# 경영유의사항 등 공개안

1. 금융기관명 : ㈜케이비손해보험

2. 제재조치일 : 2023. 4. 7.

3. 제재조치내용

| 제재대상 | 제재내용 |
|---|---|
| 기 관 | • 경영유의 8건, 개선 15건 |

4. 제재대상사실

가. 경영유의사항

(1) 해외 경영소송 및 재보험거래 관리 강화 필요

㉮ 미국지점 경영소송 관리 강화

㈜케이비손해보험(이하 “회사”라고 함)은 내규「해외사업 경영가이드라인」에 따라 해외사업에 관한 중요업무에 대해 ‘글로벌위원회(Global Committee)’를 통하여 관련 사항을 점검하도록 하고 있고, 동 위원회 운영기준 상 소송 진행 중 계약금액의 상향 필요 시 적정성을 점검하도록 하고 있으나,

미국지점에서 회계법인(◇◇◇◇)과의 손해배상 청구소송 및 재보험사(○○○○)와의 특약재보험 관련 분쟁으로 인하여 소송 비용이 크게 발생한 상황에서 관련 비용의 적정성에 대한 검토 및 점검 업무가 미흡하였고,

2022.1월 글로벌위원회에 상정된 미국지점의 신규 피소 건의 법률대리인 선임 안건과 관련하여 회사내 법무파트의 계약서 검토의견 중 비용 관련 일부 의견이 미반영되었으나 동 안건에 그 사유를 포함하지 않았으며

글로벌위원회 운영의 경우 정해진 일시에 모여 회의하는 방식으로 이루어지는 것이 아니라 시스템을 통하여 위원들이 가결 여부만을 입력할 뿐 논의사항과 관련된 의사록도 문서화되어 있지 않은 등 구체적 논의과정을 확인하기 어려운 실정이므로,

글로벌위원회의 점검 대상이 되는 예상 소송 비용의 초과 기준을 명확히 하고, 관련 소송비용 검토에 대한 실질적 논의가 가능하도록 안건을 작성하며, 의사록 작성 및 관련 임원 보고 절차를 마련하는 등 글로벌위원회 운영의 실효성을 강화할 필요가 있음

**㉰ 미국지점 재보험거래 관리 절차 강화**

회사는 내규 「해외사업 경영가이드라인」에 의하면 미국지점에 대하여 「직제 및 위임전결규칙」, 「해외점포업무규칙」 등에 따라 재보험거래 관리를 수행하도록 하고 있으나,

미국지점에서 재보험사(○○○○)와의 특약재보험 계약 분쟁 관련 중재로 인하여 회수되지 않고 있는 재보험미수금 현황 등이 리스크관리위원회에 보고되는 재보험 점검결과에서 누락되는 등 재보험 내부통제 체계가 미흡하므로,

앞으로 재보험 내부통제 점검 대상에 미국지점의 재보험거래를 포함하여 정기적으로 리스크관리위원회에 보고하도록 하는 등 미국지점의 재보험 관리를 강화할 필요가 있음

**(2) 임원 성과평가기준 정비 필요**

회사는 2022년 집행임원 성과평가기준 수립 시 타본부매출기여 항목을 신설하여 일정금액 이상의 보험가입자를 소개하는 임원에 대하여 가점을 부여하는 기준을 마련하고 소비자보호총괄책임자(이하 'CCO') 등 담당 업무와 연관성이 낮은 임원에 대해서도 이를 적용하고 있으므로,

CCO 등 임원의 직무 수행 독립성을 확보하고 담당 업무와의 이해상충을 방지할 수 있도록, 임원 각자의 업무 특성에 부합하고 본연의 업무에 집중할 수 있는 성과평가기준을 마련·운용할 필요가 있음

**(3) 재보험 출재업무 관리 강화 필요**

회사는 2021.2월 ◎◎◎㈜와 체결한 재물보험에 대하여, 재보험 출재조건에 부합하지 않는다는 사실을 사전에 인지하지 못한 상태로 인수하고

2021.6월 보험가입 물건의 전손사고가 발생한 후에야 출재대상이 아님을 확인함으로써 동 계약의 보유율이 최초 보유율 결정 시 대비 ○.○%p(◇%→◇%) 증가하여 회사의 보유손해액이 ◆◆◆억원 증가한 결과를 초래하였으므로

앞으로 재보험계약의 중요 사항에 대한 담당자 교육을 강화하고, 재보험 출재오류 등이 발생하지 않도록 사전적·사후적 점검 및 관리를 강화할 필요가 있음

**(4) 재보험계약 관련 보험금 지급 조건 확인 강화 필요**

회사는 ㈜◎◎◎과 체결한 배상책임보험계약과 관련하여 2017.10월 발생한 배터리 리콜사고에 대한 보험금을 지급하면서,

약관상 재보험자의 동의 없이 보험금을 지급할 수 없도록 되어 있으나, 주요 재보험자인 ◇◇(출재비율 □□%)와 ◇◇(출재비율 □□%)의 동의가 없는 상황에서 보험금 ■억원을 피보험자에게 지급한 후, 현재까지 보험금 지급에 동의하지 않은 재보험자 몫에 해당하는 재보험금 ■억원을 회수하지 못하여 재보험금 청구소송이 진행 중이므로

앞으로 불필요한 소송 방지 및 재보험금의 원활한 회수를 위해 재보험자 동의 등 보험금 지급 조건 확인 절차를 강화할 필요가 있음

**(5) 보험상품 개발 및 판매전략에 대한 통제절차 강화 필요**

회사는 질병의 진단비, 치료비, 수술비 등에 대하여 중층보장 구조를 구축하는 상품개발 전략에 따라, 기존 담보를 질병 종류와 치료 방법 등으로 세분화하여 2022.6월말 현재 약 △△개에 이르는 특약을 개발하였고, 신규 특약의 추가를 통한 보장 강화를 강조하면서 기존 보험계약을 새로운 보험계약으로 전환시키는 판매전략(up-selling)을 추진하였으나

세분화된 특약과 관련한 충분한 통계자료가 없어 다른 통계자료에 일정한 가정을 반영하여 위험률을 산출한 사례가 있는 등 특약에 적용된 위험률이 실제 위험을 제대로 반영하지 못할 우려가 있고

세부 특약이 보장하는 질병과 치료방법 등의 특성 상 병·의원의 과잉진료, 의료기술 발달로 인한 진단 및 치료 빈도수 급증, 보험계약자의 역선택 및 보험사기 악용 가능성 등 내재된 리스크요인에 대한 사전적·실질적 통제방안 없이 상품 판매후 손해율 악화 시 보험요율 및 가입한도 조정과 같은 사후적 대책만을 수립하고 있으므로

보험상품 개발 및 판매전략 수립 시 '장기보험리스크심의회' 및 '상품심의위원회' 등을 통한 내부통제 절차를 강화하여 보험상품에 내재된 리스크 요인에 대해 사전적이고 실질적인 방지대책을 수립·시행할 필요가 있음

**(6) 보험설계사 교육자료 등에 대한 관리 강화 필요**

회사는 보험설계사 교육자료 제작 및 관리 등에 대한 내부통제체계를 별도로 마련하고 있지 않아, 해당 교육자료에 보험상품 절판 강조 등 불건전 영업행위를 유발하거나 보험계약자가 오인할 수 있는 내용이 포함된 사례가 발견되었고

보험대리점 교육담당 직원에 대하여 교육컨텐츠 운영을 성과평가 항목으로 설정하고 회사가 제작한 교육자료를 해당 직원이 임의로 편집할 수 있도록 운영하면서, 교육컨텐츠 운영 항목 평가 시 법규 준수 여부에 대하여는 검수 등을 하고 있지 않아 교육컨텐츠에 보험설계사가 모든 질병에 대하여 보험금이 지급되는 것으로 오인할 수 있는 내용 등이 포함된 사례가 발견되었으므로

보험상품의 불완전판매 방지를 위해 보험설계사 교육자료 등의 적정성에 대한 내부 점검을 강화하고, 상품부서, 소비자보호부서, 준법감시부서 등 관련 부서간 사전 전검 및 협의절차를 마련하는 등 교육자료 관리업무를 강화할 필요가 있음

**(7) 보험계약 변경 절차에 대한 안내 강화 필요**

회사는 2017.10.1.~2022.6.30. 기간 중, 기존 보험계약을 유지하면서 새로운 보장을 추가하는 방법이 가능한 경우에도 기존 보험계약을 해지하고 같은 날 동일한 보험상품을 다시 가입한 사례가 ▲▲건 존재하는 등 기존 보험계약을 유지·변경하는 경우와 해지 후 재가입하는 경우에 대한 비교 안내가 미흡하였으므로,

보험계약자가 기존 보험계약을 해지하고 다시 동일 상품에 가입하는 경우, 보험계약자에 대한 충분한 정보 제공을 통해 의사결정이 이루어질 수 있도록 보험계약 해지 및 재가입 목적 확인, 계약변경을 통한 보장담보 추가 방법에 대한 안내 절차 마련 등 관련 업무를 강화할 필요가 있음

**(8) 자산운용 기능 이관에 따른 관리 강화 필요**

**㉮ ▽▽▽▽에 대한 통제 강화 필요**

회사는 현·예금, 개인대출 및 부동산을 제외한 대부분의 자산 운용을 ▽▽▽▽에 위탁하고 있고 회사 내 관련 인력도 ▽▽▽▽(LDI부문)으로 이동하는 등 실질적인 투자 일선운용(Front Office) 기능 자체가 자산운용사에 분리, 이관된 상황으로서,

위탁사와의 관계(KB금융지주 산하 계열사) 및 인력 이동 등으로 인해, 기존 투자건의 신용위험 및 위험 징후 발생에 대해 신속하게 인지하고 대응하는데 소극적이거나 사후관리의 적시성에 문제가 발생할 소지가 있고,

특히 ▽▽▽▽이 운용하는 펀드에 투자하는 경우 펀드의 수익률 저하나 부실 발생 등에 대해 미온적으로 대처할 우려가 있으므로

회사의 자산운용 기능 이관에 따라 자산운용의 수익성, 안정성 등이 저해되지 않도록 ▽▽▽▽에 대한 사전적·사후적 통제 및 감독을 강화할 수 있는 대책을 마련하고, 회사의 자산운용 현황 및 전략 등이 ▽▽▽▽ 내 타 부서에 유출되지 않도록 이해상충 가능성을 방지하기 위한 정보교류 차단 장치(chinese wall)를 마련할 필요가 있음

**㉰ KB자산운용에 대한 평가절차 보완 필요**

회사는 매년 ▽▽▽▽의 성과를 평가하기 위하여 시장자산과 대체자산으로 평가대상을 구분하여 평가안을 마련하고 있는데

시장자산에 대한 평가안의 경우 시장과의 비교 지표를 상당 부분 반영하고 있으나, 대체자산에 대하여는 시장과의 비교 지표를 적용하지 않고 있으므로 이를 보완할 필요가 있으며

회사내 자산운용부문의 KPI에 기초하여 ▽▽▽▽에 대한 평가안을 마련하고 있어, 자산운용부문의 KPI 확정이 지연되는 경우 ▽▽▽▽ 위탁에 대한 평가안 마련 역시 지연되고 있으므로, 평가안을 조기에 확정하여 안정적 자산운용이 가능하도록 할 필요가 있음

**㉱ 자체 자산운용 역량 강화 필요**

회사의 자산운용 담당 직원들이 Front Office 부서 근무 경험이 없는 상태에서는 장기적으로 자산배분 계획 수립 또는 개별 투자안에 대한 심사 기능이 약화되거나 ▽▽▽▽의 의견에 종속될 우려가 있고

▽▽▽▽의 사후관리 등에 대한 감시기능 역시 약화될 가능성이 있으므로 자산운용 역량 약화를 방지할 대비책을 마련할 필요가 있음

## 나. 개선사항

### (1) 이사회 및 이사회내 위원회 운영 불합리

가. 회사는 내규「지배구조내부규정」에 따라 이사회 및 이사회내 위원회 운영실적의 평가를 위해 평가 주체, 방법, 절차 등을 마련하도록 정하고 있는데

이사회 및 이사회내 위원회 운영실적에 대하여 '설문조사지를 통한 자기평가'만을 100% 반영하여 평가하고 있어, 객관적인 평가절차가 미비되어 있으므로

자기평가 이외에 주관부서의 평가, 회의 참석률 등 다면적인 방식으로 공정한 평가가 이루어질 수 있도록 합리적인 기준을 마련하는 등 관련 업무를 개선하시기 바람

나. 회사는 내규「이사회규정」등에 따라 회의자료를 회의 개최일 7일전까지 위원들에게 송부하도록 하고, 긴급한 사항이 있거나 기타 부득이한 경우에는 그 기간을 단축하거나 발송을 생략할 수 있도록 규정하고 있는데

사외이사의 원활한 직무수행을 위하여 사전에 충분한 자료가 제공될 필요가 있는데도 회사 내규를 통해 회의자료 제공을 생략할 수 있는 근거를 두는 것은 불합리하므로 관련 내규를 변경(삭제)하시기 바라며,

회의자료 제공기간을 단축할 수 있는 '긴급한 사항' 또는 '기타 부득이한 경우'에 대한 기준이 불분명하여 2017.10월~2022.3월 기간 중 개최된 이사회 등 각종 위원회에서 기간을 단축하여 자료를 제공한 비중이 높고, 안건확정 지연을 이유로 회의 1~2일 전에야 자료를 제공하는 사례도 있었으므로

회의자료 제공기간 단축 사유를 명확히 하고, 회의자료 제공기간이 단축되는 경우에는 그 사유 등을 기록하여 관리하는 등 안건 송부절차를 개선하시기 바람

### (2) 선임계리사의 독립성 확보 미흡

보험회사의 선임계리사는 최적가정심의회의 위원장으로서 최적가정 검증업무를 수행하는데, 최적가정 검증업무는 보험료 산출뿐만 아니라 회사의 내재가치 산출에도 적용되고, 특히 IFRS17 시행 이후에는 계리적 가정 등이 보험부채에 직접 반영되어 회사의 손익에도 크게 영향을 미치는 등 최적가정 검증업무의 중요성이 크게 증대되었으나,

회사는 선임계리사를 경영관리부문장(CFO) 산하에 두고 있어 이해상충 소지가 발생하고 있으므로

선임계리사가 독립적 지위에서 보험계리에 관한 사항을 최종 검증할 수 있도록 선임계리사 조직에 대한 편제를 합리적으로 개선하시기 바람

### ⑶ 보험금지급 심사기준 운영 미흡

회사는 2020.5월 법원이 '초음파유도 하의 진공보조장치를 이용한 유방양성병변 절제술(맘모톰)'에 대하여 보건복지부의 신의료기술로 승인되기 전에 시행된 경우에도 보상대상이 될 수 있다고 판결하였음에도 해당 판결 내용을 심사기준에 반영하지 아니하였고,

2022.2월 40~50대 1인 가구 여성을 주요 대상으로 하는 '자궁근종 고강도하이푸 집속술(하이푸)' 전용 수술비 담보(2021.6월 담보 신설)와 관련한 보험금 지급 심사기준을 제정하면서 해당 담보의 주요 대상인 폐경기 여성을 수술 불필요 항목에 포함하였으며,

2019년 암 관련 고지사항이 없는 초간편심사보험을 출시한 이후 전이암에 대한 진단비 지급 여부가 쟁점으로 부각되었음에도 이와 관련한 심사기준을 명확히 마련하지 않고 있으므로,

보험금 지급여부 등에 영향을 미치는 법원 판결이 있거나 담보를 신설하는 경우 이를 보험금 심사기준에 적시에 명확히 반영하고, 객관적이고 합리적인 보험금 지급 업무가 수행될 수 있도록 '맘모톰', '하이푸' 수술 및 초간편심사보험 등에 대한 보험금 심사기준을 합리적으로 개선하시기 바람

### ⑷ 보험계약소멸 사유 발생에 따른 환급금 안내·지급관리 업무 미흡

회사는 계약소멸 사유가 발생한 보험계약에 대하여 환급금 지급대상인 수익자 또는 상속인 등에 대해 계약소멸 사유 발생 시점에 2~3회의 연락을 시도한 후에는 정기적으로 연락을 취하는 등 별도 관리를 하지 않고 있으므로

계약소멸에 따른 환급금 미처리 건에 대한 연락 방법 및 주기, 지급대상자에 대한 안내 이력 관리 등 환급금 관리에 관한 절차를 마련하는 등 관련 업무를 개선하시기 바람

### ⑸ 보험금 누락방지시스템 등 운영 미흡

회사는 보험금 청구 시 제출된 증빙서류의 기재내용을 기초로 보험금지급 누락을 사전에 방지하는 '보험금 누락방지시스템'과, 자동차보험의 대인 또는 자기신체사고 등의 피해자가 장기손해보험에 가입된 경우 장기보험금 청구절차가 진행될 수 있도록 하는 '자동차-장기보험 보상연계시스템'을 운영하면서

‘보험금 누락방지시스템’의 경우, 처리 담당자 퇴사로 인해 처리결과 입력이 누락되거나, 일부 담보를 추가하면서 지급사유에 해당하는 정보를 시스템과 연계시키지 않아 해당 담보가 검증대상에서 누락되는 사례가 발생하였고

‘자동차-장기보험 보상연계시스템’의 경우, 일부 건의 처리결과 입력이 누락되거나, 고객에게 안내 후 연락이 두절되었을 때 재안내를 소홀히 한 사례 등이 발생하였으므로

앞으로 보험금 누락방지시스템 등의 검증대상의 정확성, 진단정보 입력의 누락 여부 등에 대한 사후 점검을 강화하고 고객에 대한 청구 안내 절차를 보완하는 등 관련 업무를 개선하시기 바람

### (6) 간편심사보험 운영 절차 미흡

회사는 간편심사보험에 가입한 피보험자가 간편심사보험 계약일부터 3개월 이내에 일반심사보험에 가입을 희망하는 경우, 별도 인수심사를 통해 일반심사보험을 청약할 수 있는 기회를 제공하도록 하고 있으나 간편심사보험에서 전환가능한 일반심사보험 상품의 범위를 한정하고 있어,

표준체인 피보험자가 처음부터 일반심사보험을 청약하는 경우(범위의 한정이 없음)와 간편심사보험에 가입했다가 일반심사보험을 청약하는 경우(범위의 한정이 있음), 가입가능한 일반심사보험의 범위가 상이한 문제가 발생할 수 있으므로

앞으로 전환 가능한 일반심사보험 상품의 범위를 표준체가 가입 가능한 모든 일반보험상품으로 확대하고 관련 심사기준을 업무지침 및 매뉴얼 등에 반영하여 운영하는 등 관련 업무를 개선하시기 바람

### (7) 대체투자 심사업무 불합리

가. 회사는 대체투자에 대하여 신용등급을 산정할 수 있는 평가모델을 통해 내부신용등급을 산정하고 있고 내부신용등급의 최저기준을 충족하여야 하는 대상을 대출채권으로 한정하고 있으나,

프로젝트성 간접투자는 수익증권의 형태이긴 하나 실질적으로 직접 대출채권을 보유한 것과 차이가 없는데도 대출채권의 경우와 심사기준을 다르게 운용하는 것은 불합리하므로 내부신용등급 적용대상을 실질에 맞게 확대·운용하시기 바람

나. 회사의 신용평가모델(SLCRS)에 자산군별 평가모델이 마련되어 있으나, 수익증권에 대해서는 편입자산의 자산군에 적합한 모델을 이용하지 않고 일괄적으로 ‘기타구조화금융’ 모델로 평가하고 있으므로

프로젝트성 간접투자 및 편입자산이 확정된 블라인드 간접투자의 경우에도 편입자산의 실질에 부합하는 평가모델을 적용하는 방안을 마련하시기 바람

다. 내규 「투자리스크심사제도운영지침」에 의하면 심사부서는 리스크관리 전담부서가 검토한 '위험조정투자이익률 점검결과'를 포함하여 심사보고서를 작성하여야 하며, '위험조정투자이익률'이 0 미만일 경우에는 비용이 기대이익률을 초과하여 사실상 투자의 실익이 없는 것으로 볼 수 있는데

2021년 중 자산운용심의위원회를 통과한 대체투자 ◎◎건 중 ◇◇건의 '위험조정투자이익률'이 0 미만이었으나, 심사보고서에 이에 대한 별도 언급 없이 '위험조정투자이익률' 수치를 단순히 기재하는 데 그치고 있으므로, 이를 투자의사 결정에 활용하는 방안을 마련하시기 바람

라. 블라인드 펀드에 투자하는 경우 자산운용사의 적격 여부를 투자가능 여부 판단의 핵심적인 기준으로 활용하고 내부지침 및 가이드라인을 통하여 자산운용사 선정을 위한 세부 평가기준을 마련하고 있는데

자산운용사 선정을 위한 정성평가 시 내부기준상 평가등급 정의에 따라 산출한 점수보다 실제 점수를 높게 부여한 사례가 ◆건 발견되었으므로, 자산운용사 평가 시 자의성을 배제하고 정성평가 결과를 검증할 수 있는 대책을 마련하는 등 관련 업무를 개선하시기 바람

마. 2021.12.30. 투자한 '□□□□ 펀드'(운용사: ■■■■)의 경우 벤처캐피탈 투자조합에 대한 출자 형태로서 내규상 '자산운용심의회' 부의 대상에 해당하나

전략적 투자라는 이유로 심사보고서 작성이나 '자산운용심의회' 심의 등 투자의사결정 과정을 거치지 아니하고 일반 자회사 투자 등에 적용되는 '경영협의회' 의결 절차 등으로 진행한 사실이 있으므로

관련 내규에 따라 '자산운용심의회' 부의 대상이 자의적 해석으로 누락되지 않도록 관리를 강화하시기 바람

### (8) 신용감리 업무 불합리

회사는 내규 「신용리스크관리기준」에 의하여 자산리스크파트가 운용자산에 대하여 분기 1회(자산별로는 연 1회) 신용감리(Credit Review) 업무를 수행하여 '자산운용심의회' 등에 보고하고 있는데

신용감리를 수행한 자산에 대해 운용부서의 확인·보고 필요 사항을 다음 분기에 보고하도록 권고하고 있으나 관찰대상(watchlist)을 별도로 지정하거나 위험단계별로 자산을 분류하는 등의 작업은 수행하지 않고 있으므로

감리결과에 따라 위험도가 높은 자산을 별도로 분류하여, 경영진이 운용자산의 현재 신용상태 및 직전 평가 시의 비교 결과를 파악할 수 있도록 하고,

상대적으로 위험도가 높은 자산에 대하여는 현재 1년으로 되어 있는 감리주기를 단축하고, 감리결과를 자산건전성분류에 활용할 수 있도록 하는 등 관련 업무를 개선하시기 바람

### (9) 자동차보험 책임준비금 개별추산 업무 미흡

회사는 보험사고 발생 후 피보험자 등과 종결 합의가 이루어지지 않은 자동차보험계약에 대한 결산기말 책임준비금(개별추산액)을 적립하는 과정에서

'미합의 장기치료 미결건'*의 경우, 보상담당자별로 치료종결 시점을 달리 추정하여 합리적 추산액 적립이 어려운 실정이므로

* 통상의 재해자와 사고심도와 부상정도가 유사함에도 과도하게 장기간 치료를 진행하는 보상건

미합의 장기치료 미결건에 대한 피해자별 행동패턴, 잔여추산액 및 회사 표준손해액 등을 비교하여 합리적 수준에서 자동추산적립 금액을 설정하는 기준을 마련하는 등 관련 업무를 개선하시기 바람

### (10) IT부서 자체감사 범위 불합리

IT부서 내 IT자체감사인 1명(정보보호파트 소속)을 지정하여 「IT자체감사 지침」에 따라 정기감사 및 테마감사, 상시 모니터링을 실시하고 있으나

피감사 조직을 'IT전산개발 및 유지보수, 전산센터 운영 업무에 참여하고 있는 전산조직'으로 정하고 자체감사 항목을 IT부문 전반이 아닌 특정 부문 △개로 한정하여 IT부서 자체감사를 수행하고 있어 IT 업무 전반에 대한 자체감사가 이루어지지 않고 있으므로

IT자체감사 대상 조직 및 업무범위를 IT기획 및 IT경영, IT보안 등을 포함한 IT 업무 전반으로 확대하여 운영하는 등 관련 업무를 개선하시기 바람

### (11) 전산원장 변경 통제 미흡

내규 「전산원장 관리 지침」에 따라 전산원장 변경 절차를 마련하고 IT업무관리 시스템(ITSM)을 통해 DB명령어(SQL) 또는 일괄작업(batch)으로 전산원장 변경 업무를 수행하고 있으며, 전산원장 변경 시 데이터변경 검토자 및 감사파트의 정당성 확인을 거치고 변경 전후 내용은 자동기록 되도록 운영하고 있는데

일괄작업을 통해 전산원장을 변경하는 경우 별도로 전산원장 변경 작업임을 등록하고 수행하여야 하는데 현업 및 개발자의 자의적 판단에 의해 등록이 안될 경우 정당성 확인 및 변경 전후 내용 자동기록 등 통제절차가 누락될 우려가 있으며

변경전 데이터 중 NULL값이 존재하는 경우 변경전 데이터 전체가 NULL값으로 기록되는 프로그램(자동기록 함수)의 오류도 있었으므로

전산원장 변경 시 정당성 확인 및 변경 전후 내용 자동기록 등 통제절차가 빠짐없이 이루어지도록 프로세스를 추가하고 프로그램 오류도 발생하지 않도록 점검하는 등 업무절차를 개선하시기 바람

**(12) 전산시스템 일괄작업 관리 통제 미흡**

내규「일괄작업 수행 지침」에 따라 일괄작업 요청을 받은 전산담당자는 일괄작업 수행전 반드시 책임자의 승인을 받아야 하고 수행과정에서 오류가 발생하는 경우 책임자 확인을 받아야 하나

과부하를 방지하기 위해 작업을 나눠서 수행하거나 오류발생 등으로 당일에 기존 작업을 재수행하는 경우 책임자가 추가적으로 확인하는 절차를 거치지 않고 외주인력이 작업을 재수행할 수 있도록 운영하고 있으며

중요작업으로 설정되지 않은 일괄작업은 수행과정에서 오류가 발생하여도 당일 재수행하여 정상 종료되면 오류내역을 관리하지 않고 있으므로

일괄작업 재수행 시에도 책임자 승인 등 확인절차를 마련하고 일괄작업 수행과정에서 발생한 모든 오류내역을 기록·관리하고 책임자 확인을 받는 등 일괄작업 통제절차를 개선하시기 바람

**(13) 대고객 업무 관련 대외기관 재해복구용 통신회선 구축 미흡**

내규「IT비상 대응 지침」에 의하면 전산시스템 마비 등 재해 발생 시 신속한 복구를 위하여 재해복구센터를 활용한 재해복구계획을 마련하도록 정하고 있으나

회사와 방카슈랑스 업무를 수행하는 은행, 증권사 등 ▲개 대외기관과 주전산센터와 통신회선을 연결하면서 재해복구센터(죽전)와 ▽개 대외기관과의 통신회선은 연결하지 않고 있어 재해 발생 시 방카슈랑스를 통한 보험계약 체결 등의 대고객 업무가 원활하게 진행되지 않을 우려가 있으므로

방카슈랑스 업무 이용률 및 중요도 등을 고려하여 재해복구센터로 실제 전환 시 업무 연속성 확보가 가능하도록 대외기관과 재해복구센터 간 통신회선을 연결하도록 관련 업무를 개선하시기 바람

### (14) 고객정보 파일 저장 시 통제 절차 미흡

내규 「IT정보보호 관리지침」에 따라 개인(신용) 정보의 조회, 출력, 다운로드 시 유출을 최소화하도록 응용프로그램 기능을 구현하여야 하고, 기간계시스템(NAIS)에서 고객정보가 조회되는 화면(▼▼개)은 화면캡쳐 및 출력을 제한*하고 개인(신용)정보에 대해서는 마스킹 처리하고 있으나

* 업무목적상 필요한 경우 별도 승인을 거친 후 사용

업무목적상 파일 저장이 필요한지 구분하지 않고 사용기간도 설정하지 않은 채 별도의 통제절차 없이 파일 저장이 가능하도록 운영하고 있으므로

업무시스템에서 고객정보 조회화면을 파일로 저장하는 것을 제한하고 업무 목적 상 필요한 경우에 한해서만 최소한으로 사용토록 통제하는 등 업무를 개선하시기 바람

### (15) 전자금융기반시설 및 홈페이지의 취약점 분석·평가 수행 절차 미흡

내규 「IT인프라 보안지침」 등에 따라 자체 평가반(외주 포함)을 구성하여 전자금융기반시설(연 1회) 및 홈페이지(반기 1회)에 대해 취약점 분석·평가를 수행하고 있는데

취약점 분석·평가 대상을 2019년도 ○○○개에서 2020년도 ●●●개 및 2021년도 ◎◎◎개로 대폭 축소하였으나 2020년도에는 취약점 분석·평가 대상 및 범위에 대한 검토가 이루어지지 않아서

평가대상에서 제외된 홈페이지 중 3개(통합구매, 대고객 안내, 보상대고객)에서 취약점을 이용한 해킹시도가 발생할 경우 동일한 네트워크 구간에 구축되어있는 전자금융업무 관련 홈페이지(대표홈페이지, 다이렉트, 퇴직연금 등)에 영향을 미칠 우려가 있고

발견된 취약점에 대해서는 위험도(Risk*) 및 위험수용수준(DOA**)을 고려하여 조치계획을 수립하고 있는데, 위험도는 자산등급, 취약점, 위협 등을 고려하여 적정한 기준에 따라 산정하고 있으나 위험수용수준(DOA)은 적정한 산정기준 없이 담당 부서에서 임의로 결정하고 있어 취약점 조치를 회피하기 위한 수단으로 악용될 우려가 있으므로

* 위험도(Risk) : 자산에 영향을 미칠 것으로 예상하는 피해 정도

** 위험수용수준(Degree of Acceptance) : 위험도가 DOA보다 낮을 경우 해당 취약점이 미치는 영향이 경미하다고 판단하여 위험수용으로 처리하기 위한 기준

취약점 분석·평가 대상 및 범위를 선정하기 위한 기준을 마련하고 평가대상에서 제외할 경우 사유를 확인하고 위험수용수준(DOA) 산정을 위한 객관적인 판단 기준을 마련하는 등 업무를 개선하시기 바람