경영유의사항 등 공개안

1. 금융기관명 : 디비손해보험㈜

2. 제재조치일 : 2025. 11. 13.

3. 제재조치내용

제재대상	제재내용
기 관	• 경영유의 6건, 개선사항 18건

4. 제재대상사실

가. 경영유의사항

(1) 물품구매 등 계약체결 업무 관리 강화 필요

디비손해보험㈜(이하 '회사')는 물품구매 등의 계약을 체결할 때 계약의 목적, 규모, 성질 등을 고려한 객관적 근거를 바탕으로 적정한 계약체결 절차·방법, 예정가격 등을 결정하고, 계약체결업무가 내규에 따라 적정하게 수행되고 있는지 관리·점검할 필요가 있다.

그러나 회사는 창립 기념품 등 8건의 구매계약을 체결하면서 객관적·구체적 근거 없이 "조잡한 물품의 납품이 우려된다"는 사유로 경쟁입찰이 아닌 수의계약을 체결*하였고,

* 총 8건(2020년 2.4억원, 2021년 1.7억원, 2022년 32.3억원, 2023년 1.1억원)

** 회사는 내규「계약실무지침」에 따라 계약체결 시 계약의 금액 및 성질에 따라 입찰계약 또는 수의계약으로 하여야 함

건물관리위탁계약 4건을 체결하면서 "갑작스러운 업체의 교체가 회사 업무수행에 불리하다."는 사유로 수의계약을 체결하였다.

또한 낙찰자 및 계약금액의 결정 기준 산정을 위해 예상 거래 규모, 과거 사례 등에 비추어 예정가격을 산정하는 것이 가능하였는데도, 단지 수의계약이라는 사유만으로 계약 105건의 예정가격을 산정하지 아니하였다.

회사는 각 부서에서 개별적으로 구매·용역계약을 진행함에 따라 전사 계약현황을 관리·유지하는 체계가 없고, 내규에 따라 계약체결 업무가 이루어지고 있는지 별도 점검하는 절차가 미흡하였다.

<조치할 사항>

따라서 회사는 경쟁입찰이 어려운 사유가 객관적으로 확인되는 경우 등에 한하여만 수의계약을 체결하고, 예외적인 경우*에만 예정가격을 산정하지 않을 수 있도록 하는 등 계약 관련 절차 및 기준을 보완할 필요가 있습니다.

* 예시) 100% 비가격평가 계약인 경우, 단가계약시 물량 추정이 불가능한 경우 등

또한, 계약체결 부서가 내규에 따른 절차 및 기준을 준수할 수 있도록 구체적 실무지침을 마련하는 등 계약체결 업무의 적정성 점검 절차를 강화하고, 전사 계약체결 현황을 관리·유지하는 체계를 마련하는 등 계약체결 업무 관련 내부통제를 강화할 필요가 있습니다.

(2) 이사회 운영 및 사외이사 역할의 실효성 강화 필요

회사는 이사회 및 이사회 내 위원회의 내부통제 감시 역할 제고와 원활한 직무수행 보장을 위해 회의 개최에 앞서 충분한 기간을 두고 이사회 등에 회의자료를 제공할 필요가 있다.

그러나 「이사회규정」등 관련 내규에서 이사회 및 이사회 내 위원회의 소집을 회의 개최 1일 전에 통보하도록 하면서, 회의자료 송부 기한은 따로 정하지 않아 이사회 등이 안건을 검토할 수 있는 충분한 시간을 부여하지 않을 우려가 있다.

한편 회사의 경우 이사회 의장이 사내이사로서, 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 회사는 검사대상기간 중 선임사외이사가 사외이사회를 소집한 사례가 없고, 이사회 의결시 사외이사가 안건에 대한 반대 의견을 제시한 사례를 찾아볼 수 없는 등 사외이사의 업무수행 실적과 역할이 미흡하였다.

<조치할 사항>

따라서 회사는 회의 개최 전 회의자료 송부 및 소집 일자 통지 등에 충분한 기간을 부여하여 이사회 등에서 안건 논의가 충실히 이루어질 수 있도록 하고, 사외이사회의 소집 절차 마련, 사무지원 체계 정비 등 사외이사 역할 강화를 위한 대책을 마련할 필요가 있습니다.

(3) 장기손해보험 인수지침 관련 내부통제 강화 필요

회사는 역선택 및 불량 계약의 유입 방지 등을 위해 계약 인수 관련 지침을 마련하고, 동 지침의 합리적인 수립·시행을 위해 전결권자의 승인, 리스크 검토, 보험사기 영향평가 등의 내부통제 절차를 마련하고 있다.

그러나 회사는 내규 「위임전결규정」에서 인수지침 수립 관련 중요사항은 실장, 일반사항은 본부장을 전결권자로 지정하여 의사결정 권한의 구분이 모호한 측면이 있고*, 인수지침 변경 시행일 이후에 사후 결재가 이루어지거나** 결재 이전에 변경된 인수지침이 사내 전산시스템에 먼저 반영된 사례가 있었다.

* 현재 회사 내부적으로 회사 전반적인 부분에 영향을 미치는 인수지침은 '중요사항'으로, 상품별 인수지침 등 일부에만 적용되는 개별 인수지침은 '일반사항'으로 구분하고 있으나 장기손해보험 계약 인수 전반에 영향을 미치는 '공통인수지침'도 전결권자가 혼재

** 2023년 인수지침 조정 품의 51건 중 31건(60.7%)이 시행일 당일 결재 및 사후 결재

또한, 회사는 「장기보험 공통인수지침」에서 계약 인수지침 제·개정시 위험관리를 위해 영업손익에 관련된 중대한 사안에 대해 보험RM파트의 리스크 검토 절차를 운영하도록 정하고 있으나, 대부분의 경우* 리스크 검토 절차 없이 인수지침 변경이 이루어지고 있었다.

* 검사대상기간 중 전체 인수지침 조정 품의 209건 중 7건만 보험RM파트의 리스크 검토 절차 실시

그리고 보험사기 영향평가를 실시하는 과정에서 장기U/W센터는 '실제 비용보다 초과 보험금 발생 우려'가 있다고 판단하였음에도 보험사기 취약 요인은 낮다고 평가한 사례*가 있었다.

* (예시) 대상포진진단비 100만 → 300만 가입금액 상향 건(평가부서 장기U/W센터, 2023.4.7.) 관련하여 보험사기 영향표에 모두 "아니오(보험사기 취약 요인이 낮음)"라고 평가하였으나, 추가 의견란에 기재한 내용을 보면 "실제 비용보다 초과 보험금 발생 우려가 있으나 경쟁 상황 등을 고려하여 적절하게 운영했으면 함"이라고 기재

또한, 회사는 영업부서의 요청에 따라 적절한 검토 없이 허혈성 심장 질환 진단비 등 일부 고손해율 담보에 대한 인수지침을 변경한 사례가 있고, 인수지침 변경에 따른 효과 등에 대한 정기적인 사후 검토 절차가 없었다.

<조치할 사항>

따라서 회사는 인수지침 수립 관련 의사결정 권한을 명확히 구분하고, 변경된 인수지침 시행시 전산시스템에 사전 결재문서를 등록하도록 하는 등의 조치를 통해 원칙적으로 사전 결재가 이루어지도록 하며 사후 결재가 불가피한 경우, 그 기준 및 절차를 구체적으로 마련하여 운영할 필요가 있습니다.

또한 보험RM파트의 리스크 검토 필요 사항에 대한 구체적인 기준을 마련하여 리스크 검토 절차가 임의로 누락되지 않도록 할 필요가 있습니다. 아울러 보험사기 영향 평가에 대한 추가 의견이 있을 경우 이에 대한 별도 검토 및 논의 결과를 보관하는 절차를 마련하고, 변경된 인수지침에 따른 영향 및 효과 등에 대한 사후 검토 방법과 절차를 구체적으로 마련하는 등 관련 업무를 강화할 필요가 있습니다.

(4) 대체투자 및 부동산PF 관련 리스크관리 강화 필요

회사는 내규「자산운용규정」에 자산운용 목표 설정, 투융자 관련 심사 및 투융자 심의위원회 설치에 대한 근거를 마련하고, 내규「유가증권 운용세칙」,「대체투자 운용세칙」등을 통해 대체투자, 부동산PF 관련 한도 관리, 투자심사, 사후관리 등 내부통제 절차를 마련하고 있다.

회사는 부동산, SOC, 실물자산 등 자산별 한도를 설정하고 투자 한도 준수 여부 등을 점검하고 있으나 브릿지론 대출, 해외 메자닌・지분투자, 해외부동산 PF 등 고위험 투자 부문을 선별하여 한도를 관리하는 절차가 없어 대내외 투자환경 급변시 적시 대응하기 곤란할 우려가 있다.

또한, 회사는 투자 심사시 주간사・운용사 제공 정보 및 글로벌 신용평가사의 데이터 등을 심사에 활용하고 있으나, 주요 부문・자산에 특화된 외부기관 보고서 등에 대한 활용이 미비하고 부동산PF, 인프라, SOC 등의 내부 신용등급을 산정하는 평가표상 가감점(100점 만점 중 10점)에 대한 판단 근거 및 기준이 마련되어 있지 않아 평가의 객관성이 저하될 우려가 있다.

그리고 회사는 투자자산에 일정 규모 이상의 손실 등 부실 징후 발생시 사후실사, 이해관계자 면담·회의 등을 실시하고 있으나, 동 자산에 대한 사후실사 결과 등 주요 관리사항을 투융자심의위원회에 보고하지 않고, 자산건전성 분류기준의 적정성을 정기적으로 점검·보완하는 절차가 마련되어 있지 않은 등 사후관리 체계가 미흡하였다.

<조치할 사항>

따라서 회사는 투자 한도 관리시 부동산 브릿지론 대출, 해외 메자닌·지분투자, 해외부동산 PF 등 고위험 부문을 선별하여 한도를 관리하는 절차를 마련하고, 투자 비중이 상승하고 있는 특정 부문에 대해서는 별도 한도를 부여하는 등 리스크 관리를 강화할 필요가 있습니다.

또한, 투자 심사시 주간사·운용사 제공 정보 외에 해당 자산에 특화된 보고서 등을 활용하고, 내부 신용등급을 산정하는 평가표의 객관성을 확보하는 방안을 마련할 필요가 있습니다.

그리고 부실 징후 발생 자산의 사후실사, 이해관계자 면담·회의 등 주요 관리사항을 투융자심의위원회 등에 보고하고, 정기적으로 자산건전성 분류 기준의 적정성을 점검·보완하는 등 사후관리 절차를 강화할 필요가 있습니다.

(5) IT 부문 감사업무 강화 필요

빅데이터, 챗봇 등 신기술 사업확대 등으로 인해 회사의 IT 사업 규모는 지속적으로 확대되어 왔다. 이에 따라 감사업무 수행 시 IT 부문 전반을 면밀히 점검하여 IT 업무의 지속성 및 안정성을 확보하여야 한다.

그러나 감사부서의 IT 감사 및 IT 부서의 자체 감사를 실시*하면서 IT 전문 감사 인력 부족으로 인해 감사 대상이 IT 업무 전반을 대상으로 균형 있게 구성되지 않고 보안·서비스 등 일부 IT 부문에 편중되어 왔다.

* 회사 내규「감사위원회 직무규정」및「IT조직 관리지침」에 따라 감사부서(감사파트) 및 IT부서(시스템기획파트·정보보호파트)에서 IT 감사업무 수행

또한, 감사실시 후 적시에 보고 및 개선 조치가 이루어져야 하나 감사종료 후 경영진 보고가 장기간 지체된 사례*가 확인되며 이는 관련 내규에 감사시기·기한 등을 규정하지 않은 것**에 기인하였다.

* IT 자체감사 종료로부터 117일 이후 경영진에 감사결과를 보고

**「IT조직관리지침」에 자체감사 주기 및 결과보고 기한 등을 규정하지 않음

한편, 감사 인력 구성 시 이해 상충 우려가 있는 IT 외주인력(Ⓐ)을 포함한 채로 운영하여 IT 감사의 실효성이 저하된 측면이 있다.

<조치할 사항>

따라서 회사는 감사 인력 구성시 IT 전문인력을 포함시켜 IT 업무 전반을 대상으로 균형 있는 감사를 실시하고 이해 상충 소지가 있는 외주인력은 제외하는 한편, 내규에 감사 결과 보고기한 등을 명확히 규정하여 감사실시 후 보고 및 개선 조치가 적시에 이뤄지도록 하시기 바랍니다.

(6) 외부연계 서비스 관리 강화 필요

회사는 보험상품 판매 및 보험계약 관리 등을 위해 금융결제원·은행·카드사 등 외부기관의 본인인증, 전자서명, 결제기능 등을 회사 시스템과 연계하여 활용(○○개사, ●●●개 서비스*)하고 있고 외부서비스에서 장애 발생시 회사 시스템까지 영향을 미칠 우려가 있어 체계적인 관리가 필요하다.

* (주요 외부연계서비스) 금융결제원 - 금융인증서, 은행 - 계좌결제, 신용카드사 - 카드결제 등

이에 회사는 외부서비스를 안정적으로 연계·이용하고 장애에 대응하기 위해 외부서비스, 회사 시스템 및 장애시 조치사항 등을 내부IT 관리시스템(ITSM*)에 등록하여 관리하고 있으나, 카카오-다이렉트 톡(온라인상품), 플랫폼 보험비교 서비스, 마이데이터(퇴직연금) 등 일부 외부연계 서비스의 등록을 누락하였다.

* ITSM(IT Service Management) : IT서비스를 효과적으로 관리하기 위한 내부IT 관리시스템

한편, 회사 시스템에 대해서는 재해·침해에 대비한 비상 대응 훈련을 정기적으로 실시하고 있으나, 훈련 범위에 외부연계 서비스를 포함하지 않았고 비상 훈련 관련 내규 「IT연속성 관리지침」에 외부연계 서비스 관련 사항을 반영하고 있지 않다.

<조치할 사항>

따라서 회사는 활용 중인 외부연계 서비스 정보를 ITSM에 누락 없이 등록하여 관리하고 비상 대응 훈련 관련 내규에 외부연계 서비스에 관한 사항을 반영하여 외부연계 서비스 재해·침해상황을 가정한 비상 대응 훈련을 실시하시기 바랍니다.

나. 개선사항

(1) 개인정보 처리 관련 내부통제 미흡

보험회사는 민감정보를 처리하는 경우 정보 주체에게 개인정보 처리 동의 거부시 불이익 및 이용 목적 등을 구체적으로 알기 쉽게 안내해야 한다.

그러나 회사는 2023.11월 계약 보험금 지급심사 목적으로 외부업체인 Ⓑ을 통해 건강보험심사평가원으로부터 민감정보인 진료 정보를 수집하면서,

민감정보 수집·이용 동의 화면에서 “이용자는 개인정보 수집 및 이용 동의를 거부할 수 있으나, 단 거부할 경우에는 서비스를 이용할 수 없습니다.”라고 안내하여, 개인정보 수집 및 이용 동의 거부시 불이익을 정보 주체에게 명확하게 알리지 않았고,

민감정보의 이용 목적에 대해 “회사*에서는 저장하지 않으며, 위탁사 ‘DB손해보험’에게 정보제공”이라고만 기재하여 정보의 이용 목적에 대하여 정보 주체에게 명확하게 알리지 아니한 사실이 있다.

* 수탁사인 Ⓑ

<조치할 사항>

따라서 회사가 민감정보를 수집·이용하는 경우, 정보 주체가 정보수집 거부시 불이익 및 민감정보 이용 목적을 구체적으로 명확히 인지할 수 있도록 민감정보 처리 관련 내부통제를 강화하는 등 관련 업무를 개선하시기 바랍니다.

(2) 상품개발심의위원회 운영 불합리

회사는 보험상품 개발 관련 업무의 의사결정 기구로서 일반손해보험·장기손해보험·자동차보험·퇴직연금에 대하여 각각 상품개발심의위원회(이하 ‘위원회’)를 두고 있다.

그러나 상품개발심의위원회 내부기준에 따르면 “상품개발심의 위원장*이 위원회 상정이 불필요하다고 판단할 경우” 위원회에 상정하지 않을 수 있어, 위원장의 주관적 판단으로 상품개발·개정·판매 관련 안건의 위원회 상정을 생략하여 보험상품에 내재된 보험리스크를 파악하지 못하거나 과소평가할 우려가 있다.

* 고객상품전략실장(장기, 자동차보험) 및 법인사업부문장(일반, 퇴직연금)

장기손해보험 상품개발심의위원회 기준의 경우 상품개발·개정안 확정에 관한 사항을 위원회 상정 대상으로 정하고 있으나, 위원회 상정이 불필요하다고 상품개발심의협의회(실무협의기구)에서 의결한 사항에 대해서는 안건에서 제외하도록 규정하고 있어

새로운 판매채널(방식)이 도입*되거나 신담보가 추가되는 상품을 개발**하면서 위원회 상정이 불필요하다고 협의회에서 의결했다는 사유로 상품개발심의위원회의 의결을 거치지 않은 사례가 있었다.

* 2021년 1월 "㉮보험"

** 2021년 10월 "㉯보험"

<조치할 사항>

따라서 회사는 상품개발심의위원회 안건 상정을 생략할 수 있는 안건의 범위 및 요건을 객관적이고 합리적으로 마련하여 각 위원회 기준에 반영하고, 새로운 상품개발 및 판매채널 도입 등 중요한 의사결정은 상품개발심의위원회의 심의를 거치도록 하는 등 관련 절차와 기준을 개선하시기 바랍니다.

(3) 소송 관리업무 불합리

보험회사는 소비자를 상대로 한 소송 남용을 방지하기 위해 소송제기 여부를 사전 심의하는 소송심의위원회를 설치하고, 그 운영기준 등을 명확히 마련함으로써 내부통제의 실효성을 제고할 필요가 있다.

그러나 회사는 내규 「소송심의위원회규정」에 "법률리스크관리 업무 담당 부서에서 착오 지급이 명백하다고 판단한 반환청구소송"의 경우 소송심의 위원회의 심의·의결 대상에서 제외할 수 있도록 하였으나, 착오 지급이 명백한 경우에 대한 구체적 판단 기준이 없어 자동차보상 지원파트, SIU지원파트 등 실무부서에서 임의로 판단하여 소를 제기할 우려*가 있다.

* 착오 지급이 명백하다고 판단하여 회사가 제기한 부당이득 반환청구 소송에서 패소한 사례 확인(광주지방법원 2024.1.25. 선고 2023나70861판결)

또한, 소멸시효 경과 여부를 실무부서에서 자체적으로 판단하고 있음에도 실무부서에 대한 채권 소멸시효 관련 교육이 이루어지고 있지 않으며,

실무부서의 자체적인 판단에 대해 본사에서 재점검할 수 있는 통제 절차도 미흡하여 소멸시효 경과 건에 대해 실무부서에서 임의로 판단하여 소를 제기할 우려*가 있다.

* 검사대상기간 중 소멸시효 경과 후 소송을 제기하였으나, 소멸시효 완성을 이유로 전부 패소한 사례 4건 및 소 취하 사례 3건

또한, 회사는 소송업무의 효율적인 수행을 위해 보험금 청구·지급 관련 소송제기 건수, 보험사기 유죄확정판결 관련 소송제기 건수, 그 경과 및 결과 등을 구분하여 체계적으로 관리할 필요가 있다.

그러나 회사 전산시스템상 진행 중인 전체 소송 현황, 종류별·쟁점별 소송 현황 등을 관리할 수 있는 기능이 없어, 소송업무 수행시 과거 유사사례를 확인하기 어렵고, 각 실무부서가 입력한 소송 현황 자료에 대해 총괄부서인 법률리스크관리파트에서 정확성을 점검할 수도 없으므로*, 소송 현황을 체계적으로 관리하지 못할 우려가 있다.

* 실무부서에서 회사 전산시스템상 '소송접수'화면을 통해 소송 현황 자료를 입력하고 있으나, 법률리스크관리파트가 이를 확인할 수 있는 권한이 없음

한편, 보험회사는 금융감독업무에 참고할 수 있도록 민사소송에서 일정 금액 이상으로 패소 확정되는 등 주요 정보 사항이 발생하는 경우 금융감독원에 보고해야 한다.

그러나 회사는 주요 정보 사항 보고 관련 절차가 미비하고, 소관 부서가 명확하지 않아* 검사대상기간 중 민사소송 패소금액 3천만원 이상인 23건에 대해 정보 사항 보고를 누락하고, 28건에 대해 최소 31일～최대 259일 후에 보고한 사실이 있다.

* 법률리스크관리파트(법률리스크 업무), 송무파트(소송업무) 간에 업무분장 체계가 다소 불명확한 측면

<조치할 사항>

따라서 회사는 부당이득 반환청구 소송 등과 관련하여 착오 지급 여부의 구체적 판단 기준을 마련하고, 소멸시효 완성 후 소가 제기되지 않도록 실무부서를 대상으로 관련 교육을 시행하며, 소멸시효 관련 실무부서의 자체적인 판단에 대하여 본사에서 재점검할 수 있도록 업무절차를 개선하시기 바랍니다.

또한 구체적 작성 기준을 마련하여 소송 현황 자료를 작성하고, 진행 중인 소송의 전체 현황, 종류별·쟁점별 소송 현황 등을 총괄부서에서 체계적으로 관리하고 각 부서의

소송 현황 자료가 정확하게 작성되었는지를 확인할 수 있도록 하는 등 소송 관리업무의 효율적 대응체계를 마련하시기 바랍니다.

또한 주요 정보 사항 발생시 지체없이 금융감독원에 보고할 수 있도록 주요 정보 사항 보고 관련 절차를 정비하고 총괄관리부서를 지정하는 등 업무절차를 개선하시기 바랍니다.

(4) 보험계약 변경사항 발생시 처리 절차 관리 미흡

보험회사는 보험계약의 소멸 및 보험료 납입 면제 등 보험계약 변경 사유가 발생한 경우, 해당 업무 처리가 정확하게 이루어지도록 내부 절차 및 기준을 체계적으로 운영할 필요가 있다.

회사는 장기보상지원파트에서 보험금 지급 처리시 보험계약 변경 사유가 확인되면 이를 장기보전파트 계약변경 시스템에 전달하고, 장기보전파트는 계약변경 시스템 등을 활용하여 계약변경, 갱신 등에 대한 업무 처리를 진행하고 있다.

이때, 회사는 계약 변경 사유가 동시에 발생하거나, 소송을 통해 보험금이 지급되는 경우 등에 대해서는 전산으로 자동처리 하지 않고 장기보전파트 담당자가 수작업으로 처리하고 있는데,

전산으로 자동 처리되지 않고 예외적으로 수작업으로 처리하는 사항에 대한 절차 및 기준 등은 별도로 마련되어 있지 않다.

<조치할 사항>

따라서 회사는 보험금 지급 사유 등의 발생시 보험계약 변경 사항에 대한 처리 방법, 사후 점검 사항 등에 대한 절차 및 기준을 구체적으로 마련하고, 기존 수작업 처리 대상 건의 자동화 처리를 검토하는 등 관련 업무를 개선하시기 바랍니다.

(5) 태아보험 안내 및 관리 절차 미흡

회사는 태아보험의 보험계약자가 가족관계등록부 등을 제출하여 피보험자(태아)의 출생을 통지하면 이에 따라 피보험자의 성별, 출생일, 출생일에 따른 태아 보장 기간 및 보험기간 등을 확정(이하 '태아등재')하고 있다.

이를 위해 회사는 출생예정일이 도래하기 15일 전까지 그 내용을 보험계약자에게 알리고, 보험계약자의 '출생통지'에 따라 태아등재가 이루어질 수 있도록 하고 있다.

그러나 보험계약자의 최신 연락처 정보 확인 곤란 등의 사유로 태아등재가 이루어지지 않은 사례가 있었고, 특히 출산예정일 이후 보험계약자와의 접촉을 통해 다른 보험계약의 체결이 이루어졌음에도 기존 태아보험의 태아등재가 이루어지지 않는 사례*도 확인되었으나 이에 대한 안내 절차는 미흡하였다.

* 2023.12.31.기준 보험계약 296건에 대한 태아등재가 이루어지지 않았고, 이 중 37건은 출산예정일 이후 다른 보험계약이 이루어진 경우에 해당

<조치할 사항>

따라서 회사는 태아보험 관련 출생통지를 하지 않은 보험계약자가 다른 보험계약을 추가 가입하고자 하는 경우 태아등재 관련 안내 사항을 전산시스템상 알림 팝업 등으로 담당자에게 주지시키고, 알림톡 등을 통한 안내시 간편 등록 절차를 적극 안내하는 등 관련 업무를 개선하시기 바랍니다.

(6) 피보험자 정보 변경에 따른 계약관리 미흡

회사는 보험기간 중 보험증권 등에 기재된 피보험자의 직업 또는 직무가 변경된 경우, 보험계약자 또는 피보험자가 기존 계약변경사항을 확인하여 회사에 청약하면 보험계약의 내용을 변경하는 절차(이하 '배서처리')를 운영하고 있다.

이에 따라 회사는 기존 보유계약의 피보험자가 신계약을 체결하면서 직업정보가 변경되는 경우, 보험설계사를 통하여 보험설계사별로 관리하고 있는 기존 보유계약을 대상으로 직업변경에 대한 배서처리를 하도록 하고 있다.

그러나 회사는 보험설계사가 관리하는 보험계약에 한하여 직업변경에 대한 배서처리를 할 수 있도록 하고, 담당 보험설계사가 관리하지 않는 보험계약에 대해서는 직업정보 변경을 위한 절차 및 기준이 미비하였다.

<조치할 사항>

따라서 회사는 피보험자의 직업 변경시 고객 확인 및 동의 등의 절차를 거쳐 회사 전체 보유계약 기준으로 직업정보를 관리·점검하는 절차를 마련하는 등 관련 업무를 개선하시기 바랍니다.

(7) 의료자문 편중 관리 미흡

보험회사는 보험금 지급 심사와 관련한 의료 자문시 특정 의료기관 또는 자문의에게 의료자문이 편중되는 것을 방지하기 위해, 의료자문 편중관리 기준을 합리적으로 수립·시행하여 보험금 지급 심사 업무의 공정성과 객관성을 제고할 필요가 있다.

회사는 내규「의료자문 운영규정」등에 따라 의료자문 편중관리 기준* 등이 포함된「의료자문 운영지침」을 마련하여 의료자문이 특정 자문의에게 편중되지 않도록 자문 건수를 관리하고 있다.

* 회사 의료자문 편중관리 기준 : (2021.8.1.~2022.8.30.) 월 10건, 연 120건
(2022.9.1.~현재) 월 20건, 연 240건

그러나 회사는「의료자문 운영지침」상 편중관리 기준 '월 건수'를 '누계 월 평균'으로 적용하여, 자문의별 의료자문 연간 관리 기준 건수의 절반 이상이 특정 월에 집중되는 현상*을 방지하지 못하였다.

* 이00(이비인후과): 101건(2021.10~12월), 이00(이비인후과): 68건(2022.3월),
김00(외과): 70건(2022.4월) 등

또한, 전산시스템도 연간 누계건수만 제어할 수 있고, 특정 기간 또는 특정 자문의에게 자문이 집중되는 경우를 사전에 통제하지 못하고 있다.

그 결과 2022.1분기 의료자문관리위원회 심의과정에서 의료자문 편중관리 기준을 초과하는 사례가 확인*되었고, 이후 심의 기준을 완화하여 건수를 상향 조정**하였음에도 여전히 이를 초과하여 의료자문을 수행한 자문의가 발생***하는 등 의료자문 편중을 적절히 통제하지 못하고 있다.

* 변00(이비인후과): 연 194건(2021년), 김00(흉부외과): 연 123건(2021년)

** 2022.2분기 위원회(2022.8.18.)에서 상향 조정: 월 10건(연 120건) → 월 20건(연 240건)

*** 김00(안과): 월 23건(2023.2분기 위원회 의사록)

<조치할 사항>

따라서 회사는 특정 자문의에 대해 의료자문이 편중되지 않도록 의료자문 관리 기준을 합리적으로 개정하고 의료자문 편중관리를 위한 전산시스템을 정비하는 등 관련 업무를 개선하시기 바랍니다.

(8) 모집조직 교육자료 등에 대한 내부통제절차 미흡

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

그러나 회사는 모집조직 교육에 사용되는 'GA소식지' 등의 자료를 준법관리 부서 등을 통한 사전 심의 절차 없이 영업부서가 필요할 때마다 수시로 제작하여 사용하고 있다.

그 결과 회사는 검사대상기간 중 모집조직의 교육담당자에게 배포하는 'GA소식지' 자료에 구체적 설명 없이 단순히 자사 상품이 우수하다는 내용이 포함된 문구 등을 기재한 사례가 있었다.

또한, 영업부서는 보험대리점 설계사에게 대량으로 문자메시지를 보낼 수 있는 시스템을 운영하고 있는데, 해당 시스템을 통해 회사의 통제 및 점검 절차 등을 거치지 않은 비공식 문자메시지를 전달하여 영업을 독려한 사실이 확인되었다.

문자 대량 발송 시스템을 통해 잘못된 정보가 전파되는 경우 등 불건전 영업행위가 조장될 우려가 있는데도 회사는 동 시스템의 메시지 보존기간을 단기(2개월)로 운영하고 있어 준법감시 부서 등의 내부통제가 적정하게 이루어질 수 없는 실정이다.

<조치할 사항>

따라서 회사는 보험모집조직 교육 목적으로 작성되는 자료 등을 사전 심의 대상에 포함하고, 사전 심의 기준 및 절차 등을 강화하며, 동 자료에 대한 작성 주체, 준수사항 등을 구체적으로 마련하시기 바랍니다. 또한, 모집조직의 불건전 영업행위를 유발할 수 있는 비공식적 문자메시지 등의 작성·배포·활용을 통제하기 위한 관리 및 점검 체계를 마련하는 등 내부통제 절차를 개선하시기 바랍니다.

(9) 모집조직 자체 제재 관련 업무 불합리

회사는 내규「불완전판매 제재 운영기준」및「불완전판매 제재 운영지침」에 따라 모집조직의 불건전 영업행위에 대한 제재기준을 운영하고 있다.

하지만 회사는 모집인의 제재 대상 평가 기간을 연 단위로 운영*하여, 장기간에 걸쳐 반복적으로 위반행위가 발생하더라도 1년 단위로만 제재 양정 수준이 결정**되는 문제가 있다.

* 평가 기간 내 2회 제재시 당월 1단계, 3회 이상 제재시 2단계 가중 제재

** 2019.1월~2023.12월 기간 중 보험설계사(3명)가 2~3개년에 걸쳐 총 8번의 제재를 받았음에도 이 중 가장 높게 적용된 제재는 설계 제재(업무정지) 5일에 불과

또한, 내규「불완전판매 제재 운영지침」에 따르면 "신계약 설계제어 이상 제재를 받은 모집인이 완전판매 과정(대면·비대면) 교육*을 수료할 경우" 설계제어 기간을 50% 감경하도록 정하고 있는데, 감경 적용 횟수 등을 제한하고 있지 않아 제재시마다 감경이 가능하며, 다수 위법행위로 인한 가중 제재 대상에 해당하더라도 교육에 의한 50% 감경을 적용하고 있다.

* 2020년 회사가 자체 제작한 온라인 교육 자료로 1시간 20분 분량이며 완전판매모니터링, 모니터링 제재, 금융소비자보호법 등 내용을 포함

또한, 해당 교육자료는 1가지 종류뿐이어서 여러 차례 수강하더라도 계속 동일한 내용으로 진행되어 그 제재의 실효성이 떨어질 우려가 있다.

<조치할 사항>

따라서 회사는 모집인 제재시 불완전판매 방지를 위한 실효성이 제고될 수 있도록, 제재 대상 평가 기간, 가중 및 감경 요건 등을 합리적으로 개편하고, 제재 관련 교육 내용의 내실화 방안을 마련하는 등 관련 업무를 개선하시기 바랍니다.

(10) 보험대리점 영업행위 등에 대한 관리 미흡

회사는 금융소비자의 권익 보호를 위해 보험대리점이 위탁업무를 수행할 때 법령을 준수하고 건전한 거래 질서를 해치는 일이 없도록 성실히 관리하여야 하고, 내규「금융소비자보호 내부통제기준」에 따라 업무 위탁 기준 등의 준수 여부를 철저히 점검·관리하여야 한다.

그러나 회사의 자회사인 법인보험대리점 Ⓒ가 2020.1월~2024.1월 기간 중 전화로 모집한 보험계약의 통화품질 모니터링 실시를 소홀히 하였는데도, 이에 대한 사후 점검을 실시하지 않는 등 보험대리점에 대한 내부통제 절차가 미흡하였다.

<조치할 사항>

따라서 회사는 보험대리점의 통화품질 모니터링 실시의 적정성을 정기적으로 점검하고, 보험대리점 영업기준 등의 준수 여부를 점검·관리할 수 있는 체계를 보완하는 등 관련 업무를 개선하시기 바랍니다.

(11) 부동산PF 사업성 평가 및 관리업무 미흡

보험회사는 부동산 PF의 특성과 위험요인을 충분히 반영하여 객관적이고 합리적인 사업성 평가를 실시하고, 사업성 부족 사업장에 대한 적정한 분류를 통해 충당금 적립 등 사후관리를 함으로써 자산운용의 건전성을 제고할 필요가 있다.

회사는 내규 「자산건전성분류기준」에 따라 매월 말 자산건전성을 분류하고, 「PF 사업성평가 및 건전성분류 가이드라인」에 따라 매분기별 사업성을 평가하여 건전성 분류에 반영하고 있으나,

PF 사업성평가에 대한 세부기준을 손해보험협회의 「부동산 프로젝트 파이낸싱 리스크관리 모범규준」에 따른 기준보다 완화하여 평가하고 있다.

* 협회는 분양률이 60% 이상인 경우, '양호'로 평가하도록 정하고 있으나, 회사는 분양률이 Exit 분양률 대비 30%p 이상 낮은 상태가 9개월 이상 지속되지 않는 경우 '양호'로 평가할 수 있도록 규정

또한, 비분양형(물류센터 등) 사업장의 경우 분양률을 지표로 하여 평가할 수 없음에도 현행 기준에 따르면 분양률 이외에 고려할 수 있는 평가지표가 부족하며, 평가기준이 구체적이지 않음에 따라 대출의 실질적 내용이 반영되지 않아 부동산 PF 대출의 사업성 평가가 미흡한 사례*가 있었다.

* (㉠) EOD 사유 발생, 매입확약 취소 가능성 등 향후 사업성 저하를 초래할 수 있는 잠재적 요인이 존재함에도 '양호' 등급 부여

(㉡) 최초 대출 조건 기준으로 연체에 해당함에도 만기 연장시 변경된 이자수취 방식 기준으로 연체여부를 판단하여 '보통' 등급 부여

<조치할 사항>

따라서 회사는 개정된 「부동산 프로젝트 파이낸싱 리스크관리 모범규준」을 참고하여 PF 사업성 평가 세부 기준을 정비하고, 향후 사업장별 실질이 반영된 등급이 부여될 수 있도록 평가 및 관리업무 절차를 개선하시기 바랍니다.

(12) 유가증권 자산건전성 분류 기준 불합리

회사는 내규 「자산건전성분류기준」에서 주식 및 수익증권에 대해 회계기준에 의한 평가금액을 취득금액과 비교하여 자산건전성 등급을 분류하고, 이때 EOD 선언, 불리한 투자조건 변경 등 이슈가 발생한 경우, 자산건전성 등급과 내부 신용등급을 감안한 자산건전성 등급 중 낮은 등급으로 분류하도록 정하고 있다.

그러나 비상장 주식 등 시장가치에 기초하지 않은 유가증권의 경우 공정가치 산정의 객관성, 시의성이 부족한 측면이 있고,

내부 신용등급의 경우 원리금 상환능력, 사업환경 등 평가표를 기준으로 50점 이상(100점 만점)시 '정상'으로 구분하고 있으나, 평가표 상 주관적 판단 요소로 작용할 수 있는 가감점(10점)에 대한 판단의 근거나 기준이 미흡하여 평가의 객관성이 떨어질 우려가 있다.

<조치할 사항>

따라서 회사는 비상장 주식 등 시장가치에 기초하지 않은 유가증권에 대한 건전성을 분류하는 경우 회사가 내부적으로 관리하는 '유지관리 자산' 및 '중점 관리 자산'의 분류 기준을 활용하고 이에 따라 건전성 분류를 재검토하는 등 관련 업무를 개선하시기 바랍니다.

(13) 부동산PF 대출 계약서 작성 불합리

회사는 부동산PF 대출과 관련한 계약 체결시 차주의 권익을 부당하게 제한하지 않도록 유의해야 한다.

하지만 회사는 차주와 부동산PF 계약을 체결하면서 대출금이 조기 상환되더라도 선급된 이자를 반환하지 않는다는 조항, 어떠한 경우에도 차주가 지급한 수수료·비용은 반환되지 않는다는 조항 등 차주에게 불리하게 적용될 수 있는 내용이 포함된 계약을 체결한 사례가 있었다.

<조치할 사항>

앞으로 회사는 부동산PF 취급시 건전한 업무 관행이 정착될 수 있도록 관련 계약서(약정서) 작성 내용, 권리·의무 조항 등에 대한 검토 및 확인 절차를 강화하는 등 관련 업무를 개선하시기 바랍니다.

(14) 오픈소스 소프트웨어 운영관리 미흡

오픈소스 소프트웨어*(이하 '오픈소스')는 인터넷에 소스코드가 공개되어 누구나 사용이 가능하나, 공개된 소스 코드의 결함으로 보안취약점 노출시 안전한 버전으로 업데이트하는 보안패치가 필요하며 사용시 라이선스 고지, 소스 코드 변경시 공개 등 사용에 따른 제약조건 위반시 분쟁이 발생**할 수 있다.

* 오픈소스 소프트웨어(Open Source Software) : 인터넷 저장소에 소프트웨어 개발시 사용한 소스코드를 공개하는 조건으로 누구나 복제, 개작 등 활용이 가능한 소프트웨어

** 국내 오픈소스 라이선스 위반에 따른 분쟁사례

① 국내 A사와 B사간 오픈소스를 개작한 가상사설망 소프트웨어 사용과 관련된 법적분쟁이 발생하였고 비영리 오픈소스재단에서 개입하면서 최종적으로 관련 소스코드를 공개

② 국내 C사는 美 D사가 개발·공개한 오픈소스를 개작하여 사용하면서 이를 공개하지 않아 소송합의금으로 약 23억을 지불

이에 회사는 운영체제(OS : Operating System), 웹서버, 웹 어플리케이션 서버(WAS : Web Application Server*)를 ◎◎◎본의 오픈소스로 사용하면서 회사 내규 「보정(patch)관리 매뉴얼」에 따라 금융보안원에서 긴급 공지한 보안취약점**에 대해 보정작업을 수행하고 있다.

* WAS(Web Application Server) : 홈페이지(웹서버)에 정보조회 등 사용자 요청에 대해 WAS 內 웹애플리케이션을 실행(요청사항을 해석)하여 필요한 데이터를 DB에서 가져오거나 계산 등 필요한 처리를 거쳐 그 결과를 사용자에게 돌려주는 기능을 수행하는 소프트웨어

** OS·WEB·WAS관련 Log4j 취약점, WEB·WAS관련 SpringShell 취약점

하지만 일부 오픈소스를 보안패치* 제공이 종료된 제품으로 사용하거나 패치를 누락한 채 사용하고 있어 조치하지 않은 취약점으로 인한 시스템 결함이 침입 경로로 악용되거나 시스템 오류·장애 시 신속한 대응이 어려울 수 있다.

* 소프트웨어에 내포된 보안취약점, 오류 결함의 수정 및 기능 개선을 위해 개발자가 제공

한편, 회사는 오픈소스가 활용된 상용소프트웨어 도입 시 회사 표준계약서*에 따라 도입제품의 지적 재산권 귀속 관계, 분쟁 발생시 책임 관계 등을 구매계약서에 규정하여 사후 분쟁에 대비하고 있다.

* 표준계약서 제13조(소유권 및 지적재산권)에 구매제품의 지적재산권의 귀속관계, 소유권, 저작권, 분쟁시 공급자 책임을 명시

하지만 상용소프트웨어로 도입되지 않은 오픈소스는 라이선스 고지 등 오픈소스 사용제약에 따른 준수사항*을 지키지 않으면 소송 등 분쟁에 휘말릴 우려가 있다.

* 오픈소스는 사용 시 저작권표시, 라이선스 고지 등을 통상적인 준수사항으로 정하고 있으며 일부 라이선스(GPL: General Public License)는 해당 오픈소스 코드를 개작하여 활용할 때 변경내용을 의무적으로 공개하도록 하고 있음

<조치할 사항>

따라서 회사는 내규 「인프라구성·변경관리지침」및 「보정관리 매뉴얼」에 오픈소스를 관리 대상으로 규정하고 ITSM에 등록·관리*하는 등 도입·설치·변경·폐기 생명주기로 관리하여 보안·기술·법적 리스크에 대비하시기 바라며

* 정보처리시스템명, 도입일, 설치일, SW명, 세부버전, 기술지원 종료여부(EoS), 개발중단여부(EoL), 라이선스 유형별 준수사항 등

사용 중인 오픈소스에 대한 보안취약점 권고사항을 재확인하여 보안위험의 경·중 및 시스템 영향도에 따라 우선순위를 정하여 보안패치를 설치하거나 상위버전으로 업그레이드 또는 제품교체 방안을 마련하여 추진하시기 바랍니다.

(15) 일괄작업 통제 절차 운영 미흡

회사는 일괄작업 수행시 전산장애를 야기하지 않도록 오류를 최소화해야 하며 사후승인에 의한 일괄작업은 불가피한 경우로 한정하여야 한다.

그런데 회사가 2019. 11. 20. ~ 2024. 3. 31. 기간 중 수행한 일괄작업(□□□,□□□건)의 ■■.■%(△△,△△△건)에서 오류가 발생하였고, 특히 동일 유형의 오류가 반복적으로 발생하였음에도 로직 수정 등 필요한 조치가 이뤄지지 않았다.

또한, 불가피한 경우에 한하여 사후승인 일괄작업을 수행하였으나, 동 기간 일괄작업이 ▲▲,▲▲▲건(目目.目%, 일 평균 皿皿.皿건)으로 다소 높게 나타났다.

<조치할 사항>

따라서 회사는 반복적인 오류의 원인이 되는 프로그램 처리 방식을 개선하고 오류건에 대한 보고·통제절차를 강화하며, 사후승인 비중을 축소하는 방안을 마련하여 일괄작업의 안전성을 높이시기 바랍니다.

(16) 프로그램 변경 통제 절차 운영 미흡

회사 내규 「위임전결규정」은 시스템 개발 및 운영 관련 작업유형을 중요도에 따라 경미·일반·중요사항으로 구분하고 있으나, 그 구체적 기준이 명확하지 않아 회사는 전산장애 등 특별한 사유가 있을 때만 수행해야 하는 긴급·사후 이행을 경미 사항으로 임의 분류하여 지나치게 자주 수행하고 있다.

또한, 회사 내규「변경관리지침(어플리케이션)」에 따르면 금전 또는 대고객에 영향이 있는 중요 변경사항은 '변경자문회의'(CAB: Change Advisory Board)의 영향도 분석 및 비용검토 등을 거쳐 수행하여야 하나,

회사는 입증자료 없이 회의내용을 형식적으로 ITSM에 기재하거나 타 회의('공통영향도 회의', '상품개정 관련 심의협의회' 등)로 갈음하고 있는 등 내규와 다르게 운영하고 있다.

<조치할 사항>

따라서 회사는 정기 이행의 예외로 수행되는 긴급·사후 이행의 대상 및 결재 절차 등을 명확히 정의하여 긴급·사후 이행의 빈도가 지나치게 높아지지 않도록 통제 절차를 강화하는 한편,

금전 또는 대고객 영향이 있는 중요 변경사항은 관련 규정에서 정한 회의체 검토 등의 프로세스를 철저히 준수하여 운영하시기 바랍니다.

(17) 데이터베이스 접근통제 관리 미흡

회사 내규「데이터베이스 보안관리 지침」에 따르면, 중요 DB에 추가·조회 등 작업시 수행기록을 유지하여야 하고 회사는 인가된 단말기에 DB 접근 제어프로그램을 설치하고 단말기의 DB 접근기록을 접근제어시스템에 남기는 방식으로 이를 준수하고 있다.

하지만 동 내규에 '중요 DB'의 범위를 정의하지 않고 있어 일부 중요 DB의 작업기록이 누락될 가능성이 있고, 접근기록을 DB 서버에 남기는 대신 접근제어시스템에 저장하고 있어 인가된 단말기가 아닌 WAS서버에서 DB로 직접 접속시 WAS서버의 DB 접근기록이 누락될 우려가 있다.

한편, 회사 내규「정보보호 관리지침」은 통신용 비밀번호를 암호화하도록 규정하고 있고 이에 따라 WAS서버 설정파일에 DB접속 비밀번호를 암호화하여 저장하고 있으나, 일부 비밀번호를 보안에 취약한 암호화방식으로 저장하여 권한 없는 자가 이를 복호화하여 DB에 무단으로 접속할 우려가 있다.

<조치할 사항>

따라서 회사는 내규 「데이터베이스 보안관리 지침」의 '중요 DB' 범위에 전자금융 관련 데이터베이스가 모두 포함되도록 명확히 규정하고 WAS서버의 DB 접근기록이 누락되지 않도록 하며* WAS 설정파일의 DB 접속 비밀번호를 안전한 방식으로 암호화 하시기 바랍니다.

* DB 서버에 접근제어시스템을 추가 설치하는 등 DB 서버의 모든 DB 접근기록이 누락되지 않도록 조치

(18) 정보처리시스템 운영체제(OS) 관리 미흡

회사는 시스템 안정성 확보를 위해 시스템 운영체제에 대한 지속적인 유지·관리 등을 통하여 장애 및 취약점에 대한 보정작업을 실시하여야 한다.

하지만 회사 전체 서버 ▨,▨▨▨대 중 ▧▧▧대(약 ▦▦%)는 기술지원이 종료된 운영체제를 사용*하고 있어 오류로 인한 시스템장애, 신규 취약점을 이용한 침해사고가 발생할 우려가 있다.

* (기술지원 종료 운영체제 예시) IBM社 AIX 6.1은 2017.4월에 제조사 기술지원이 종료

<조치할 사항>

따라서 회사는 운영체제 오류로 인한 전산장애 및 취약점을 악용한 침해사고 등이 발생하지 않도록 기술지원이 종료된 운영체제에 대한 업그레이드 또는 시스템 재구축 등을 수행하시기 바랍니다.