경영유의사항 등 공개안

1. 금융회사명 : 코리안리재보험주식회사

2. 제재조치일 : 2024. 3. 18.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의 8건, 개선 13건

4. 제재대상사실

가. 경영유의사항

(1) 이사회 역할 및 운영방식의 실효성 강화 필요

(가) 이사회 의장 선임시 적격성 검증 절차 강화 필요

사외이사 중심의 이사회를 통해 경영진 견제 기능을 제고하고 이사회의 독립성을 확보하기 위하여 이사회 의장은 사외이사 중에서 선임하는 것이 바람직하고, 예외적으로 사내이사를 이사회 의장으로 선임하는 경우 적격성 여부 등에 대하여 충분한 논의를 거쳐 투명하게 선임 절차를 운영할 필요가 있으나,

2021.3월 보험업 및 경영경력이 없는 대표이사의 특수관계인을 회장(사내이사) 및 이사회 의장으로서 선임하면서, 그 선임 사유, 이사회의 책임과 역할을 고려한 적격성 여부 등에 대한 검증 절차가 미흡하였으므로,

앞으로 이사회의 역할과 독립성이 제고될 수 있도록 사외이사가 아닌 자를 이사회 의장으로 선임하는 경우 그 선임의 적정성 등에 대한 객관적 검증 절차를 강화할 필요가 있음

(나) 선임사외이사 등 사외이사의 역할 강화 필요

이사회 구성원 7명 중 3명이 대주주이고 이사회 의장을 대주주 겸 대표이사의 특수관계인으로 선임하고 있어, 사외이사들의 효율적인 경영진 견제기능을 제고하기 위한 선임사외이사의 책임과 역할이 요구되고 있으나,

검사대상기간 중 선임사외이사가 사외이사회의를 소집한 사례가 전혀 없으며, 특히 자기주식 취득과 관련하여 자본조달정책의 일관성여부, 자기주식 취득으로 인한 대주주와 회사간 이해상충여부 등에 대해 사외이사회의에서 논의가 이루어지지 않는 등 선임사외이사의 업무수행 실적이 미흡한 실정이므로,

사외이사회의 소집절차 마련 등 사외이사의 역할과 효율적 업무수행을 제고하기 위한 대책을 마련할 필요가 있음

(다) 이사회 및 이사회내 위원회 운영방식의 실효성 강화 필요

이사회는 회사의 중요사항에 대한 심도있는 검토를 통해 경영진에 대한 효과적인 감독 역할과 책임을 강화하고, 이사회내 위원회의 실효성 있는 운영을 통해 전문성과 효율성을 제고할 필요가 있으나,

회사는 이사회 및 이사회내 위원회를 1~2일에 걸쳐 집중 개최하고 있고, 회의 개최 1일 전까지 회의자료를 통지할 수 있도록 내규 「이사회규정」에 규정하고 있으며, 2020.1월~8월 기간 중 5차례에 걸쳐 자기주식 취득 의결 안건을 상정하면서 담당부서가 검토한 문제점 등을 회의자료에 포함하여 제공하지 않은 사례가 있었으므로,

앞으로 안건의 중요도에 따라 회의개최 시기, 회의자료 배포시기 등을 달리 운영하고, 각 안건별 장·단점 등에 대한 충분한 정보제공이 이루어질 수 있도록 하는 등 이사회 및 이사회내 위원회 운영절차를 실효성 있게 정비할 필요가 있음

(2) 리스크관리 조직체계 및 리스크 사전점검 기능 강화 필요

(가) 리스크관리 조직체계 정비 필요

회사는 리스크 관련 주요 의사결정을 결정을 위해 리스크관리위원회를 설치하고 리스크관리위원회의의 업무보좌 및 실무사항 논의를 위해 리스크관리전문위원회, 투자심의위원회를 운영하고 있으나,

리스크관리위원회는 위원수가 2명에 불과하여 결원 발생시 위원회가 정상적으로 개최되기 어렵고

리스크관리전문위원회는 구성원의 △△%(2023.6월말 현재 총 OO명 중 □□명)가 영업관련 위원으로 구성되어 있어 리스크관리 관련 의사결정이 영업부서와 독립적으로 이루어지기 어려운 상황이므로,

회사는 리스크관리위원회 및 리스크관리전문위원회 등의 의사결정 기능의 실효성을 제고하고, 영업 과정에서 발생할 수 있는 제반 위험에 대한 견제 기능 강화 등 리스크관리 목적에 충실히 부합될 수 있도록, 리스크관리위원회 및 관련 조직체계에 대한 정비 방안을 마련할 필요가 있음

(나) 리스크 사전점검 기능 강화 필요

회사는 내규「리스크관리규정」등에서 신상품 개발 및 이에 대한 재보험계약 인수 등 잠재적 리스크가 크다고 판단될 경우 거래체결 및 업무수행 전에 리스크관리팀으로부터 주요 리스크에 대한 사전점검을 받도록 규정하고 있으나,

사전점검을 위해 필요한 세부 종목별, 위험별 체크리스트를 체계적으로 마련하지 않고 각 담당자마다 표준화되지 않은 방식으로 점검을 실시하고 있어 담당자의 역량 및 전문성에 따라 점검 내용 수준의 편차가 크게 발생할 수 있고,

또한, 사전점검 결과에 따른 조치방안 마련 등 리스크관리팀 의견에 대한 영업부서 등 업무부서의 검토 및 반영 절차가 마련되어 있지 않고 사후적으로 이행 결과를 점검하는 별도 절차도 없어 리스크 사전점검 기능의 실효성이 부족할 수 있으므로,

회사는 리스크 사전점검이 체계적이고 실효성있게 운영될 수 있도록 점검 항목 등을 구체적으로 마련하고, 이에 대한 조치방안 및 점검절차 마련 등 리스크 사전점검 결과에 대한 사후관리를 강화할 필요가 있음

(3) IFRS9, IFRS17 등 신회계제도 시행에 따른 관련 내부통제 체계화 필요

2023.1월 IFRS9, IFRS17 등 신회계제도 시행에 따라 회사는 기대신용손실모형을 통하여 운용자산 관련 대손충당금을 평가·적립하고, 계리적 가정 산출 등을 통해 보험계약부채를 평가·적립하기 위한 체계적인 검증 절차 및 기준 등을 운용하여 하나,

회사는 보험계약부채 평가시 계리적 가정에 대한 별도 검증절차를 구체적으로 마련하지 않았고, IFRS9 제도 시행에 따라 대손충당금 적립기준을 변경하고 IFRS17 제도 시행에 따라 발생사고부채 추정방식을 변경하였으나, 변경 기준 등에 대한 내규반영이 미흡한 실정이므로,

보험계약부채 평가시 계리적 가정 관련 기초통계, 산출방법·결과 등에 대한 검증체계를 강화하고, 대손충당금 적립기준, 발생사고부채 추정방식 및 검증기준 등 제도 변경에 따른 명확한 절차 및 기준을 마련하여 운용하는 등 신회계제도 시행에 따른 내부통제 체계를 강화할 필요가 있음

(4) 재보험자 협의요율 산출 기준 및 관리 절차 강화 필요

재산종합보험의 보험요율 산출식을 구성하는 '기본요율'에 대해 개별업종(일반 업종 ◑◑개) 별로 보험사고 발생률(위험률) 등을 고려하여 산출하지 않고 보장대상 건물의 용도(Occupancy)를 기준으로 분류한 ◒◒개 업종군별로 '단일요율(업종군 요율)'을 산출하였으나,

단일요율을 적용하는 동일 업종군에 포함되어 있는 개별업종 간의 보험사고 발생률(위험률) 차이가 크게 발생한 사례가 있어 단일요율이 해당 업종군을 대표하는 적정한 기본요율이라고 보기 어려운 측면이 있고,

또한, 원수보험회사 등에 제공하는 협의요율의 산출·적용 등을 위한 요율매뉴얼이 마련되어 있으나 동 매뉴얼에서 정하고 있는 방식과 다르게 요율이 산출된 사례가 있는 등 요율 산출과정의 일관성 및 신뢰성이 저하될 우려가 있으므로,

앞으로 보험사고 발생률(위험률)을 기준으로 업종을 분류하는 등 기본요율 산정 체계를 합리적으로 정비하고, 협의요율이 매뉴얼 등과 다르게 임의로 산정되지 않도록 요율 검증 절차 및 관리 체계를 강화할 필요가 있음

(5) 보험 미수금 및 미지급금 정산 업무 관리 강화 필요

보험미수금은 대손충당금 및 유동성 리스크를 증가시키고 장기화될 경우 회수 가능성이 낮아지게 되며 보험미지급금은 대외 신뢰도에 부정적인 영향을 미치게 되므로 회사는 발생 원인을 면밀히 분석, 관리하여 내부요인으로 인한 발생을 최소화하고, 외부 요인으로 인해 발생하는 보험미수금 등에 대해서는 신속하게 확인·처리하여 감축시킬 필요가 있음

2023.3월 말 기준 회사의 보험미수금 및 보험미지급금 규모는 각각 ▣▣▣▣▣억원, ▤▤▤▤▤억원이며, 이 중 회사 내규에 따라 '요주의' 이하로 분류하고 있는 보험미수금 및 보험미지급금은 각각 ▧▧▧▧억원, ▩▩▩▩억원으로 거래사와의 계수(금액, 수수료 등 계약 관련 정보) 불일치, 거래사와의 정산 관련 서류 교환 지연, 거래사 파산 등으로 인해 발생하고 있는데도

회사는 주요 중개사 및 고액건 위주로 보험미수금 등을 관리하고 있어 개별 미정산 사유 및 회수 진행 과정에 대한 확인이 어렵고 신속한 업무처리를 위한 유인이 부족하며

보험미수금 등 발생 건에 대해 관련 부서(정산팀, 영업팀, 손사팀 등) 간 원인 확인요청·검토결과 등을 관리할 수 있는 시스템 등이 구축되어 있지 않고 장기 미처리 건에 대한 대응 체계가 마련되어 있지 않음

또한, 정산 업무 담당자는 거래사와 계약번호별 정산내역을 비교하여 계수 일치 여부를 확인하고 있는데 업무시스템에 실제 정산대상이 아닌 계수까지 등록되어 있는 등 담당자가 거래사 내역과 비교해야 하는 정산 대상량이 방대하여 처리가 지연·누락될 우려가 있으므로

앞으로 보험미수금 등을 체계적으로 확인·관리·처리할 수 있는 시스템을 마련 하고 미정산 계약을 신속히 처리하기 위한 관련 부서 간 협조체계를 구축하는 한편, 정기적으로 보험미수금 등에 대한 건별 미정산 사유를 유형별로 분석하여 대응방안을 수립하는 등 관련 업무를 강화할 필요가 있음

(6) 대체투자 의사결정 절차 강화 필요

회사는 내규「리스크관리규정」에 “투자심의위원회 위원장은 필요하다고 판단시 투자심의위원회 결의사항을 전문위원회에 부의할수 있다”고 규정하면서,

2022.11월 투자심의위원회에서 부결된 대체투자건을 투자심의위원회 위원장의 판단으로 리스크관리전문위원회에 재부의하여 가결한 사례가 있었으나,

동 대체투자건의 경우 의사결정에 있어 특별히 고려해야 할 위험 등 추가적인 리스크관리 논의가 필요한 건이라 보기 어렵고, 리스크관리전문위원회에 부의할 필요성에 대해 별도로 검토된 사실이 없으며

리스크관리전문위원회에서는 투자심의위원회의 부결 사유인 위험요인에 대해서 별다른 논의 없이 투자대상회사와의 거래관계 등의 위험관리와 관계없는 이유로 해당 투자건을 가결한 사실이 있었으므로,

앞으로 리스크관리전문위원회에 부의된 사안에 대해서도 투자에 대한 최종 결정은 투자심의위원회에서 이루어지도록 하는 등 투자 의사결정에 대한 업무분장 및 집행권한을 명확히 하고, 투자심의위원회 결정사항에 대한 리스크관리전문위원회 부의시 그 필요성, 요건, 투자심의위원회 결과 등이 충실히 논의될 수 있도록 하는 등 대체투자 의사결정 절차를 강화할 필요가 있음

(7) 중·장기적인 자본적정성 관리계획에 따른 일관성 있는 자본정책 수립·시행 필요

회사는 추가적인 자기자본확충이 요구되는 공동재보험(2022년 시행)과 신지급여력제도(2023년 시행) 도입을 앞두고 2020.1~8월 중 5차례에 걸쳐 약 ◉◉◉억원의 자기주식을 취득하여 자본을 축소시킨 반면, 2019.10월~2023.3월 중에는 4차례에 걸쳐 ◆◆◆◆억원의 신종자본증권을 발행하여 자본을 조달하는 등 상반된 자본정책 시행으로 인해 자본조달의 효율성과 일관성이 저하된 사실이 있었으므로,

앞으로 중·장기적 관점의 자본적정성 관리계획을 강화하고, 세부적인 자본정책의 검토·실행시 중장기적인 회사의 자본적정성 수준 등을 면밀히 검토하여 일관성 있는 자본정책이 수립·시행될 수 있도록 하는 등 자본적정성 관리를 강화할 필요가 있음

(8) IT사업 추진 및 정보기술운영위원회 운영 미흡

(가) 정보기술운영위원회에서는 내규「정보기술처리업무규정」,「계약규정」등에 따라 주요 정보기술 사업에 대한 사업 추진의 타당성 검토 및 효과분석을 실시하여 사업 추진 여부 및 수립된 예산을 심의·의결하고 있는데

주요 정보기술 사업이 지연 또는 미추진되는 사례가 다수 발생하고 매년 예산 책정 및 집행금액을 비합리적으로 산정함에 따라 정보기술 사업 추진 예산의 집행 실적이 저조(5년간 평균 ▧▧% 수준)한 상황이 지속되고 있음에도, 사업 지연 또는 미추진 사유에 대하여 검토하지 않는 등 실질적 사업 수행 여부나 예산수립 및 집행의 적정성 등에 대한 심의기능이 미흡하여 주요 정보기술 사업이 적기에 추진되지 않는 경우 정보시스템 안전성 저해 또는 업무 비효율이 발생할 우려가 있으므로,

앞으로 정보기술운영위원회는 사업 규모, 업무 영향도 등을 고려한 사업별 우선순위를 선정하여 사업 추진 여부를 심의·의결하고, 심의·의결된 사업이 미추진되거나 지연되는 경우 그 사유와 수립한 예산 대비 집행 실적의 적정성에 대한 사후 심사 절차(감사팀 참여)를 마련하여 IT사업 계획 및 추진실적에 대한 관리를 강화할 필요가 있음

(나) 정보기술 사업 계약 체결에 관하여는 계약금액, 구축 완료일자, 대금지급 방법 등 계약이행에 필요한 내용을 포함한 계약서 작성 기준을 수립하고 있으나

정보처리시스템 도입·구축 사업 추진 시 검수가 완료되었음에도 '기능·만족도 상이' 및 '이행의 안전성 확보' 등 내부 사정, 요구조건 미충족으로 인한 지체상금 부과 여부 검토, 장비 불량 등의 사유로 대금 지급을 유예한 사례가 있는데, 계약상대방과 별도의 계약변경이나 합의 없이 대금 지급이 지연되는 경우 계약상대방과 분쟁이 발생할 우려가 있으므로

정보처리시스템 도입·구축 사업 계약서상 계약조항을 이행하지 못하는 사유가 발생하였거나 계약조항을 변경할 경우 감사팀의 사전 승인 절차를 감사규정 등 내규에 반영하여 동 절차를 운용할 필요가 있고

사업 검수시 요구조건, 도입물품, 성능·기능 등 계약서의 내용대로 도입되었는지에 대한 검수가 객관적으로 이루어지도록 이해당사자를 배제하여 공정하게 실시한 후 사업 추진을 결정한 전결권자의 승인을 득하여 검수확인서를 발급하도록 절차를 보완하여 계약 관련 내규에 반영하고 검수절차가 투명하게 운영될 수 있도록 관리를 강화하시기 바람

2. 개선사항

(1) 스위스 현지법인에 대한 리스크관리 체계 미흡

회사는 스위스 현지법인(재보험 전업사, 이하 '현지법인')과의 재보험거래로 인해 2020년(현지법인의 영업개시년도)부터 2022년까지 ◆◆◆◆억원의 손실이 발행하였고, 2020년 이후 3차례에 걸쳐 ◍◍◍◍억원(총 출자금 : ◎◎◎◎억원)을 추가 출자하는 등 회사의 재무건전성에 악영향을 미치고 있으나 다음과 같이 현지법인에 대한 리스크관리를 소홀히 한 사실이 있었음

회사는 현지법인(출재사)과의 계약관리 등의 업무를 담당하는 본사(수재사) 글로벌사업팀 담당 임원으로 하여금 현지법인의 이사회 의장도 겸임하도록 함으로써

현지법인(출재사)의 경영 책임자와 본사(수재사)의 계약관리 책임자로서의 역할 간 이해상충 상황이 발생하는 등 현지법인(출재사)이 본사(수재사)로 출재하고자 하는 계약의 적정성을 객관적인 관점에서 심사하기 어렵고,

현지법인과 계약 체결시 별도 인수기준 없이 계약의 ▣▣%(대재해 계약은 ▥▥%)를 인수함으로써 현지법인의 자체 리스크관리 유인이 감소되었으며,

현지법인의 급격한 영업 성장에 대한 회사의 리스크 통제장치가 마련되어 있지 않아 현지법인의 무리한 영업정책으로 인해 회사의 재무리스크가 증대할 우려가 있으므로

앞으로 현지법인 관리업무와 현지법인과의 재보험계약 체결 업무 등 이해상충 소지가 있는 업무에 대하여 직무간 상호견제와 균형이 이루어질 수 있도록 업무분장을 조정하고, 현지법인과 계약 체결시 수재위험을 평가하고 평가된 위험 정도에 따라 수재율 및 계약 조건을 차등하여 설정하는 등 합리적 인수절차를 마련하는 한편, 현지법인의 영업성장에 따른 상시점검 등을 통해 체계적 리스크 통제장치를 마련하는 등 해외 현지법인에 대한 리스크관리 업무를 개선하시기 바람

(2) 대체투자 자산의 실사 관련 업무 미흡

(가) 회사 내규 「대체투자 및 기업대출 업무 운용 기준」에 의하면 블라인드 펀드의 경우 운용사의 본사 혹은 주된 영업소에서 실사를 수행함을 원칙으로 정하고 있으나

동 내규에서 "블라인드 펀드와 같이 투자대상 자산을 특정할 수 없는 경우 의사결정기구가 마련한 대체 절차를 실시해야 한다"고 정하고 있어 블라인드 펀드에 대한 실사 규정이 상충되고 '의사결정기구'와 '대체 절차'에 대해 정의하지 않아 실사 업무 수행시 기준이 모호하며

검사대상기간 중 3건의 블라인드 투자 건에 대해 정당한 사유 없이 대체 절차*를 시행한 사실이 있으므로,

* 운용사의 본사 혹은 주된 영업소가 아닌 회사(코리안리) 회의실에서 실시

앞으로 블라인드 펀드 실사에 대한 내규의 정합성을 제고하고 실사 기준 및 절차에 대한 구체적 요건을 보완하는 등 관련 업무를 개선하시기 바람

(나) 회사는 실사 수행시 투자 유형별로 실사가 필요한 주요 사항에 대하여 유형별 체크리스트를 작성하여 실사 항목의 완전성을 확인하도록 내규를 마련하고 있는데

일부 투자 건에 대한 실사 체크리스트에 실사 일시 등이 누락 또는 오기 되어 있고, 리파이낸싱 투자 건에 대해 최초 대출 투자 건의 실사 체크리스트가 첨부되어 투자심의위원회 안건 자료로 제공한 사례가 있고

특히, 회사(회의실)에서 진행한 실사의 경우 실사 체크리스트의 내용이 운용사와의 단순 질의응답으로만 구성되어 있어 실사 본연의 기능을 수행하였다고 보기 어려우며,

내규상 담당운용역이 운용기획팀과 함께 실사 관련 체크리스트 등에 대해 연 1회 이상 타당성 점검을 하도록 정하고 있으나 동 규정 제정 이후 체크리스트에 대한 타당성 점검을 실시한 적이 없으므로,

앞으로 유사사례가 재발하지 않도록 대체투자 실사 관련 체크리스트 점검 결과의 정확성과 유효성을 점검하는 절차를 마련하고, 체크리스트 항목의 적정성과 실효성을 정기적으로 점검하는 등 관련 업무를 개선하시기 바람

(3) 손절매 관련 업무 불합리

회사 내규 「자산운용 및 관리규정」에 의하면 기준가 대비 시가하락률이 상품군별 손실한도를 초과한 경우 정해진 영업일 이내 매각 또는 환매(이하 '손절매')하는 것을 원칙으로 하고, 투자심의위원회 사전 승인을 받은 경우 계속 보유가 가능하도록 정하고 있으나,

회사는 "●●●●●●" 및 "○○○○○○"투자와 관련하여 손절매 사유가 발생하였음에도 투자심의위원회의 사전 승인이 아닌 사후 승인에 근거하여 동 자산을 계속 보유한 사실이 있고,

유보기간 이후 다시 손실한도를 초과하는 경우에 대한 대책으로 단순히 유보기간 연장을 위해 투자심의위원회의 재승인을 추진하거나, 손실이 발생한 가격으로 추가 매수하여 단순히 매입 단가를 낮추는 방안만을 제시하는 등 리스크 관리에 대한 적극적 검토가 부족하므로

앞으로 손절매 대상 자산의 계속 보유를 위한 객관적 원칙을 수립하고, 손절매 유예를 위한 절차 및 방법을 구체화하는 한편, 손절매 유보 이후 수익률 제고를 위한 실효성 있는 대책 및 관리방안을 마련하는 등 관련 업무를 개선하시기 바람

(4) 의무보험에 대한 협의요율 적용대상 확인 미흡

국가계약법 시행령 등에서 정한 요건을 충족하는 공사계약은 의무적으로 공사손해보험에 가입하도록 하고 있고 법령에 따라 의무적으로 가입하여야 하는 보험상품의 경우 보험개발원이 참조순보험요율을 제시하고 있으나,

회사는 검사대상기간 중 정부발주공사와 관련한 공사보험계약에 대하여 보험요율을 산출하여 원수보험사에게 제시하면서 해당 계약이 보험개발원에서 제시하는 참조순보험요율을 적용할 수 있는 의무보험에 해당하는지에 대해서 확인하는 절차 없이 회사의 내부(협의)요율만을 산출한 사실이 있었으므로,

앞으로 협의요율 산출시 의무보험 해당 여부 확인 및 참조순보험요율 적용 가능 여부 검토 절차를 마련하는 등 관련 업무절차를 개선하시기 바람

(5) 보험미수금에 대한 관리체계 미흡

회사는 '회수의문' 및 '추정손실'로 분류된 자산을 조기에 상각하여 자산건전성을 확보할 필요가 있으나,

해외 파산사 및 국내 원수보험사에 대한 일부 보험미수금의 경우 체계적인 상각처리기준이 없어 '추정손실' 이하의 부실자산에 대하여 장기간 상각하지 않은 사례가 있었으므로

앞으로 미수기간, 회수가능성 등을 감안하여 체계적인 보험미수금 상각처리기준을 마련하고, 회수가능성이 낮은 부실자산을 적극적으로 관리하는 등 관련 업무를 개선하시기 바람

(6) IT감사 및 자체감사 강화

감사실은 「IT감사업무 편람」에 IT부문 중점 감사항목 등을 마련하여 이에 따라 IT부문 감사를 수행하고 있고, 정보기술팀은 내규 「정보기술업무 자체감사 운영기준」에 따라 IT부서 자체감사를 실시하고 있는데

「IT감사업무 편람」에 감사 종류에 따른 감사항목, 실시주기 등이 명시되지 않아 검사대상기간 중 IT감사를 4회 실시하면서 종합검사는 2019년 1회만 수행하였고 2022년에는 미실시 사유 등을 검토하지 않은 채 IT감사를 실시하지 않은 바 있고

IT감사 결과 지적사항에 대해 조치대상 부서는 일부 지적사항이 이행되지 않았음에도 완료 보고를 하였고, 감사팀은 해당 부서에 재조치를 요구하지 않는 등 지적사항에 대한 사후이행 관리가 소홀하며

IT부서 자체감사와 관련하여서는 IT장애 수시감사 수행 대상 등 상세기준이 없어 장애발생시 수시감사 여부를 신속하게 결정하기 어렵고 일부 감사결과를 확인한 결과 점검 내용 및 증빙자료가 미흡한 사례가 있어

IT감사 및 자체감사 관련 세부 실시기준을 마련하고 지적사항 이행관리, 점검내용 및 증빙자료 관리 등 관련 업무처리 방법서 등을 마련하여 IT감사업무를 개선하시기 바람

(7) 프로그램 및 일괄작업 통제 미흡

(가) 내규「정보기술업무관리기준」에 따라 프로그램 변경 시 사용자 인수테스트를 수행하여야 하고 운영시스템 반영 후 배포결과 확인(개발자) 및 통제결과 검증(감사자) 절차를 수행하고 종결처리해야 하나

내규 등에 사후 사용자 인수테스트를 허용하는 구체적 요건이 명시되어 있지 않음에도 일부 프로그램 변경 시 인수테스트를 수행하지 않고 프로그램을 운영시스템에 先반영하였으며, 프로그램 반영 완료일로부터 1개월 이상이 경과하였음에도 사용자 인수테스트 결과 확인 등 업무절차가 완료(종결처리)되지 않는 등 업무처리가 지연되고 있으므로

프로그램 변경 시 긴급반영 외에는 사용자 인수테스트를 완료하고 운영시스템에 반영하도록 절차를 마련하고 프로그램 반영 후 업무절차상 종결처리가 지연되지 않도록 시스템을 보완하는 등 단계별 절차를 적시에 이행하도록 통제 절차를 강화하시기 바람

(나) 내규「정보기술업무관리기준」에 따라 일괄작업(batch)은 책임자의 승인을 득한 작업의뢰서에 근거하여 수행하여야 하고 배치작업관리시스템(Framework)을 통하여 일괄작업 변경·실행 등을 관리하도록 규정하고 있는데

일괄작업을 변경하거나 비정기 일괄작업을 실행하는 경우 작업의뢰서 없이 처리하고 있으며 개발자 등 담당자 이외의 직원의 배치작업관리시스템 계정에 일괄작업 변경·실행 권한을 부여하고 있어 일괄작업이 임의로 변경 또는 실행되어 사고가 발생할 우려가 있으므로

일괄작업 변경·실행 시 모두 작업의뢰서에 따라 수행하고 책임자 승인을 받는 등 관리절차를 마련하고 업무별 배치작업관리시스템 계정 권한을 분리하여 운영하는 등 일괄작업 통제 절차를 개선할 필요가 있음

(8) 데이터베이스 접근권한 등 운영 미흡

(가) 내규「정보기술업무처리규정」,「신용정보내부관리규칙」,「개인정보내부관리규칙」등에 의하면 임직원에 대한 직무를 개발과 운영 등으로 분리한 후 전산자료의 유출 등을 방지하기 위하여 DB 접근통제 시스템 등을 통해 접근권한을 업무 수행에 필요한 최소한의 범위로 업무담당자별로 차등 부여하여야 하나

프로그램 개발 직원(외주직원 포함) 및 현업부서 직원에게 운영 데이터베이스 접근권한을 부여하고 있고 전산자료 변경내역에 대한 적정성을 사후 확인하지 아니하여 작업자 실수 등으로 전산오류 또는 전산자료 무단 변경이 발생할 우려가 있고

개인(신용)정보 처리시스템의 직급·업무에 따른 조회권한 차등부여 및 조회자, 조회일시, 대상정보, 목적, 용도 등 조회기록의 적정성에 대한 점검이 미흡하여 개인신용정보가 최신성을 유지하지 못하거나 개인(신용)정보 과다 조회, 업무 목적外로 개인(신용)정보가 조회·활용될 우려가 있으므로

운영업무 담당 직원을 제외한 나머지 직원에게 부여된 운영 데이터베이스 접근권한을 회수하고, 데이터베이스 접근권한을 재점검하여 업무 목적상 필요한 임직원에게만 최소한으로 부여하는 한편,

데이터베이스 및 업무화면에 대한 개인신용정보 조회권한(직급별·업무별)의 적정성을 재점검하고, 아래와 같은 절차를 내규에 반영하여 개인신용정보 보호대책을 강화하시기 바람

① 개인정보처리시스템(업무화면 포함) 조회권한 부여 시 준법감시팀장의 사전 결재 절차

② 개인(신용)정보를 이용하는 업무화면 등에 대한 조회 권한의 직급별·업무별 차등 부여 여부, 개인(신용)정보 조회기록(조회자, 조회일시, 대상정보, 목적, 용도 등) 및 업무용 단말기 보관 여부, 데이터베이스 접근권한의 적정성에 대한 점검 주기를 명시하고 상기 점검 결과를 신용정보관리·보호인이 대표이사에게 보고(승인)하는 절차

(나) 데이터 검증, 백업 등을 위해 운영시스템에 임시테이블을 생성하면서 임시테이블 생성 의뢰서 작성이 누락되고 책임자 승인 없이 테이블을 생성하였으며 테이블 사용목적이 종료되었음에도 이를 삭제하지 않고 있는 등 임시테이블에 대한 관리가 소홀하므로

임시테이블을 불가피하게 생성할 경우 사용목적, 사용기간 등을 명시하고 책임자의 승인을 받아 생성하며 사용목적이 종료된 임시테이블은 즉시 삭제하는 등 관리 절차를 마련·운영하시기 바람

(다) 테스트데이터 사용 시 변환 솔루션(SQL Canvas Trans)을 통해 중요데이터를 변환하여 사용하여야 하고 테스트 종료 시에는 즉시 삭제하여야 하나

데이터 변환 대상에 대한 기준이 마련되어 있지 않고 이용목적, 사용기간, 변환처리 승인자 등을 포함한 신청 및 폐기에 대한 세부절차가 없어 변환 대상이 누락되거나 변환데이터가 적시에 삭제되지 않을 우려가 있으므로

테스트데이터 변환 대상 기준, 신청 및 폐기 절차 등 테스트데이터 변환에 대한 세부절차를 포함한 관리정책을 마련·운영하시기 바람

(9) 비상대책 수립·운용 및 전산센터 운영관리 강화

(가) 내규 「위기관리 실무 매뉴얼」에 따라 장애, 재해 등 긴급상황 발생 시 업무가 중단되지 않도록 매년 재해복구 훈련을 실시하는 등 업무지속성 확보 방안을 수립·운용하고 있으나

현업부서 업무담당자 및 IT부서 책임자 없이 재해복구 훈련을 실시하거나, 정보처리시스템 구성 변경 및 신규 업무 현황 등을 동 매뉴얼에 적시에 반영하기 아니하여 비상상황 발생 시 업무지속성 확보가 어려울 수 있으므로

핵심 업무를 포함한 훈련 대상 업무, 업무별(현업 및 IT부서) 담당자, 비상상황 발생 시 비상대응 조직 및 운용 절차, 비상 지원인력 또는 외부 전문업체 활용방안 등을 동 매뉴얼 명시하여 재해복구 모의훈련을 실시하는 한편,

매년 정기적으로 「위기관리 실무 매뉴얼」을 점검하여 변경 및 신규 추가사항 확인 시 즉시 반영토록 관련 절차를 마련하여 비상대책 수립·운용의 실효성을 확보하시기 바람

(나) 전산센터內 서버 등 전산장비를 시건장치 없이 전산랙(RACK)에 탑재·운용하거나 상기 전산랙에 미사용 전산장비(△△△대)가 전원 및 네트워크 회선이 연결된 상태로 운용중인 전산장비와 같이 탑재되어 있어 비인가자의 접근이나 작업자의 단순 실수 등으로 인한 보안사고나 전산장애가 발생할 우려가 있고,

전산자료가 저장된 백업테이프를 전산센터 통로에 방치하고 있어 비인가자에 의한 전산자료가 유출될 우려가 있으므로

전산랙에 시건장치를 설치하여 관리자 승인 후 전산장비 접근이 가능토록 통제하고, 미사용 전산장비를 회수(창고 이동 또는 폐기 등)하여 비인가자의 접근, 작업자의 단순 실수 등으로 인한 보안사고 또는 전산장애 발생 가능성을 최소화하는 한편,

전산자료의 백업테이프를 내화금고 등 안전한 장소에 보관한 후 접근기록을 관리하고, 정기적으로 백업테이프 보관 개수 및 접근기록 등 관리현황을 정보관리최고책임자에게 보고하는 절차를 내규에 반영하여 전산센터 운영관리를 강화하시기 바람

(10) 정보처리시스템 안전성 확보 및 보안대책 강화

(가) 정보처리시스템 및 업무용 단말기에 대한 IP주소 부여 기준을 마련하지 아니하여 운영·테스트·개발 등 정보처리시스템 유형별, 운영·개발 담당 및 내·외부직원 등 업무용 단말기 특성별로 네트워크를 분리하여 IP주소를 설정하지 않고 있어

개발 및 테스트 서버의 장애 또는 보안 취약점이 운영 서버로 전이되거나 중요 단말기 보안정책이 완화될 우려가 있으므로

정보처리시스템 및 업무용 단말기에 대한 IP주소 부여 기준을 내규에 반영하고 운용 중인 정보시스템과 내·외부직원에게 부여된 IP주소 대역을 일제 점검하여 새로운 기준에 따라 재부여하고

신규 정보처리시스템 설치 또는 내·외부직원 전입 시 유형별(정보처리시스템: 운영, 테스트, 개발 등, 임직원: 중요 단말기·일반 단말기, 내·외부 인력별, 직무별) IP주소 대역에 따라 구축·적용될 수 있도록 사전 검토 절차를 마련하는 등 IP주소 관리체계를 강화하시기 바람

(나) 정보처리시스템의 장애 예방 및 성능의 최적화 등을 위해 정보처리시스템의 사용현황 및 추이 분석 등을 정기적으로 실시하지 않고 있고 정보시스템별 CPU, 메모리, 저장장치 등 전산 자원 임계치를 설정하지 않고 있어

검사대상기간 중 CPU 및 저장장치 저장 용량이 각각 ▨▨%, ▦▦%를 초과하는 사례가 지속적으로 발생하고 있음에도 용량 증설 검토 등의 조치를 하지 않아 성능부족 등으로 인한 전산장애가 발생할 우려가 있으므로

시스템별 자원 사용률 임계치 설정 및 전산 자원 임계치 초과 시 원인분석 및 용량 증설 검토 등을 포함한 절차를 내규에 반영하고, 동 절차에 따라 클라우드를 포함한 정보처리시스템의 전산 자원 사용현황 및 추이 분석을 정기적으로 실시하여 성능관리 보고서를 정보관리최고책임자에게 보고하는 한편,

시스템별로 설정된 전산 자원의 임계치를 초과하는 등 이상 징후를 보이는 경우 시스템 관리자가 즉시 대응할 수 있도록 시스템 성능관리 모니터링 체계를 구축·운용하는 등 정보처리시스템의 성능관리를 강화하시기 바람

(다) 내규 「정보보호업무관리기준」에 의하면 정보처리시스템의 안전한 운영을 위하여 운영체계 등의 긴급하고 중요한 보정(patch) 상황이 발생하면 즉시 보정작업 적용 여부를 결정하고, 긴급보정 이외에도 정기적으로 보정작업 필요성에 대하여 검토하여야 하나

운용 중인 정보처리시스템 총 ◇◇◇대 중 ◎◎◎대는 보정작업 필요성 검토 및 보정작업을 실시하지 않거나 제조사의 기술지원이 종료된 노후 장비를 운용하고 있어 시스템 장애에 대한 신속한 대응이 어렵고 신규 취약점을 이용한 해킹 및 악성코드 등에 의한 침해사고가 발생할 우려가 있으므로

시스템별 보정사항에 대한 필요성을 정기적으로 검토·관리(내규에 절차를 반영)하여 검토 결과를 정보관리최고책임자에게 보고한 후 이를 토대로 보정작업을 실시하는 한편,

기술지원이 종료된 운영체제 등의 구체적인 전환계획을 수립하고 전환 전까지 유지보수를 받는 등 정보처리시스템에 대한 보정작업 및 노후 장비에 대한 보안대책을 강화하시기 바람

(라) 내규「정보보호업무관리기준」등에 따라 정보처리시스템의 가동기록 및 접속일시, 접속자 등을 확인할 수 있는 접근기록은 1년 이상 기록·보관하여야 하나

데이터베이스 및 방화벽을 제외한 나머지 정보처리시스템에 대한 가동 및 접근기록과 전체 정보처리시스템(서버, 네트워크 장비 등 포함)에 대한 접근기록 이상 여부를 정기적으로 점검하고 있지 아니하여 사고 발생 시 사고원인 추적 및 근거자료로 활용이 어려울 수 있으므로

서버, 데이터베이스 네트워크, 보안장비 등 전체 정보처리시스템의 가동기록 및 접근기록의 보관 여부, 보관 기한(1년 이상) 준수 여부, 기록·보관 항목의 적정 여부를 일제 점검하고 내규에 가동 및 접근기록 점검 주기 및 절차를 반영하여 동 점검결과를 정보관리최고책임자에게 보고하는 등 정보처리시스템 가동 및 접근기록 관리를 강화하시기 바람

(11) 개인신용정보 비식별화 조치 미흡

내규「신용정보내부관리규칙」에 따라 회사는 개인신용정보를 보유하지 않는 것을 원칙으로 하되 우연한 사정으로 개인신용정보가 유입된 경우, 발견 즉시 이를 비식별화하여야 하고, 신용정보관리·보호인은 신용정보의 수집·보유·제공·삭제 등 관리 및 보호 실태와 관행에 대한 정기적인 조사 및 개선 업무를 수행하여야 하는데도

(가) 회사는 검사대상기간 동안 내부망에 있는 기간계시스템 데이터베이스에 보관 중인 주민등록번호 ▣▣▣건(중복 제외)을 비식별화하지 않았으며

(나) 신용정보관리·보호인은 검사대상기간 동안 매년 신용정보 관련 법령 및 규정 준수 여부에 대해 점검을 하였음에도 상기 데이터베이스 내 주민등록번호의 비식별화 미조치 사실을 발견하지 못하는 등 개인신용정보의 관리 및 보호 실태에 대한 점검업무는 다소 미흡함

(12) 클라우드 서비스 이용절차 운용 미흡

2019.2월 클라우드 마스터플랜을 수립한 이후 기간계 및 정보계 시스템 등 대부분의 시스템을 클라우드로 전환하여 운용 중이나

2019.6월 내규「정보기술업무관리기준」을 개정하여 '업무 중요도 관리' 기준을 마련하면서 정보의 중요도, 업무중단시 영향 등의 평가항목 없이 고유식별·개인(신용)정보 포함 시에만 중요업무로 판단하는 것으로 규정함에 따라 전체 시스템이 비중요 업무로 평가되는 현상이 발생하였고,

회사의 고유식별·개인(신용)정보 미보유 원칙과 달리 실제 데이터베이스에 고유식별·개인(신용)정보를 보유하고 있는 점 등을 충분히 고려하지 못하여 기간계시스템 등 클라우드 전환 시스템에 대한 업무 중요도의 평가에 오류가 존재할 우려가 있으므로,

2023.2월 정보의 중요도, 업무중단시 영향 등 평가항목을 추가한 개정된 내규에 따라 전체 시스템의 업무 중요도를 재평가하시기 바람

(13) 정보보호 교육 및 외부인력 보안관리 강화

(가) 회사는 인사총무팀 주관으로 매년 임직원 정보보호 교육을 시행하고 있으며, 2021년부터는 교육 대상을 외주직원까지 확대하여 시행하고 있으나

정보보호 교육 미수료자가 매년 지속적으로 발생하고 있으며, 미수료율이 높은 수준이므로, 교육 미수료자에게 패널티를 부과하는 등 임직원 정보보호 교육을 강화할 필요가 있음

(나) 내규 「보안관리기준」에 따라 외부인력 투입 시 '보안서약서' 및 철수 시 '투입해제 인력 보안확약서'를 징구하여야 함에도

계수입력용역계약(사옥관리대행계약에 포함) 수행과 관련하여 자회사인 KR실업㈜ 계수입력 담당 인력이 철수 시 '투입해제 인력 보안확약서'를 징구하지 않았음