를 모니터링하고 있다.

하지만 회사는 취약한 암호 알고리즘을 웹사이트(메인 홈페이지, 본인인증, 모바일센터, 모바일 옴니채널, 영업지원시스템)에 사용할 수 있도록 내규에 규정<sup>1)</sup>하고 있으며, 암호키 및 암호키 관리대장의 관리가 미흡<sup>2)</sup>하다.

- 1) TDES(Triple Data Encryption Standard), RC4(Rivest Cipher 4) 등 취약한 암호 알고리즘을 사용할 수 있도록 설정, 이 중 TDES는 내규에서 사용 가능한 암호 알고리즘으로 규정
- 2) 암호키 유효기간 설정 기준 및 암호키 생애주기별(주입·운용·갱신·폐기) 세부 관리방안이 부재하며, 암호키 관리대장을 관리 담당자 외 다른 직원(정보보호부)이 접근·열람 가능

### < 조치할 사항 >

그러므로 회사는 동 웹사이트에 취약한 암호 알고리즘을 사용할 수 없도록 조치한 후 취약점 점검 등을 통해 조치의 적정성을 확인하고, 사용 가능한 암호 알고리즘 및 암호키 유효기간 설정 기준을 포함한 암호키 생애주기별 세부 관리방안을 관련 내규에 반영하며, 암호키 관리 담당자 및 책임자 등 권한이 있는 사람만 암호키 관리대장에 접근·열람이 가능하도록 통제를 강화하는 등 암호 관리체계 운영을 개선하시기 바랍니다.

## (11) 중요단말기 관리 미흡

회사는 내규 「IT보안세칙」에 의해 정보처리시스템 관리용 단말기 등을 중요 단말기로 지정하고 일반 단말기에 적용하는 보호대책 이외에 인터넷 접속 금지, 악성코드 감염 여부를 매일 점검하는 등 강화된 보호대책을 적용하여 운영하고 있다.

하지만 정보처리시스템에 접속할 수 있는 관리·운영 목적의 가상단말기 (VDI, Virtual Desktop Infrastructure) 59대를 중요단말기로 지정하지 않았으며, 중요단말기(16대)에 대한 악성코드 예약검사 및 CMOS 비밀번호 설정 등의 보호 대책이 미흡<sup>1)</sup>하고 자산관리를 소홀<sup>2)</sup>히 하여 이로 인한 해킹 등의 보안 위협에 노출되거나 비상시 신속한 대응이 어려울 수 있다.

- 1) 백신 프로그램(V3)을 통해 최신 업데이트 및 실시간 감시는 수행되었으나 예약검사가 실행되지 않은 단말기가 존재하고(2대), USB 저장장치 부팅디스크를 이용한 해킹 방지를 위해 부팅 시 사용하는 CMOS(Complementary Metal-Oxide Semiconductor) 비밀번호를 설정·점검하지 않았으며(16대), 단말기 본체 및 USB 포트를 봉인하지 않음(9대)
- 2) 자산관리표를 부착하지 않았거나 자산관리번호를 현행화하지 않음(9대)

### < 조치할 사항 >

회사는 중요단말기의 지정 기준 및 절차를 정비하여 관리·운영 목적으로 정보 처리시스템에 접속할 수 있는 단말기 등을 중요단말기로 지정하고, 중요단말기에 대한 악성코드 검사, CMOS 비밀번호 설정, 단말기 본체 및 USB 포트의 봉인, 최신 자산관리표 부착 등 적절하게 조치한 후 이를 지속 관리할 수 있도록 관리적·물리적·기술적 보호대책을 강화하시기 바랍니다.

## (12) 전산센터 관리·운영 미흡

회사는 내규 「데이터센터 운영세칙」에 따라 전산장비를 출입 통제구역으로 지정한 전산실에 배치하고 출입 카드, 감시카메라(CCTV) 등으로 출입을 통제하며, 시스템 운영 담당자가 전산장비 및 부대설비의 상태를 점검하고 서버와 주변장치를 운영·통제하도록 규정하고 있다.

하지만 2023년 1월 합병 이후, 서버 등 전산장비 이전은 완료하였으나 전산실의 운영 환경에 대한 관리가 다소 미흡하여 개선이 필요하다.

전산설비 및 기반시설의 미흡사항

| 구 분                     | 세부 미흡사항                                                                                                                                                                                                                   |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 서버, 서버랙 등<br>전산설비       | <ul style="list-style-type: none"><li>○ 서버랙 후면 하단의 케이블 홀 마감재(콜드락)가 다수 파손 (검사기간 중 조치완료)</li><li>○ 일부 서버랙의 전력 및 온습도 모니터링 장비 등 미설치</li><li>○ 서버랙 외부로 케이블(통신·전원) 노출</li><li>○ 서버랙 내 운영 중인 장비와 유휴 장비를 동일 전원에 연결하여 운용</li></ul> |
| CCTV,<br>공조설비 등<br>기반시설 | <ul style="list-style-type: none"><li>○ 타 계열사와의 구역 분리를 위해 케이지를 추가 설치하면서 감시카메라(CCTV) 사각지대가 발생</li><li>○ 항온항습기의 공급 온습도와 실제 개별서버 간의 온습도 편차가 큰 상태이므로 전산실 내 온습도의 조정 및 최적화 필요</li></ul>                                         |

또한 주전산센터 관리·운영을 지주사에 위탁하면서 전력·소방 등 안전과 직결된 기반시설의 세부 점검내역에 대한 적정성을 자체적으로 확인하지 않아 관리 소홀로 인한 안전사고가 발생할 위험이 있고, 사고 발생시 책임소재가 불분명한 문제가 발생할 우려가 있다.

### <조치할 사항>

회사는 전산센터 내 전산설비의 미흡사항에 대해 신속하게 보완하는 한편, 기반시설 점검에 대해서는 회사의 전산센터 관리자가 자체적으로 적정성 점검을 수행하는 절차를 관련 내규에 반영하는 등 전산센터 관리·운영을 개선하시기 바랍니다.

### (13) 일괄작업 통제 불합리

회사는 내규 「데이터 관리세칙」에 따라 업무시간 이외 혹은 비상 상황으로 긴급한 데이터 변경이 필요한 경우, 예외적인 방법으로 처리\*하고 관련 작업기록을 시스템에 남기도록 하고 있다.

\* 긴급 변경내용을 책임자에게 유선 보고 → DBA를 통해 데이터 변경내용을 운영계에 반영  
→ 개발자와 업무담당자가 테스트 → 긴급 변경내용을 시스템에 기록 후 책임자 승인

하지만 긴급 일괄작업을 수행하는 경우 사후 이력 관리가 미흡하여 작업을 수행한 날로부터 책임자의 승인까지 장기간 소요되는 사례\*가 다수 있어 중요 일괄작업에 대한 적정성 확인이 적시에 수행되지 않을 우려가 있다.

\* 긴급 일괄작업 수행일로부터 책임자 승인까지 43일, 59일, 95일 등 소요

또한 일괄작업을 재실행해야 하는 오류\*가 반복적으로 발생하고 있으나 별도의 원인분석 없이 발생한 오류에 대해서 임시 조치만 수행하고 있다.

\* 일괄작업 시스템(AUTOSYS) 상 '원인불명의 처리 실패 오류', '로그 부재로 확인이 불가능한 오류'

#### <조치할 사항>

회사는 긴급 일괄작업을 수행하는 경우 작업내용 및 결과에 대한 적정성에 대해 적시에 책임자 승인까지 완료하고 관리될 수 있도록 관련 내규에 절차를 마련하시기 바랍니다.

또한 동일·유사한 유형의 오류가 지속·반복적으로 발생하는 일괄작업이나 프로그램에 대해서는 주기적으로 점검하는 내부 기준을 수립하고 원인분석 및 관련 프로그램 개선 등을 통해 오류 발생을 최소화하시기 바랍니다.