경영유의사항 등 공개안

1. 금융기관명 : 메리츠화재해상보험㈜

2. 제재조치일 : 2024. 9. 2.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의 18건, 개선 16건

4. 제재대상사실

가. 경영유의사항

(1) 이사회 역할 및 운영의 실효성 강화 필요

㉮ 금융지주 및 계열사와의 거래에 대한 이사회의 감독 역할 강화 필요

이사회는 회사 경영진으로부터 독립성을 확보하여 효율적으로 경영진을 지휘·감독함으로써 보험회사 경영의 투명성과 책임성을 제고할 수 있도록 운영되어야 한다.

특히, 메리츠화재해상보험(주)(이하 '회사') 대표이사는 검사대상기간 중 ㈜메리츠금융지주(이하 '금융지주')의 대표이사를 겸직하고 있어, 이사회는 금융지주 및 계열사와의 거래에 있어 이해상충 발생 여부 및 회사 건전성에 미치는 영향 등을 면밀히 검토할 필요가 있었다.

그런데 이사회 의장인 대표이사는 검사대상기간 중 총 11회에 걸쳐 회사와 금융지주 간 거래에 대한 의결권을 직접 행사한 사실이 있었다. 또한 계열사와의 거래에 있어 사외이사의 문제 제기에 대해 명확한 근거 제시 없이 대표이사가 직접 답변한 사례도 있었으며, 해당 사안에 대해 다른 이사들은 별도 문제 제기나 추가 사실관계 확인 없이 안건을 의결하였다. 이에 따라 이사회 운영의 독립성·실효성이 저해되고 경영진에 대한 효과적 감독 역할이 미흡한 실정이었다.

<조치할 사항>

따라서 금융지주 및 계열사와의 거래에 대한 이사회 의결시 이해상충 및 의결권 제한 여부 등에 대한 점검 절차를 강화하고, 이사회 의결안건에 대한 이사의 발언 및 문제 제기에 대한 독립성을 보장하고 이에 대한 객관적인 정보 및 근거가 제공될 수 있도록 하는 등 이사회의 독립성과 경영진에 대한 감독 역할을 강화할 필요가 있습니다.

㉯ 사외이사의 역할 및 이사회 운영 절차에 대한 관리 강화 필요

회사의 경우 이사회 의장이 사내이사로서 회사의 대표이사와 금융지주의 대표이사를 겸임하고 있어, 효율적인 경영진 견제 기능 제고를 위한 선임사외이사 등 사외이사의 적극적 역할*과 책임이 요구되는 상황이다.

* 사외이사 전원으로 구성되는 사외이사회의 소집·주관, 사외이사의 효율적인 업무수행 지원, 사외이사의 책임성 제고를 위한 지원 등

그러나 검사대상기간 중 선임사외이사가 사외이사회를 소집한 사례가 없고, 이사회 의결시 사외이사가 안건에 대한 반대 의견을 제시한 사례를 찾아 볼 수 없는 등 사외이사의 업무수행 실적과 역할이 미흡하였다.

또한, 이사회는 회사에 대한 충분하고 정확한 정보를 바탕으로 주요 경영사항에 대한 심도 있는 검토를 통해 경영진에 대한 효과적인 감독 역할을 수행할 필요가 있다.

그런데 회사는 사외이사에게 이사회 개최 하루 전에야 자료를 제공한 사례가 있는 등 안건검토를 위한 충분한 시간이 부족하여 이사의 원활한 직무수행에 지장을 초래할 우려가 있었다.

또한 이사회 운영 결과의 사후 관리에 있어서도 안건 통지일, 의결권 행사 위원 성명 등을 사업보고서 등에 잘못 기재한 사례가 있었다.

<조치할 사항>

따라서 회사는 사외이사회의 소집 절차 마련, 사무지원 체계 정비 등 사외이사의 역할 강화를 위한 대책을 마련하고, 이사회 등의 소집, 안건통지 및 회의자료 제공, 사후 기록 관리 등에 대한 절차 및 기준을 정비하는 등 이사회 운영의 실효성을 제고할 필요가 있습니다.

(2) 장기적 성과 제고를 위한 성과보수체계의 정비 필요

보험업은 장기에 걸쳐 성과가 실현되는 특성이 있으므로 보험회사는 단기 성과를 우선하여 과도한 위험을 부담하여서는 아니되고, 보험상품 개발·보험영업·자산운용 등 전반에서 지속 가능한 성장, 소비자 신뢰 등이 확보될 수 있도록 장기적 가치를 창출할 필요가 있다.

따라서 보험회사의 성과보수 체계는 회사의 장기적 가치를 제고하고, 임직원이 장기 성과에 대한 적절한 책임을 지고 보수 수준에 부합하는 성과를 창출하여 사회적 신뢰와 책임성을 높일 수 있도록 운영되어야 한다.

그러나 회사는 2020년~2023년 동안 대표이사의 성과평가지표를 ROE ○○%, 인보험 시장점유율(M/S) 순위 □□%, 주주수익률 등 단기 실적 또는 단기 수익성 지표 위주로 구성하였다.

또한, 회사는 임원의 이연 성과보수에 대해 연도별 ROE를 복리로 계산하도록 하고 있는데, 이러한 성과보수 산출 방법의 경우 임원이 과도한 위험을 부담하여 단기성과를 추구할 유인이 있다.

한편 회사는 2020년~2023년 중 임원에게 지급할 성과보수의 총액 산정시 회사의 성과평가 결과와 상관없이 성과보수 지급 전 세전 당기순이익만을 직접적인 성과로 인식하여 매년 세전 당기순이익의 일정비율(目.目%)을 임원 성과보수의 총 지급규모로 산정하였다.

그리고 임원에 대하여는 표준연봉에 개인별 성과평가지표 달성도를 고려하여 성과보수를 결정하고 있으나, 대표이사에 대한 성과보수는 성과평가 결과와 관계없이 임직원 성과보수 지급 전 세전이익의 일정비율(▣.▣%)로 산정하였다. 또한 대표이사는 성과보수를 ○○년간 이연하여 지급하되 퇴직하는 경우 △년 이상 이연된 성과보수는 일시에 지급할 수 있도록 운영하였다.

이와 같은 회사의 성과보수체계는 중장기적 가치 제고를 고려하여 운영되어야 하는 보험산업의 특성, 성과보수 지급에 따른 재무건전성 변화, 보험산업의 제도변화 등을 반영하지 못한 측면이 있다.

<조치할 사항>

따라서 회사는 중장기적 관점에서 보험산업의 특성과 재무건전성 변화 등을 반영하여 성과보수체계가 운영될 수 있도록, 회사 및 대표이사의 성과평가지표 구성, 임원에 대한 이연 성과보수의 장기성과 연계 방식, 성과보수의 총 지급 규모 산정 및 대표이사 성과보수의 산정·지급 방안 등에 대한 종합적인 개선 대책을 마련하고, 불합리한 성과보수 체계로 인해 단기적 이익만을 추구하여 과도한 위험을 부담하지 않도록 유의하시기 바랍니다.

(3) 공시이율 산정 체계 및 절차 강화 필요

장기손해보험 만기환급금 또는 해지환급금의 재원이 되는 적립부분 계약자적립금은 공시기준이율*에 '조정률'을 반영한 공시이율에 따라 산출된다. 따라서 회사는 공시이율 산출의 합리성 및 예측가능성이 제고될 수 있도록 조정률을 객관적이고 투명하게 결정할 필요가 있다.

* 운용자산이익률과 외부지표금리 수익률을 고려하여 산출

그러나 회사는 금번 검사대상기간 중 운용자산이익률 상승 등으로 공시기준이율이 상승하였는데도 공시이율을 오히려 더 낮게 산정하거나, 외부지표 금리 및 운용자산이익률이 모두 상승하고 있음에도 공시이율을 상대적으로 소폭으로만 조정하거나 여전히 낮은 수준으로 유지하는 한편, 공시이율을 예정이율* 보다 장기간 더 낮게 운영하는 등 조정률 결정에 대한 일관성이 부족하고 이에 대한 구체적 기준이 미흡한 실정이다.

* 장기손해보험 계약자적립금 중 보장 부분은 확정금리인 예정이율로 부리하며 적립 부분은 변동금리인 공시이율을 적용

한편 회사 「공시이율 적용에 관한 세부지침」에 따르면 공시이율 결정절차는 자산운용 기획 담당 부서, 장기보험 상품 담당 부서 등이 참여하는 '공시이율 결정 회의체'에서 결정하도록 하고 있다.

그러나 회사는 검사대상기간 중 참석 대상 부서의 이견이 없었다는 이유로 동 회의체를 개최한 실적이 없었다.

이에 따라 공시이율 산정의 기초가 되는 공시기준이율이 상승하고 있는데도 공시이율을 반대 추세로 결정하는 등에 대한 충분한 논의 없이 공시이율을 결정하였다.

<조치할 사항>

따라서 장기손해보험에 대한 공시이율이 공시기준이율, 금리 변동위험 등을 고려하여 합리적으로 결정될 수 있도록 관련 기준 및 절차를 정비하고, '공시이율 결정 회의체'의 실효성을 제고할 수 있는 방안을 마련하는 등 공시이율 산정 체계를 강화할 필요가 있습니다.

(4) 보험계약 인수심사 관리 체계 및 절차 강화 필요

회사「내부통제기준」등에 따르면 보험계약심사는 역선택 및 불량계약의 유입 방지를 위해 독립성과 전문성을 확보하도록 하고 있다. 이에 따라 회사는 보험계약 심사부서가 본연의 업무에 충실할 수 있도록 성과평가지표를 설정·운영할 필요가 있다.

그러나 회사는 보험계약심사를 담당하는 장기보험팀의 성과평가지표에 매출 확대를 포함하고 있었다. 이에 따라 보험계약심사 부서의 독립성과 전문성에 반하는 부적절한 계약심사가 이루어질 우려가 있었다.

한편 보험가입한도는 위험보장 목적에 부합하게 설정·변경해야 하므로 보험가입한도를 변경하고자 하는 경우에는 그 사유를 면밀히 검토할 필요가 있다.

그러나 회사는 유사암진단비 등 일부 담보에 대한 보험가입한도 변경시 명시적 근거 없이 매출 확대 등을 이유로 수시로 이를 변경하였다. 이에 따라 보험계약심사 기능이 약화됨으로써 불량계약 유입 등의 우려가 있었다.

<조치할 사항>

따라서 회사는 보험계약심사 부서가 매출 목표에 영향을 받지 않도록 조직 체계와 평가기준을 정비하고, 객관적·합리적 근거를 통해 위험보장 목적에 부합할 수 있도록 보험가입한도를 설정·변경하는 방안을 마련하는 등 보험계약 인수심사업무에 대한 관리 체계를 강화할 필요가 있습니다.

(5) 계리적 가정 설정 및 검증 절차 강화 필요

보험부채를 공정가치로 평가하는 IFRS17 제도의 시행에 따라 회사는 내·외부 정보를 활용한 편향되지 않은 최적의 계리적 가정에 따라 보험부채를 평가해야 한다. 이에 따라 회사가 사업계획을 수립하는 시점에서는 계리적 가정의 추정 오차에 따른 예실차를 고려하지 않는 것이 타당하다.

그러나 회사는 2023년 사업계획 수립시 ▧,▧▧▧억원(2023년 예상 당기순이익 ▨.▨▨조원의 ◉◉%)을 2023년도 예실차 이익으로 달성하겠다는 목표를 설정하고 이를 이사회 안건으로 상정한 사실이 있었다. 이에 따라 회사가 의도적으로 계리적 가정을 실질과 달리 보수적 또는 공격적으로 설정하는 경우에는 보험부채가 왜곡되어 나타날 우려가 있다.

<조치할 사항>

따라서 회사는 계리적 가정 수립시 가정관리위원회 등을 통해 검증 절차를 강화하여 예실차가 발생하지 않는 최적의 계리적 가정으로 사업계획을 수립하고, 사업계획의 이사회 보고시 IFRS17 제도에 대한 이사회의 이해도를 제고하는 등 계리적 가정 설정 및 사업계획 수립 절차를 강화할 필요가 있습니다.

(6) 명령휴가·순환근무 제도 실효성 제고 필요

보험회사는 금융사고 예방을 위한 내부통제의 중요성을 인식하고, 사고위험 부문에 대한 순환근무제, 명령휴가제 등 인사관리 체계를 강화하여 상호견제 및 사고 예방 기능의 실효성을 제고하여야 한다.

회사는 금융사고 방지를 위해 경리, 자산운용 등 금융사고 발생 가능성이 높은 부서를 선정하고 동 부서에 대해 명령휴가·순환근무 제도를 운영 중이나, 출납·수납 업무를 수행하는 일부 부서*를 적용대상에 포함하지 않았다.

* 부동산 운용실, 상품전략실, 구상지원파트 등

또한, 명령휴가 대상 부서를 매년 1개 부서만 선정하여 동 부서 인원 중 2명에 대해서만 명령휴가를 실시하였고, 실시 방법도 불시 명령이 아닌 사전 안내 방식으로 운영하였으며, 실시 이후 준법감시부서 등에서 점검결과를 사후 확인하는 절차도 마련하지 않았다.

한편, 2023년 9월말 현재 순환근무 적용 대상 인원 중 ○○○명 중 153명(□□.□%)이 3년을 초과하여 동일 보직에서 근무하고 있는 등 금융사고 방지를 위한 제도 운영의 실효성이 미흡한 실정이다.

<조치할 사항>

따라서 회사는 명령휴가 및 순환근무 대상 부서 및 실시 인원을 확대하고 명령휴가의 불시명령 시행, 사후점검 절차 및 기준을 마련하는 등 명령휴가 및 순환근무제도의 실효성을 제고하여 금융사고 예방을 위한 내부통제 기능을 강화할 필요가 있습니다.

(7) 장기보험 손해조사비율 산출업무의 합리성 제고 필요

보험회사는 예정손해조사비율을 산출할 때, 과거 실제 지급된 손해조사비와 보험료 수입을 통한 손해조사비 재원 규모의 변동 추세를 합리적으로 고려하고, 객관적 통계자료 및 기법 등을 통해 향후 지출될 손해조사비를 일관성 있게 산출할 필요가 있다.

회사는 예정손해조사비율 산출을 위해 2021년부터 「장기손해보험 손해조사비율 산출 및 적용기준」을 마련하여 시행*하고 있다.

* 예정손해조사비율 = (분자) 손해조사비(= 지급손해조사비×물가·임금증감률×추세계수) ÷
(분모) 보장보험료×안전할증

그러나 회사는 예정손해조사비율을 산출하면서 사고발생 건수만을 사용하여 실제 손해조사비(분자)의 기초통계 기간과 적용시점 사이의 추세 변동만을 반영함으로써 보장보험료(분모)의 변동 요인은 고려하지 않았으며, 기초통계기간 적용 방식의 기준 없이 기초통계 기간으로 2021년에는 ▣년, 2022년에는 ▥년을 적용하였다. 또한, 물가상승률 등 안전할증 반영시 고려 요소가 내부지침에 명확히 기재되어 있지 않았다. 이에 따라 예정손해비율 산출 과정의 합리성과 일관성이 저해되는 문제가 있었다.

<조치할 사항>

따라서 회사는 예정손해조사비율 산출시 손해조사비와 보장보험료 변동의 정합성을 제고하고, 기초통계 기간과 안전할증 등에 대한 적용 기준을 구체적으로 마련하여 시행하는 등 장기손해보험 손해조사비율 산출 절차를 강화할 필요가 있습니다.

(8) 보험모집조직 교육 관련 내부통제 강화 필요

보험회사는 보험소비자의 합리적 선택이 침해되지 않도록 보험상품에 대한 정확한 지식과 정보를 제공하고, 보험계약 체결을 권유할 때 건전한 모집질서를 저해하는 일이 없도록 모집조직을 충실히 교육·관리하여야 한다.

그러나 회사는 검사대상기간 중 모집조직 교육담당자에게 배포하는 '영업방향' 자료에 구체적 설명 없이 단순히 자사 상품이 우수하다는 내용이 포함된 문구 등을 기재한 사례가 있었다.

또한, 모집조직 교육에 사용되는 '소식지' 자료는 준법관리부서·소비자보호부서 등을 통한 사전 심의절차 없이 영업부서가 필요할 때마다 수시로 제작하여 사용하고 있었다.

한편, 회사 영업부서는 금융감독원이 절판마케팅 등을 통한 불건전 영업행위 방지를 요구*한 이후에도 모집조직에 운전자보험 및 어린이보험 등의 절판마케팅을 반복적으로 독려한 사례가 확인되었다.

* 불합리한 상품개발·판매 관련 유의사항 통보(2023.7.19.), 일부 보장성 상품 구조개선에 따른 영업 관련 유의사항 통보(2023.7.27.) 등

<조치할 사항>

따라서 회사는 보험모집조직 교육 목적으로 작성되는 자료 등에 대한 사전심의 대상 확대, 사전심의 기준 및 절차 강화 등을 추진하고, 동 자료에 대한 작성 주체, 준수사항 등을 구체적으로 명확히 마련할 필요가 있습니다. 또한 모집조직으로 하여금 불건전 영업행위를 유발할 수 있는 비공식적 안내메시지 등의 작성·배포·활용을 차단하기 위한 대책을 마련하는 등 내부통제를 강화할 필요가 있습니다.

(9) 보험계약 해지시 안내절차 강화 필요

보험계약의 가입·해지와 관련하여 보험계약자의 이해관계는 보험상품별 특성에 따라 다를 수 있고, 보험상품에 대한 충분한 정보가 없으면 보험계약자가 유·불리를 인지하지 못한 채 불리한 선택을 할 가능성이 있으므로 보험회사는보험계약자의 권익이 충실히 보장될 수 있도록 금융상품에 대한 정보를 성실하고 정확하게 제공할 필요가 있다.

그러나 회사는 2019. 7. 1.~ 2023. 8. 31. 기간 중 기존 보험계약을 해지하면서 10년 이상 납입하고, 장기 유지된 보험계약에 대해 ①보험료를 완납(또는 거의 완료)하여 만기까지 보장만 받으면 되고 ②기존에 면책기간이 설정되어 있는 담보를 가입했거나 또는 질병·부위 부담보 조건으로 계약을 체결했다면 보장 받을 수 있는 시점이 도래하는 등 기존 보험계약을 유지하는 것이 신계약을 체결하는 것보다 보험계약자에게 유리할 가능성이 있는 경우가 있다.

따라서 회사는 기존 보험계약 해지 단계에서 보험계약자에게 보험료 납입기간 만료일까지 남은 기간, 보장되는 사항, 보장기간 등의 정보를 정확히 제공하여 보험계약자가 중도 해지 유·불리를 알 수 있는 상태에서 보험료 납입기간 만료일까지 계약 유지여부를 선택할 수 있도록 할 필요가 있다.

<조치할 사항>

이에 따라, 회사는 보험계약 가입·해지 절차를 진행하면서 보험계약자의 선택에 영향을 미칠 수 있는 보험료 납입 만료 시점, 잔여 보장기간 등에 대한 객관적인 보험계약정보를 충분히 제공하여 보험계약자가 합리적으로 판단을 할 수 있도록 안내 절차를 강화할 필요가 있습니다.

(10) 의료자문제도 관리 강화 필요

회사는 보험금 지급심사 과정에서 질병이나 장해의 진단 등 의학적 소견이 필요한 보험사고에 대해 의료자문을 실시하고 있으며, 이를 위해 「의료자문 업무처리 지침」을 마련하여 운영하고 있다.

동 지침에 따르면 의료자문의 적정성 심의 등을 위해 의료자문관리위원회를 설치하여 의료자문 실시대상 선정 기준의 적정성, 자문의 선정 및 편중 방지 기준의 적정성, 의료자문 실시 현황, 자문의 선정 현황 등을 심의하도록 정하고 있다.

그런데 2021년 4분기 이후 장기보험에 대한 의료자문 실시 건수가 크게 증가하였는데도 동 위원회에서 증가 원인을 분석하거나 관리 방안을 논의한 사실이 없는 등 위원회 운영이 미흡하였다.

또한, 2022년 1월~2023년 9월 기간 중 회사와 보험수익자가 장기보험의 보험금 지급 사유에 대해 합의하지 못해 제3의료기관에 의료자문(이하 '제3의료자문')을 실시한 결과, 159건 중 98건이 보험금 지급 사안으로 결정되었다.

이에 따라 의료자문 대상이 된 보험사고에 대해 현행 지급심사 기준이 적정한지 검토할 필요가 있었으나 이를 위한 검토 및 확인 체계는 마련되어 있지 않았다.

한편, 회사는 의료자문 편중을 방지하기 위해 장기보험의 경우 특정 자문병원의 자문건수가 분기별 전체 자문건수의 30%를 초과(자문의는 10%)하지 않도록 운영하고 있다.

그런데 2020년~2023년 동안 특정 병원에 대한 자문 비중은 최고 18.1%(2021년 2분기)였고, 특히 2023년의 경우에는 8.5%~9.1% 수준이었다. 이에 따라 의료자문 편중의 관리 유인이 낮은 등 회사의 편중 판단 기준이 높게 설정되어 있어 그 실효성이 미흡한 실정이다.

그리고 회사는 보험수익자와 합의하여 제3의료자문 기관이 결정된 경우에만 의료기관명 및 날짜 등을 전산시스템에 기록·관리하고 있다. 이에 따라 제3의료자문 기관 선정 관련 보험수익자간 이견 발생 여부, 보험수익자 의견 등을 확인할 수 없어 보험금 처리 과정에 지연이 발생하는 경우 이에 대한 원인 파악 및 신속한 대응이 어려운 상황이다.

<조치할 사항>

따라서 회사는 의료자문관리위원회를 통해 의료자문의 증가 원인, 특정 병원에 대한 자문 비중 등을 면밀히 분석·심의하여, 의료자문 실시 및 자문의 편중 기준 등의 적정성 검토 체계를 강화하고, 의료자문 결과에 따라 현행 보험금 지급심사 기준의 적정성을 재점검할 수 있는 절차를 마련할 필요가 있습니다. 또한, 의료자문 진행 과정을 전산시스템에 기록·관리하여 주기적으로 지연 여부 등을 점검하는 등 의료자문제도 운영 절차를 강화할 필요가 있습니다.

(11) 금전사고 방지를 위한 보험금 지급 절차 관리 강화 필요

보험회사는 보험수익자가 아닌 제3자의 계좌로 보험금을 지급(이하 '제3자 보험금 지급')하는 경우 위임서류를 확인하고 적정성을 점검하는 체계를 마련하는 등 금전사고 방지를 위한 내부통제 절차를 충실히 갖춰야 한다.

이에 따라, 회사는 보험금 청구시 고객 안내, 위임 관련 서류 접수 및 확인, 관리자 확인 및 점검 등 기본적 통제 절차는 수립·실시하고 있다.

다만, 자동차보험 및 일반보험 보상부서의 경우 장기보험 보상부서에 비해 제3자 보험금 지급 관련 금액별 실무 담당자 전결 처리 권한이 높게 설정되어 있었다.

또한, 금전사고 방지를 위해 장기보험 및 일반보험 보상부서는 결재 상신과 결재 처리가 동일한 PC IP에서 이루어지지 않도록 전산으로 통제하고 있으나 자동차보험 보상부서는 이러한 통제가 이루어지지 않아 상호 점검을 통한 업무처리가 미흡하였다.

한편, 자동차보험 및 일반보험 보상부서는 제3자 보험금 지급 건에 대한 사후점검을 실시하고 있으나 일정 금액 초과건 등으로 점검 대상이 한정되어 있었고, 일반보험 보상부서는 사후 점검기준을 명확하게 수립·운영하지 않았다.

<조치할 사항>

따라서 회사는 금융사고 예방을 위해 제3자 보험금 지급 관련 담당자 확인 및 관리자 승인 절차를 보완하고, 전산시스템 정비, 사후 점검 확대를 추진할 필요가 있으며, 이에 대한 확인·점검 절차 등에 대한 구체적 기준을 수립하여 운영하는 등 금전사고 방지를 위한 내부통제 절차를 강화할 필요가 있습니다.

(12) 책임준비금 산출 및 검증 업무 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, 2023년 상반기 책임준비금 산출 과정에서 다음과 같이 미흡한 점이 있었다.

㉮ 최선추정부채(BEL) 산출에 관한 사항

상품개발비, 교육훈련비와 같이 보험계약 포트폴리오에 직접 귀속시킬 수 없는 원가와 관련된 현금흐름은 이행현금흐름에 포함하지 않는 것이 타당하나, 회사는 2023년 상반기 상품개발부서의 급여 등 상품개발비 △△억원, 보험계약 판매에 직접 귀속되지 않는 채용 관련 광고비 등 광고선전비 □억원, 영업부서 명패비 등 교육훈련비 ■■억원 등 ▨▨억원을 최선추정부채(BEL)에 포함하여 산출하였다.

또한, 무·저해지환급금 보험은 보험료 납입기간 중에는 환급금이 없거나 적고, 보험료 납입 완료 후 환급금이 크게 증가하므로 보험료 납입기간 중 해약률을 표준형 보험보다 낮게 설정하는 것이 합리적인 계약자 행동 가정에 부합하나, 회사는 종합보험, 세만기 보험 등의 경우 무·저해지환급금 보험의 납입기간 중 해약률을 표준형 보험보다 높게 설정하여 최선추정부채(BEL)를 산출하였다.

그리고 Ⓐ보험상품 등 총 187건의 계약변경 보험계약에 대한 최선추정부채 산출 과정에서 갱신종료기간, 보험종료연령 등에 대한 프로그램 입력 오류 등이 발생한 사례가 확인되었다.

㉯ 위험조정(RA) 산출에 관한 사항

위험조정(RA) 산출시 해지위험액은 해지율 가정에 해지 충격 수준만큼 할증하여 계산하여야 하나, 회사는 Ⓑ보험상품 등 총 465종 갱신형 보험상품의 위험조정(RA)을 적립하면서 갱신시점의 해지율 가정에 해지 충격 수준을 할증하지 않은 사실이 있다.

㉰ 보험계약마진(CSM) 산출에 관한 사항

한국채택국제회계기준 제1117호 적용 관련 소급기간 이전에 발행된 보험계약의 보험계약마진(CSM)은 '현행추정부채'와 '위험마진'의 합계에서 이행현금흐름을 제외한 값으로 산출되고, 이 때 '위험마진'은 각 연도말(t) 시점의 요구자본을 (t+1)시점의 할인율로 (t+1)기간 할인하는 방식으로 산출되어야 하나, 회사는 회계 전환일(2022.1.1.)의 위험마진 산출시 각 연도말(t) 시점의 요구자본을 (t+1)이 아닌 t시점의 할인율로 t기간만 할인한 사실이 있다.

또한, 회사는 보험계약마진(CSM) 상각률을 산출하면서 '(유)금리연동형 연금' 보험계약 포트폴리오에 포함된 Ⓒ보험상품 등 2000년 전후 판매한 연금상품(4종)에 대하여 특약의 '미래제공 보장단위'를 고려하지 않고 주계약의 '미래제공 보장단위'로 계산하였고, 투자서비스의 보장단위 계산시 '계약자 적립액'이 아닌 '계약자 적립액에 예정이율을 곱한 값'을 적용하여 상각률을 산출한 사실이 있다.

<조치할 사항>

따라서 회사는 최선추정부채(BEL) 산출시 보험계약 포트폴리오에 직접 귀속시킬 수 없는 사업비 등은 이행현금흐름이 아닌 당기손익으로 인식하고, 무·저해지환급금 보험의 납입기간 중 해약률을 표준형보다 높지 않게 설정하며, 계약변경시 발생한 오류를 수정하는 한편, 위험조정(RA) 산출시 갱신형 상품의 해지 충격 수준을 할증하여 반영하고, 공정가치법 보험계약마진(CSM) 산출시 요구자본 할인율과 일부 연금상품의 상각률을 합리적으로 산출하는 등 한국채택국제회계기준 등에 부합하도록 책임준비금 산출 및 검증 업무를 강화할 필요가 있습니다.

(13) 손절매 실시 기준 및 사후 관리 강화 필요

회사는 내규 「리스크관리규정」, 「금융투자상품세부운용지침」에 평가손율이 일정 기준을 초과할 경우 다음 거래일 이내 반대매매를 실시하는 것을 원칙으로 하고, 유동성 부족, 시장위기상황 등으로 매각이 어려운 예외적인 경우에는 3영업일 이내에 투융자심의위원회 및 리스크관리실무위원회의 승인을 통해 매각을 유예할 수 있도록 정하고 있다.

그러나 회사는 2019. 7. 13. 이후 손절매 대상이 된 자산 전건(17건)에 대하여 손절매를 실시하지 않고 매각을 유예하였으며, 이 중 7건은 내규상 정한 3영업일을 초과하여 투융자심의위원회 승인 절차를 거친 사실이 있다. 이에 따라 내규상 손절매 원칙 기준이 제대로 적용되지 아니하고 예외 사유에 대한 구체적 판단 기준 부재로 담당자마다 자의적으로 판단될 우려가 있다.

관련 내규에는 매각 유예 후 최초 개최하는 리스크관리위원회에 이를 보고하도록 정하고 있으나, 리스크관리위원회에 대한 보고 없이 '월간 리스크관리 현황' 자료를 통해 이메일 등으로 위원들에게 개별적으로 송부하였다.

또한, 회사 내규 「투융자심의위원회운영지침」에서 매입가 5억원 이하의 투자에 대해서는 자산운용 담당 임원의 승인으로 손절매 예외가 가능하도록 정하고 있으며 이에 대한 별도 리스크 검토 절차는 운영하지 않고 있다.

한편, 회사는 손절매 유보 이후 해당 자산의 수익률 제고 등을 위한 리스크 관리방안을 구체적으로 마련하지 않고 있다. 손절매 자산 예외 유보기간에 대하여는 구체적 근거 없이 1년, 3년, 펀드청산시점 등으로 설정하였으며, 검사기준일 현재 손절매 유예대상 자산의 수익률 대부분이 손절매 기준 이하이거나 전액 손상된 경우도 있는 등 사후관리가 미흡한 실정이다.

<조치할 사항>

따라서 회사는 손절매 예외 사유에 대한 구체적·객관적 기준을 마련하고 이에 대한 판단 근거를 관련 위원회 안건 등에 기록·관리할 필요가 있으며, 매입가 5억원 이하 자산의 손절매 예외승인에 대해서도 리스크 검토 절차를 강화하고, 손절매 관련 내규상 절차 및 기준을 준수하여 손절매 관리의 실효성을 제고할 필요가 있습니다. 또한 손절매 예외 승인시 유보 기간에 대한 근거, 수익률 제고를 위한 대책 및 리스크관리 방안을 마련하는 등 손실자산에 대한 사후관리를 강화할 필요가 있습니다.

(14) 부동산 PF 및 대체투자 한도 설정·관리 업무 강화

회사는 「프로젝트파이낸싱(PF) 등 업무운용지침」, 「대체투자 운용지침」에 따라 부동산 PF 및 대체투자 자산의 투자한도를 설정하고 한도 초과여부를 점검하고 있다.

회사는 2020년 1월부터 부동산 PF대출 한도를 총한도와 잔액한도로 구분하여 관리하고 있는데, 총한도에 대한 익스포져를 산정하는 경우 미인출잔액은 공사진행 일정에 따라 차주의 요청에 의해 인출될 수 있는 금액이므로 실제 인출가능한 약정액 기준으로 산정할 필요가 있으나 회사는 미인출잔액에 반영률을 곱하여 계산하였다. 또한 2023년 8월 한도 기준을 합리적 근거 없이 운용자산에서 총자산으로 변경한 사실이 있었다.

한편 회사는 대체투자 자산에 대해 상품별·투자지역별 한도를 리스크관리위원회 승인을 통해 설정하고 있다. 그러나 총한도와 잔액한도를 구분하여 설정하는 부동산 PF 대출과 달리 대체투자 자산에 대해서는 총한도를 별도로 설정하지 않았다. 또한 투자지역별 한도는 약정금액 기준으로 상품별 한도는 잔액 기준으로 설정하는 등 한도 설정의 일관성이 미흡하였다.

<조치할 사항>

따라서 회사는 부동산 PF대출 및 대체투자 자산의 한도 설정시 운용자산을 기준으로 하고 대체투자 자산에 대해서도 총한도를 설정·운영할 필요가 있으며, 익스포져는 실제 인출 가능한 약정액 기준으로 산정하는 등 부동산 PF대출 및 대체투자 한도 설정·관리 업무를 강화할 필요가 있습니다.

(15) 부동산 PF 및 대체투자 사후관리 강화 필요

회사는 「프로젝트파이낸싱(PF) 등 업무운용지침」, 「대체투자 운용지침」 등에 따라 투자 현황 및 경과 등에 대한 점검 업무 등을 수행하고 있으며, 투자자산의 사후관리를 위해 사업성 평가, Credit Review 및 자산건전성 분류 등을 실시하고 있다.

회사는 부동산 PF 사업성 평가 등급을 '양호', '보통', '악화우려'로 분류하고 있는데, '양호', '악화우려' 등급 평가시 적용된 계획 누계공정률, 시공사 책임준공 주체의 신용등급 등의 항목이 '보통' 등급 평가시에는 반영되지 않아 전체 등급 간 객관적 비교·평가가 어려운 실정이다.

또한, 사업성 평가 등급 분류시 예외 사항은 제한적으로 운영될 필요가 있으나, 평가등급을 상향 조정할 수 있는 7개의 평가 예외 조항을 운영하면서 일부 예외 조항을 통해서는 '악화우려'에서 '양호'등급으로 상향 조정할 수 있도록 하였고, 그 판단기준도 불명확하여 담당자에 따라 자의적으로 판단될 우려가 있었다.

회사는 Credit Review시 자체 기준에 따라 자산을 A~D등급으로 분류하고 있으나 등급 분류기준이 구체적으로 명확히 마련되어 있지 않고, 평가 근거를 별도로 관리하는 체계가 마련되어 있지 않는 등 객관성·일관성 확보가 미흡하였다.

한편, 관련 내규에 자산건전성 분류, 사업성 평가 및 Credit Review(C, D 등급)은 월별로 대상 자산에 대한 이슈를 반영하도록 하고 있으나, 1개월 지연하여 평가한 사례가 확인되었다.

또한, Credit Review 및 자산건전성 분류 관련 사후관리 보고서 작성시 부서별·담당자별로 작성 양식 및 항목 등을 상이하게 기재하는 등 사후관리 업무의 일관성이 미흡한 측면이 있었다.

그리고 Credit Review 및 사업성평가 보고서에는 향후 진행상황 모니터링, 인허가 진행과정 모니터링 예정, 공정률 모니터링 실시 등으로 기재하였으나, 실제 점검 내용, 이행 여부 등을 관리하지 않아 이를 확인할 수 없었다.

<조치할 사항>

따라서 회사는 사업성 평가 및 Credit Review 등과 관련하여 등급별 평가항목, 평가기준 등을 구체적으로 명확히 마련하고 등급평가 예외 조항을 재검토하고 평가·산출 근거를 기록·관리하는 등 관련 업무의 객관성·합리성을 제고할 필요가 있습니다. 또한 관련 내규에 따라 대상자산의 이슈를 적시에 파악·검토하고 사후관리 보고서 작성시 기재 항목·내용 등의 일관성을 확보하는 한편, 사후 모니터링 내용에 대한 점검 및 확인 절차를 정비하는 등 부동산 PF 및 대체투자 관련 사후관리 업무를 강화할 필요가 있습니다.

(16) 부동산 PF 수수료 집행 관련 적정성 점검 강화 필요

회사는 초과수익 창출, 신규 투자자금 확보 등을 위해 기존에 투자한 부동산 PF대출을 만기 이전에 매도(이하 '셀다운')하는 과정에서 자문·중개·주선 등의 명목으로 각종 수수료를 지급하고 있다.

그러나 회사는 셀다운 수수료 산정 등에 대한 기준 및 절차를 마련하지 않았고 감사·준법·인사총무·리스크관리 등 유관부서의 사전검토 및 통제 절차 없이 셀다운 업무에 대한 의사결정 및 수수료 산정 등의 업무를 투자금융부 단독으로 처리하고 있었다.

이에 따라, 검사대상기간 중 59건의 셀다운 수수료 지급률(수수료지급액/셀다운 약정금액)이 ◉.◉◉%~◈.◈◈%로 편차가 크게 나타났는데도 이에 대한 적정성 점검 및 확인이 제대로 이루어지지 않았고, 셀다운 관련 수수료지급 대상 업체의 실제 업무 내역 및 실적 등의 적정성을 점검할 수 있는 체계도 마련되어 있지 않았다.

<조치할 사항>

따라서 회사는 부동산 PF 셀다운 수수료 지급업무가 적정히 수행될 수 있도록 유관부서의 점검 및 확인 절차를 강화하고 셀다운 업무에 대한 사전검토 및 사후관리 철저 등 내부통제 강화 방안을 수립·시행할 필요가 있습니다.

(17) 정보시스템 감리 업무 강화

「전자금융감독규정」 제22조에 따르면 금융회사는 감리 시기, 감리 실시기준 등을 포함하여 정보시스템에 대한 감리 지침을 작성·운용해야 한다.

이에 따라, 회사는 회사 내규 「IT감리지침」을 작성·운용하고 있으며, 동 지침에서 목적, 적용범위, 대상·시기 등에 관한 사항을 정하고 있다.

회사는 검사대상기간(2019. 7. 13. ~ 2023. 11. 3.) 중 한 차례의 IT감리(퇴직연금 자산운용시스템 구축 관련)를 실시하였는데, 시스템 구축 완료 후 종료 감리만 실시한 사실 및 감리 영역을 실효성 있게 구분하지 않고 일부 영역(프로젝트 관리·시스템개발)에 대해 체크리스트 점검 수준의 감리를 실시하였다.

이에 따라, 분석·설계 단계의 부적합 사항이 발견될 경우 시정조치할 시간을 확보하지 못하거나 감리가 필요한 주요 부분에 대한 감리가 누락될 우려가 있다.

<조치할 사항>

따라서 회사는 IT감리 대상의 성격, 수행기간 등에 상응하는 감리가 적시에 실효성 있게 이루어질 수 있도록, 「IT감리지침」에 감리 시점* 및 유형 등을 명확히 규정하여 충분한 시정조치 시간을 확보하는 한편, 주요 사항에 대해 반드시 감리를 수행하도록 개선하시기 바랍니다.

* (예) 개발감리 시기 : 중간감리(설계단계종료 후), 종료감리(이행단계 전)

(18) 정보시스템 운영체제 보정업무 강화

회사는 운영 중인 정보시스템에 대해 시급한 기능개선 또는 취약점 보완 등 중요한 보정 필요사항이 발생하는 경우, 서비스 영향도 등을 파악한 후 시스템 운영에 지장을 초래하지 않는 범위 내에서 즉시 보정작업 여부를 결정하여야 한다.

하지만, 운영시스템(○,○○○대) 중 제조사 기술지원이 종료된 노후화된 장비가 ◆◆◆대(△△.△%), 2024년 상반기 중 기술지원 종료 예정 장비가 ◎◎◎대(▣▣.▣%)에 달하였으나, 시스템 교체 및 기술지원 연장계약 여부를 검토하지 않아,

기능개선 또는 취약점 보완 등을 위한 보정작업이 곤란하고, 장애 발생 시 신속한 대응이 어렵거나 해킹·악성코드 등에 의한 침해사고 발생이 우려된다.

<조치할 사항>

따라서 회사는 노후화된 정보시스템에 대한 교체 및 기술지원 연장계약 계획을 수립하고, 동 계획에 따른 소요 예상 금액을 2024년도 정보기술부문 예산(안)에 반영하는 한편,

전체 정보시스템을 대상으로 제조사 기술지원 종료 여부를 매년 점검하고, 담당 임원에 보고한 뒤 예산(안)에 반영하는 절차를 내규에 반영하시기 바랍니다.

나. 개선사항

(1) 보험사고 조사부서 성과평가지표 불합리

회사는 2020년 6월 자동차보상 부문 인력의 효율적 운영을 목적으로 자동차보상지원센터 산하에 '장기손해조사유닛' 조직을 신설하고 특정 보험사고 청구건*에 대한 조사를 담당하도록 하였다. 이에 따라 '장기손해조사유닛'은 보험사고 조사 후 그 결과를 보험금 지급 심사담당자에게 전달하고 심사담당자는 최종 보험금 지급 여부를 결정하고 있다.

* 일부 정액 담보의 보험금 반복 청구건 등

회사는 보험사고 조사과정에서 보험소비자에게 불리한 업무처리가 발생하지 않도록 조사담당자 등의 성과평가지표(KPI)를 합리적으로 마련하고 부당한 보험금 부지급 등의 유인으로 작용할 수 있는 지표는 배제할 필요가 있다.

그러나 회사는 장기손해조사유닛의 생산성을 측정하는 지표 산출시 보험계약해지 실적 등을 포함하고 있었으며, 2021년~2023년 기간 동안 '장기손해조사유닛' 부서원의 성과평가지표 중 보험계약해지 등 '계약정비' 항목*의 비중이 ◯◯%~□□%에 이르고 있어 보험사고 조사과정의 객관성과 공정성이 저해될 우려가 있었다.

* 계약 해지, 담보 삭제, 담보 가입금액 감액, 직업급수 변경, 부담보 설정 등

<조치할 사항>

따라서 회사는 보험금 지급 및 보험사고 조사과정에서 불합리한 성과평가지표로 인해 보험소비자의 권익이 침해되지 않도록 성과평가지표에서 보험계약 해지 등의 항목을 제외하고, 보험금 지급의 정확성, 신속성 등이 확보될 수 있는 지표를 포함하는 등 보험사고 조사부서의 성과평가지표를 합리적으로 개선하시기 바랍니다.

(2) 계열회사 자산운용 거래에 대한 승인 및 관리 절차 미흡

회사 이사회는 매년 차기 회계연도에서 예상되는 계열회사와의 자산운용 관련 거래에 대해 포괄적으로 사전 승인하고 있으며, 이사회는 해당 거래의 승인 시 그 목적 및 내역 등을 점검하고 거래 내용과 절차의 공정성 등을 확인할 필요가 있다.

그러나 회사는 포괄승인 한도의 사용 내역 및 현황, 구체적인 투자 내역, 포괄승인 한도 증액 시 사유 등에 대해 이사회에 충분한 정보를 제공하지 않았으며, 이사회도 별도 의견 제시나 질의 없이 이를 승인하고 있었다.

또한 담당 부서도 이사회로부터 승인받은 포괄승인 한도의 초과 여부 등에 대한 점검 체계를 갖추지 않는 등 이사회 승인 및 사후관리 절차가 미흡하게 운영된 사실이 있었다.

<조치할 사항>

따라서 회사는 계열회사 자산운용 관련 거래와 관련하여 이사회의 의사결정에 필요한 충분한 정보를 제공하고, 이사회로부터 승인받은 사항에 대해 정기적으로 자산운용 거래 내역을 점검하고 이에 대한 보고 및 관리체계를 마련하는 등 관련 업무를 개선하시기 바랍니다.

(3) 투자자산 현장 실사 및 사업성 분석 기준 불합리

회사는 내규 「대체투자 운용지침」, 「프로젝트파이낸싱 등 업무 운용지침」 등에서 투자절차를 규정하고 있으며, 회사는 이를 합리적으로 운영·관리함으로써 투자절차의 일관성과 실효성을 확보할 필요가 있다.

회사는 「대체투자 운용지침」 등에서 투자자산에 대한 실사 원칙 및 이에 대한 대체 절차 등을 정하고 있다. 그러나 실사 주체를 명확히 규정하지 않아 실사 과정에서 투자자산의 효익과 리스크를 충분히 판단하기 위해 운용부서 인력과 심사부서 인력이 함께 참여하여야 하는데도 일부 투자 건에서 운용부서의 참여 없이 심사부서 인력만 현장 실사에 참여한 사례가 있었다.

한편, 「프로젝트파이낸싱 등 업무 운용지침」에서는 “외부 전문기관의 사업성 분석 보고서가 있는 경우”, “주간사의 사업성 분석 보고서가 있는 경우” 등에는 사업성 분석·조사를 축소할 수 있도록 규정하고 있다.

다만 “브릿지론”, “각종 통계자료나 자료 등이 미흡하여 분석·조사가 어려운 경우” 등에도 사업성 분석·조사를 축소할 수 있도록 하였는데, 이 경우 부동산 PF대출 등의 수익성, 안정성 및 관련 위험 등이 충분히 파악되지 못할 우려가 있다.

<조치할 사항>

따라서 회사는 투자자산에 대한 현장 실사의 실효성이 제고될 수 있도록 운용부서와 심사부서가 함께 실사에 참여하는 방안을 검토하고, 부동산 PF대출 등에 대한 사업성 분석이 효과적으로 이루어질 수 있도록 사업성 분석 축소 사유를 정비하는 등 관련 절차 및 기준을 합리적으로 개선하시기 바랍니다.

(4) 리스크관리실무위원회 등 운영 미흡

회사는 리스크관리위원회의 효율적 의사결정을 보조하기 위해 ‘리스크관리실무위원회’를, 중요 투·융자 사안에 대한 합리적·객관적 의사결정을 위해 ‘투융자심의위원회’를 구성·운영하고 있다.

회사는 내규 「리스크관리실무위원회 운영지침」, 「투융자심의위원회 운영지침」에 따라 투자 관련 사안에 대한 심의를 하고 있으나, 다음과 같이 동 위원회의 운영에 미흡한 점이 있었다.

㉮ 리스크관리실무위원회 구성 및 운영 불합리

회사 투융자심의위원회는 자산운용실장, 자산운용기획팀장, 리스크관리팀장 등 3인으로 구성되어 있으며, 리스크관리실무위원회는 투융자심의위원회 위원 3인과 경영지원실장 등 4인으로 구성되어 있다. 또한 리스크관리실무위원회는 재적의원 2/3 이상의 출석과 출석위원 3/4 이상의 찬성을 의결요건으로 정하고 있다.

이에 따라, 투융자심의위원회 위원과 리스크관리실무위원회의 위원이 중복되고, 투융자심의위원회 소속 위원 3명이 찬성하면 리스크관리실무위원회 안건은 모두 가결될 수 밖에 없는 등 리스크관리실무위원회의 독립적 심의 기능과 견제 기능이 형해화될 우려가 있다.

또한, 내규「대체투자 운용지침」에서 투융자심의위원회 부의대상 투자건 중 총자산의 1%를 초과하는 거액 투자 사안에 대해서는 리스크관리실무위원회에서 승인하도록 정하고 있으나,

대규모(예: 총자산의 1% 초과) 부동산 PF대출 투자시 리스크파트의 심의 절차를 운영하고 있지 않다. 이에 따라 투자 위험성이 높은 사안에 대해 투융자심의위원회의 심의만으로 투자가 결정되는 등 리스크 관리가 미흡한 점이 있었다.

㉯ 자산배분전략(SAA)에 대한 리스크 관리 미흡

회사는 2015년부터 전략적 자산배분계획(SAA)*을 리스크관리위원회 부의대상에서 제외하고, 사업계획의 일부인 연간 투자계획에 자산 배분 전략을 포함하여 운영하고 있다.

* 전략적 자산배분(Strategic Asset Allocation) : 주로 보험사에서 활용하는 중장기 투자계획으로, 투자목적과 제약조건을 정한 이후 포트폴리오 최적화를 통하여 자산의 비중을 결정

그러나 자산 포트폴리오 구성 전략이 포함된 연간 투자계획을 자산운용실장 전결사항으로 정하고 있어, 자산배분전략에 대한 전사적 리스크 검토 및 관리가 충분히 이루어지지 않고 있다.

<조치할 사항>

따라서 회사는 고위험 투자자산에 대한 리스크 관리 및 심의 기능이 강화될 수 있도록 리스크관리실무위원회의 구성 및 의결 요건 정비 등 위원회의 독립성 및 전문성을 강화할 수 있는 방안을 마련하고, 부동산 PF대출 중 거액 투자건, 자산배분전략 등에 대한 리스크 관련 위원회의 심의 기능을 강화하는 등 관련 업무를 개선하시기 바랍니다.

(5) IT부서 자체감사 업무 미흡

회사 IT부서 자체감사자는 회사 내규 「IT내부감사지침」에 따라 연간감사계획을 수립해야 하나, 해당 연도에 실시할 IT부서 자체감사의 전반적인 계획은 수립하지 않은 채, 연 1회 실시하는 정기감사에 대한 계획만을 수립*하고 있으며

* 매년 11월 (연간) 정기감사 계획 보고 → 12월 정기감사 실시

정기감사 시 IT내부통제 관련 항목(6개*) 및 IT내부감사협의제도의 자율과제만을 점검하고 있어 IT전반을 살펴볼 수 있는 종합적이고 체계적인 자체감사가 이루어지고 있지 않다.

* 1. 계약관리 재무건전성 평가 및 SLA(서비스 품질수준 평가) 협약 여부, 2. 프로그램 변경 제3자 검증 실시 여부. 3. 배치실행 책임자 승인 여부, 4. 전산원장 변경 적정 여부, 5. 시스템 권한 관리 적용 여부, 6. 외주직원 권한 통제 적정 여부

<조치할 사항>

따라서 회사는 IT 부서 자체감사 계획 수립 시 업무 전반을 종합적으로 점검할 수 있도록 연도별 중점 영역을 선정하는 등 체계적으로 계획을 수립하고, IT 내부통제 항목에 대해서는 상시 점검을 병행하는 등으로 자체감사를 개선하시기 바랍니다.

(6) IT부문 내규 관리 미흡

회사는 IT부문 업무절차에 대해 내규(규정 및 지침) 및 매뉴얼을 마련*하고 제·개정시 회사 내규 「위임전결규정」에 따라 전결권자의 승인을 받고 있으며, 회사 내부업무포털(규정·예규시스템)에 이를 게시하도록 운영하고 있다.

* 규정 2종, 지침 10종, 매뉴얼 16종

하지만 개정내규 시행 이후에야 전결권자 승인을 받거나 내부업무포털에 개정 이후 게시하거나 파일을 잘못 게시하는 등의 관리가 미흡한 사례가 있다.*

* (사례) 「IT감리지침」 시행 : 2023. 1. 2., 전결권자 승인 : 2023. 1. 31., 포털 게시 : 2023. 8. 31.

또한, 현재 운용하지 않는 업무절차가 내규에서 삭제되지 않는 등 현행화되지 않았으며 내규 간 내용이 일치하지 않는 등 개정이 적절하게 이루어지지 않고 있다. 이에 따라, 임직원이 내규를 참고하며 업무를 수행하기 어려울 우려가 있다.

<조치할 사항>

따라서 회사는 IT부문 전체 내규 및 매뉴얼을 점검하여 내용을 현행화하고 내규 간 불일치 사항이 없도록 내규를 정비하시기 바랍니다.

또한, IT부문 내규의 제·개정사항 발생 시 시행 전 전결권자의 승인을 받아 내부업무 포털에 게시하고, 제·개정 절차에 지연된 사항이 없는지 주기적으로 점검하여 관리를 강화하시기 바랍니다.

(7) IT사업계획 수립 및 아웃소싱 서비스 관리 미흡

회사는 회사 내규「IT업무관리규정」에 따라 IT발전심의위원회를 설치하여 주요 정보화 추진실적 및 계획, IT부문의 주요 사업을 심의·의결하고 있다.

하지만 IT사업계획 수립 시 전년도 IT부문 사업 중 예산이 집행되지 않은 사업에 대해 원인분석 없이 동 사업의 예산을 이월하여 편성하거나 사업을 추진하지 않는 등 사후관리가 미흡하다. 이에 따라, 개발사업이 지연되는 등 주요 IT업무 수행에 차질이 발생할 우려가 있다.

회사는 전산시스템 유지보수 계약관리를 위해 외부업체와 통합 유지보수 계약을 체결하고 있다. 그리고 무상 유지보수 기간 만료 등으로 신규체결·갱신이 필요한 경우 통합 유지보수업체와 변경약정을 체결하고 있다.

하지만 변경약정 체결을 통해 신규체결·갱신한 유지보수 계약에 대해 계약 체결 일시, 서비스 명세 등을 확인하기 위한 상세 계약자료를 관리하지 않고 있다. 이에 따라, 유지보수 계약이 적절하게 체결·갱신되지 않는 경우 전산시스템 장애 발생 시 신속한 기술지원 및 조치가 이루어지지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 IT부문 사업의 추진사항에 대해 정기적으로 점검하고 정보화 계획 수립 시 IT발전심의위원회에서 미착수 사업의 사유 및 재추진 여부를 포함하여 심의하는 등 관련 절차를 강화하고, 앞으로 통합 유지보수업체와 변경약정 체결 시 통합 유지보수 업체와 실제 기술지원 수행업체 간의 계약 증빙서류를 제출하도록 계약서에 의무조항을 반영하는 등 관련 절차를 강화하시기 바랍니다.

(8) IT업무 연속성 확보대책 미흡

회사는 회사 내규 「IT비상대책지침」에 따라 재해복구계획서(DRP)를 마련하고 재해복구 모의훈련을 연 2회 실시하는 등 업무지속성 확보방안을 수립·운용하고 있다.

하지만 재해복구계획서 중 일부 내용*은 실무와 상이한 부분이 있고 재해복구계획서 개정 시 전결권자(부서장)의 승인을 받지 않고 있다.

* 재해복구시스템 복구 매뉴얼, 재해복구 Application 점검표 등

또한, 재해복구 모의훈련 시 현업 또는 IT부서 담당자가 참여하지 않고 업무검증을 수행한 사례가 확인되는데, 훈련이 형식적으로 수행되어 비상 상황 발생 시 전자금융 업무의 연속성이 저해될 우려가 있다.

<조치할 사항>

따라서 회사는 정기적으로 재해복구계획서 전반을 점검하여 실무와 일치하도록 수정하고 개정 시 전결권자의 승인을 받는 등 관리 절차를 마련하시기 바랍니다.

또한, 업무별 현업 및 IT부서 담당자가 연 1회 이상 재해복구 모의훈련에 참여하여 업무검증을 수행하도록 하는 등 실효성을 강화하시기 바랍니다.

(9) 정보시스템 유지보수 산출물 관리 미흡

회사 내규 「응용시스템개발지침」에 따르면, 회사는 개발 요청사항을 반영한 사용자 요구 정의 명세서를 작성·검토해야 하며 단위·통합·시스템·인수 테스트를 실시하고 테스트 산출물을 기록 및 관리하여야 한다.

현업부서의 전산처리의뢰서 작성 시, ITSM(IT서비스관리시스템)에 테스트 시나리오 및 결과를 필수 입력 항목으로 정하고 있어 관련 산출물은 모두 작성되고 있으나,

첨부파일 형태로 입력할 수 있도록 구성한 '요구사항 정의서'는 작성률이 54.9%(검사대상기간 중 전산의뢰 6,657건 중 3,654건)에 그치고 있으며, 화면 설계서, 프로그램 설명서, 인터페이스 정의서, 배치흐름도 등은 작성하지 않고 있는 등 정보시스템 유지보수 산출물 작성·관리가 미흡하다.

<조치할 사항>

따라서 회사는 정보시스템 유지보수 유형에 따라 필수적으로 작성해야 할 산출물을 정하여 이를 회사 내규 및 ITSM에 반영하는 등 정보시스템 유지보수 산출물 관리를 강화하시기 바랍니다.

(10) IT장애 관리 불합리

회사 내규 「정보시스템운영관리지침」에 따르면, 장애관리담당자는 IT장애발생 시 장애복구내용 및 향후대책을 포함하여 장애관리 책임자에게 보고하고 승인받아야 하나,

검사대상기간 중 총 70건의 IT장애가 발생하였는데도 장애보고서만 작성한 채 장애관리 책임자의 승인*을 받지 않았다.

* 전건(70건) 구두 보고

또한, 작성된 장애보고서는 장애 원인 분석, 장애 등급 산정, 향후 추진계획 확인 등 필수 항목이 누락되어 있으며, 담당자의 실수에 의한 IT장애도 다수 발생하고 있다.

<조치할 사항>

따라서 회사는 IT장애 발생 시 장애보고서 작성 후 책임자 승인을 받는 절차를 마련하고, 승인 과정에서 장애보고서 항목 누락 여부, 인적 장애 여부 등을 확인하는 절차를 마련·운용하시기 바랍니다.

(11) 전산원장과 회계원장 대사 업무 미흡

회사는 「전자금융감독규정」 제27조 제3항, 제4항에 따른 전산원장 대사 작업을 수행하기 위해 2014. 2. 24. A회계법인과 '전산원장 계정대사 시스템 구축' 계약을 체결하고, 정기대사* 및 소급대사** 수행을 위한 시스템 구축을 완료하였다.

* 정기대사 : 월마감 시에 실시하는 전산원장과 회계원장의 비교·검증 작업
** 소급대사 : 정기대사시 확인되지 않은 장애·오류 건 등을 사후적으로 확인·반영하기 위한 대사

회사는 검사대상기간(2019. 7. 13. ~ 2023. 11. 3.) 동안 동 시스템을 통해 매월 정기대사 작업은 정상적으로 실시하였으나, 소급대사 작업은 실시한 이력이 없다.

<조치할 사항>

따라서 회사는 소급대사 주기 및 범위 등을 정하고 이에 따라 소급대사 작업을 수행하여 대사작업의 정확성을 제고하시기 바랍니다.

(12) 정보처리시스템 성능관리 미흡

회사는 회사 내규 「정보처리시스템운영기준」 및 「IT용량관리기준」에 따라 CPU, 메모리, 디스크 등에 대한 적정 임계치를 설정하고 성능점검을 주기적으로 수행한 후 사용량 추이를 보고하는 한편, 용량 관리 모니터링·분석을 주기적으로 실시하여 성능 부족으로 인한 사고를 미연에 방지하여야 한다.

하지만 전산자원별 적정 임계치가 설정되지 않은 상태로 정보시스템을 운영하여 검사대상기간 중 전산자원의 최대 처리용량 초과 등의 성능 부족으로 인한 장애가 다수 발생하였고,

전체 성능관리 대상 서버 중 일부에 대해서만 모니터링을 실시*하는 등 정보시스템 용량관리에 대한 분석이 적정하게 이루어지지 않고 있다.

* 기간계 10대(기간계 서버 중 10.5%), 채널계 10대(2.2%), 정보계 11대(19.3%) 등 저조한 수준

<조치할 사항>

따라서 회사는 보험 코어 업무를 담당하거나 모니터링이 필요한 서버를 모니터링 대상으로 추가 선정하고 전산자원별 적정 임계치를 설정하는 한편, 용량부족 시 긴급 용량증설 절차를 마련하여 안정적인 성능관리를 수행하시기 바랍니다.

(13) 인터넷 주소(IP) 관리 대책 미흡

회사 내규 「정보시스템 운영기준」 및 「정보보안관리지침」에 따르면, 회사는 인터넷 주소(이하 'IP주소')는 내부/외부 직원, 운영/개발 등 업무 특성별로 네트워크를 적절하게 분리하여 사용하여야 한다.

그러나 정보계, 채널계 전체 서버 중 일부*는 운영 및 개발 서버의 IP 대역이 혼재되어 있어, 악성코드 감염이나 보안 취약점으로 인한 보안사고 발생시 개발 서버의 피해가 운영 서버로 확산될 위험이 있다.

* 전체 서버 535대 중 20대(3.7%)(정보계 자산운용 시스템, 신지급여력제도 시스템 등)

<조치할 사항>

따라서 회사는 운영 서버 대역에 할당된 개발 서버에 대해서 IP변경을 완료하고, 네트워크 주소관리 대책에 대하여 주기적인 점검이 이루어질 수 있도록 관련 절차를 내규에 반영하여 운영하시기 바랍니다.

(14) 정보시스템 보호대책 운용 미흡

㉮ 회사는 데이터베이스(DB)에 대한 접근권한 통제 및 명령어 수행 이력을 관리하기 위해 데이터베이스 접근통제 솔루션을 운영하고, 데이터베이스 접근권한은 현업 및 IT 부서장 승인 후 부여하고 있다.

하지만 비상용콜센터 등 일부 운영 데이터베이스는 업무담당자에게도 접근권한을 부여하고 있음에도 전산자료 조회내역에 대한 적정성을 점검하지 않고 있다. 그 결과, 업무담당자 착오 등으로 시스템 정상 가동에 영향을 미치거나 업무목적 외 중요정보를 과다 조회할 우려가 있다.

<조치할 사항>

따라서 회사는 임직원에게 부여된 데이터베이스 접근권한을 점검하여 불필요한 권한을 회수하고, 업무 목적상 운영 데이터베이스에 접근권한을 요청한 부서장은 업무목적 외에 정보조회 등을 주기적으로 점검하여 정보보호최고책임자에게 전달하는 절차를 마련하는 한편,

업무담당자 착오 등으로 운영 데이터베이스의 정상 가동에 영향을 미치지 않도록 2024년도 정보기술부문 예산(안)에 테스트 또는 검증용 데이터베이스 도입 비용을 반영하여 테스트·개발 환경을 구축하시기 바랍니다.

㉯ 회사 내규「정보보안관리지침」제26조에 따르면, 시스템 접속 계정을 공유하거나 도용하는 것은 금지되어 있으나, 타 부서원이 접속 계정 및 비밀번호를 보관하고 있는 사례가 확인되는 등 중요정보 무단 조회·변경과 같은 보안사고가 발생할 우려가 크다.

<조치할 사항>

따라서 회사는 계정 공유 및 도용을 방지하기 위해 임직원 보안 교육을 강화하고, 중요정보 접근 시 시스템 계정 접속에 대한 인증절차 강화방안 등을 마련하시기 바랍니다.

㈐ 회사는 이용자 비밀번호를 정보시스템에 암호화하여 저장·보관하고 있으나, 금융보안원 및 한국인터넷진흥원(KISA)에서 권고하지 않는 양방향 암호화 방식(AES, RC2)이나 안전성이 낮은 일방향 암호화 방식(SHA1)을 적용하고 있어, 해킹 등으로 이용자 비밀번호가 노출될 우려가 있다.

<조치할 사항>

따라서 회사는 양방향 암호화 방식 또는 보안 강도가 약한 일방향 암호화 방식으로 암호화된 이용자 비밀번호를 보안전문기관에서 권고하는 안전한 암호화 방식으로 수정하고, 시스템 개발 또는 도입·유지보수 시 안전한 암호화 방식이 적용될 수 있도록 암호화 방식의 적정성을 사전 검증하는 절차를 마련하시기 바랍니다.

(15) 자체 보안성심의 절차 불합리

회사는 전자금융 서비스의 신규 오픈 또는 변경이 발생하는 경우 업무담당자가 보안담당자에게 요청하여 자체 보안성 심의를 실시하고 있다.

하지만 자체 보안성 심의 대상에 포함되는 '신규 전자금융업무'의 기준 및 세부 평가항목 등이 포함된 세부 절차를 마련하지 아니함에 따라

업무담당자가 착오 등으로 자체 보안성심의를 정보보안팀으로 요청하지 않는 경우 자체 보안성심의 없이 신규 전자금융업무 서비스가 제공되거나, 인증 절차 등 보안성 확보를 위한 필수 심의항목이 누락된 채로 보안성심의가 이루어질 우려가 있다.

<조치할 사항>

따라서 회사는 자체 보안성심의가 적정하게 수행되도록 '신규 전자금융업무'의 판단기준 및 세부 평가항목을 내규에 반영하여 자체 보안성심의 업무를 수행하시기 바랍니다.

(16) 전산자료 관리방식 미흡

회사는 데이터베이스 內 금융정보는 계약 관계 종료 시 별도로 분리하여 보관한 후 업무담당자의 접근을 통제하고, 동 정보의 보유기간이 경과하거나, 계속적인 보관 등을 위해 정보 파기 및 재이용 기준을 마련하고 있다.

하지만 계약 관계가 종료된 정보에 대한 분리 보관방식이 일관되지 않고*, 정보 재이용 시 사전통지 또는 정보주체 동의서 등 관련 자료를 시스템에 등록·보관하고 있지 않아 분리 보관 및 정보 재이용에 대한 적정성 확인이 어려울 수 있다.

* 매일 금융정보를 비식별화 처리하거나, 매주 이관 후 원 정보를 삭제하는 등 일관되지 않음

<조치할 사항>

계약 관계가 종료된 정보에 대한 분리보관 방식을 일관되도록 개선하고, 정보 재이용 시 사전통지, 정보주체 동의서 등 관련 근거 자료를 시스템에 등록·보관하는 절차를 마련하는 한편, CPO(개인정보보호최고책임자)는 유관 부서(법무부서 등)와 함께 계약 관계가 종료된 정보의 분리보관, 파기, 재이용의 적정 여부에 대한 점검을 강화하시기 바랍니다.