제재내용 공개안

1. 금융회사명 : 한국투자증권㈜

2. 제재조치일 : 2024. 11. 26.

3. 제재조치내용

제재대상	제재내용
기관	○ 경영유의사항 8건 ○ 개선사항 15건

4. 제재대상사실

가. 경영유의사항

(1) 신용공여 금리결정 체계 운영 강화

(가) 신용공여 이자율 결정 시 관련 부서장들로 구성된 “대출금리산정위원회”를 운영하고 있으며, 동 위원회의 의결에 따라 금리요소 및 대고객금리 산정의 적정성을 심사하고 있으나,

별도의 심사기준이 없고, 회의에서 논의된 사항을 기록·유지하고 있지 않는 등 신용공여 금리에 대한 적정성 심사가 임의적이고 형식적*으로 이루어지고 있으므로,

* 모든 안건이 별도 의견없이 만장일치 가결 처리

구체적인 심사기준을 마련하고, 위원회 구성을 임원급으로 격상하여 논의결과 등을 기록·유지하는 등 위원회 운영의 실효성을 제고할 필요가 있음

(나) 신용공여 이자율 결정 시 경쟁사 금리 등을 고려해 대고객 금리를 미리 정한 뒤, 이에 맞춰 목표이익률을 조정하는 방식을 취하고 있는 바, 기준금리 및 원가요소가 하락하여도 대고객 금리는 동일하게 부과되는 문제점이 있으므로,

금리 원가요소 및 목표이익률을 객관적으로 산정한 뒤 기준금리에 가산하여 대고객금리가 결정될 수 있도록 신용공여 금리 산정체계를 합리적으로 개선할 필요가 있음

(2) 공매도 관련 내부통제 강화

(가) 한국투자증권은 자체적인 공매도 관련 잔고관리시스템(WINK 등)을 구축하여 운영하고 있으나,

부서 간 내부 대차거래 시 대여부서의 대여가능 수량이 충분하지 않음에도 대차거래가 이루어질 소지가 있는바, 차입부서에서 대여부서의 대차잔고를 초과한 차입신청이 사전에 차단될 수 있도록 공매도 관련 잔고관리시스템 운영을 강화할 필요

(나) Compliance부는 금융투자협회「금융투자회사의 증권 대차 및 공매도 업무처리 모범규준」을 준수하기 위해 부서별 해당 사항에 대해 업무절차 수립 및 이행 결과 회신을 요청하였으나

이행 결과에 대한 점검을 소홀히 하여 공매도 업무 관련 내부통제가 체계적으로 이루어지지 않은 사실이 있으므로, Compliance부는 공매도 수행 및 점검 관련 총괄조직 및 부서간 업무절차와 방법을 명확하게 정립하고 내규화하여 공매도 관련 내부통제장치 운영을 강화할 필요가 있음

(다) 한국투자증권은 내규「내부통제기준시행세칙」제31조에 독립거래단위 운영 기준을 마련하고 있으나,

부서내 다수의 독립거래단위 운영 시 업무프로세스별 소속 임직원의 직무 분장이 미흡하고 부서내 독립거래단위의 독립성을 유지할 수 있는 운영 관리방안이 미비하므로 이에 대한 구체적인 내부관리기준을 마련하고 내규 등에 따라 독립적인 운영을 강화할 필요가 있음

(3) 투자자문업자와 업무제휴 시 커미션 지급구조 합리화

한국투자증권은 투자자문사와 위수탁계약을 체결하여 동사의 거래플랫폼을 통해 투자자에게 투자자문서비스를 제공하고, 해당 투자자의 계좌에서 동사가 취하는 모든 보수·수수료의 일정 비율을 자문사에게 커미션으로 지급하고 있는 바,

수탁자(증권사)가 위탁자(자문사)에게 대가를 지급하는 계약구조가 비정상적이고, 자문사가 제공한 자문서비스와 무관한 거래에 대해서도 커미션을 일괄지급하는 것은 불합리하므로,

제휴계약 구조를 개선하여 주체별 책임과 권한을 명확히 하고, 실제 자문사가 제공한 서비스와 관련이 있는 거래에 대해서만 커미션이 지급될 수 있도록 관련 제휴 서비스 운영을 합리화할 필요가 있음

(4) 대체투자에 대한 리스크관리 강화

(가) 대체투자에 대한 사후관리 강화

투자의사결정시 정해진 셀다운 기한을 준수하지 못한 건에 대한 사후관리시, 내규상 검토하기로 되어 있는 항목*에 대한 기재가 누락되어 검토가 미진할 우려가 있으므로

* 셀다운 지연 사유, 셀다운 지연 또는 실패시 대응계획, 스트레스 상황을 가정한 셀다운 지연, 실패로 인한 대응계획 등

셀다운 지연 투자건에 대하여 회사의 대응방안과 관련된 내용을 사후관리 보고서에 포함후 보고하도록 개선할 필요가 있으며,

부동산PF 대출채권(매입확약 등 지급보증 포함)에 대해 여신등급 10등급(정상) 및 16등급(EOD 발생)으로만 구분하고 있어 실질적으로 EOD가 발생하지 않은 모든 사업장에 대해 정상채권으로 분류하고 있는바

사업일정 지연, 분양율 저조 등 사업성 악화가 확인되는 경우 여신등급을 조정하는 등 리스크 관리를 강화할 필요가 있음

(나) 대체투자에 대한 스트레스테스트 실효성 제고

금융투자회사는 거시경제변수 등을 감안한 대체투자 관련 주요 변수가 회사의 익스포져에 미치는 영향을 주기적으로 분석하여야 함에도, 회사는 담보가치 하락, 분양률 등 두 가지 요인만을 기준으로 스트레스 테스트를 수행하고 있는 바,

다양한 대내·외 시장충격에 대해 선제적으로 대응할 수 있도록

이자율, 공사비용, 시공사 부도율 등 리스크 요인을 추가로 선정하는 한편, 회사의 투자형태 및 리스크 속성 등의 특성을 반영하는 다양하고 실효성 있는 스트레스 테스트 방안을 마련할 필요가 있음

(5) 유동성 위기상황 분석 미흡

한국투자증권은 해외법인 등을 고려한 종합적인 유동성리스크를 관리하여야 하며 유동성 시나리오의 적정성을 정기적으로 점검하여야 하나,

유동성 시나리오 분석에 해외법인 등을 고려하지 않고, 시나리오 적정성에 대한 정기적인 점검절차가 마련되어 있지 않은바, 유동성 위기상황분석을 강화할 필요가 있음

(6) 리스크관리위원회 운영 절차 강화

「리스크관리위원회규정」제6조에 따르면 위원이 직접 회의에 출석하거나, 모든 위원이 음성을 동시에 송·수신하는 통신수단을 이용하는 경우에 대한 결의 방법만을 정하고 있으나

리스크관리위원회는 위원회 규정상의 방법이 아닌 서면에 의한 심의·결의로 진행되는 바, 위원회 개최요건 및 결의 방법 등을 구체화하여 하는 등 위원회 운영 절차를 강화할 필요가 있음

(7) 신용공여 한도관리 강화

▤▤▤▤부는 신용공여 한도 관리시, 기본 여신한도가 부여된 투자자와 별도의 한도 승인을 받은 투자자를 구분하지 않고 실제 실행된 신용공여 금액만을 기준으로 한도를 관리하고 있어, 공모주 청약 등의 사유로 일시에 신용공여 수요가 집중되는 경우 신용공여 가능금액이 단기간에 소진되어 투자자와의 분쟁이 발생할 소지가 있으므로,

한도 승인액의 규모 및 실행일정 등을 관리하는 체계를 마련하고 관련 규정을 정비하는 등 신용공여 한도관리 절차를 강화할 필요가 있음

(8) IT부문 감사체계 강화

회사 내규 「감사위원회규정」, 「감사위원회직무규정」 및 「IT자체감사시행세칙」에 따라 정보기술 및 정보보호 부문에 대한 감사를 실시하고 있으나

☆☆실 및 □□본부는 자체 감사결과 지적사항에 대한 조치 이행여부를 점검하지 않아 지적사항이 개선조치되지 않거나 차기 수시감사 시 동일하게 지적되는 등 검사 사후관리가 미흡하고

◎◎◎◎담당, ▣▣▣▣▣▣본부, ◇◇본부(■■■■■■부)는 정보보호 및 IT부문 자체감사 업무를 수행하지 않아 일상적인 업무처리 수행과 그 결과의 적정성에 대한 점검이 이루어지지 않고 있으므로

회사는 감사결과 지적사항에 대한 조치 이행결과를 징구하고 조치이행 여부를 정기적으로 점검하는 한편, ◎◎◎◎담당, ▣▣▣▣▣▣본부, ◇◇본부는 본부 내 자체감사자를 지정하고 업무 특성에 맞는 점검항목 및 점검방식에 대한 세부 매뉴얼을 마련하여 자체감사를 실시하는 등 □□부문 감사체계를 강화할 필요가 있음

나. 개선사항

(1) 신용공여 금리요소 산정 및 적용 부적정

한국투자증권은 「금융투자업자의 대출금리 산정 모범규준」에 따라 신용공여 금리요소를 산정하고 있는데,

‘신용프리미엄’ 산정 시 해당 자산에 대한 예상손실을 ‘0’으로 인식해 대손충당금을 전혀 쌓지 않고 있음에도 고객에게 최고 1.14%p를 부과하고, ‘업무원가’ 산정 시 온라인(뱅키스) 계좌의 신용공여 업무와 무관한 은행개설 수수료 등을 포함하여 산정하고, ‘목표이익률’ 산정 시 명확한 산정기준 없이 과거 대고객 금리에서 타 원가요소를 단순히 제하여 결정하고 있는 등 일부 금리요소 산정기준을 불합리하게 운용하고 있는바

회사가 인식하는 예상손실을 초과하여 고객에게 신용프리미엄을 부과하지 않고, 신용공여 업무와 무관한 비용이 고객에게 부과되지 않도록 개선하는 한편, ‘목표이익률’ 산정시 객관적 기준을 세워 경영상 적정 마진 수준으로 합리적으로 결정하고, 동 수준의 적정성에 대한 평가체계를 구축할 필요할 필요가 있음

(2) 투자일임재산 운용 관련 내부통제 개선 필요

투자일임재산 운용 시 내부통제가 미흡하여 투자자 간 투자일임재산이 거래되거나 계열회사 주식을 한도를 초과하여 투자일임재산에 편입한 사례가 발견되는 바

투자일임재산의 불건전 운용행위를 사전·사후 통제할 수 있도록 전산시스템을 포함한 내부통제를 개선할 필요가 있음

(3) 부동산PF 등 관련 성과보수 산정방식 개선

대체투자 관련 임직원의 성과보상시 내규 「대체투자 리스크관리지침」(§7②)에 따라 영업용 순자본비율(NCR) 위험값을 활용하여 관리회계상 내부손익 및 성과보수를 산정하는 경우 거래별로 리스크 수준이 차등화되도록 위험값을 세분화하여야 하는데도

투자자산별로 동일 위험값을 적용하고 있는 바, 거래의 사업성, 부실여부 등을 고려하여 거래별로 리스크를 달리 적용할 수 있도록 개선방안을 마련할 필요가 있음

(4) 리스크관리실무위원회 부의대상 명확화 필요

인수(투자) 자산의 금액 및 셀다운 여부 등을 기준으로 리스크관리실무위원회, 리스크관리위원회, 이사회에 부의하고 있으나

내규 「리스크관리규정」(§7①) 리스크관리실무위원회 부의사유에 지급보증, 부실가능 자산 대응방안 보고*가 규정되어 있지 않으므로 이를 명시하는 등 부의대상을 명확화하여 위원회를 운영할 필요가 있음

* 내규「투자관리지침」§13①에 반영되어 있으나, 리스크관리실무위원회 부의 대상을 총괄하여 규정하는 내규 '리스크관리규정'에 명확히 규정할 필요

(5) 동일인 신용공여 한도관리 방식 등 개선 필요

(가) 한국투자증권은 내규인 「신용리스크관리세칙」에 동일인 신용공여* 한도(자기자본의 25% 이내)를 반영하여 익스포저 한도관리를 하고 있으나, 직접 대출이 아닌 CB, 수익증권 등 형태로 자산을 취득하여 동일인 한도규제를 회피할 가능성이 있으므로,

* 동일인에 대한 신용공여, 기업금융업무 관련 대출, 지급보증 금액 합계

내규에 거래형태(대출, CB, 수익증권 등)와 관계없이 실질적인 거래상대방을 기준으로 신용공여 금액을 합산하도록 명확히 규정할 필요가 있음

(나) 한국투자증권은 비우량등급의 채권 총량 관리를 위해 트레이딩성 자산을 운용할 경우, BBB등급 이하 익스포저한도(자기자본의 40% 이내)를 내규로 규정하여 운영하고 있는데 동 한도관리시 비트레이딩 성격의 무등급 편입물을 대상자산에 포함하는 등 운영에 실효성이 미흡한 바,

한도관리 대상자산* 범위를 재검토하고 이를 내규에 반영하는 등 신용리스크 한도관리의 실효성을 제고할 필요가 있음

* 예시: 신용등급 존재하거나 신용등급(변화)가 중요한 의미를 지니는 자산 등

(6) 인수주식 관련 내규 개선 필요

한국투자증권의 내규*에서는 실권주 등 IB본부 취득주식에 대해 1개월이내 이를 처분하도록 규정하고 있으나,

「금융투자업감독규정」에서는 회사가 기업공개 주관업무를 수행하는 경우 과거 취득한 주식 등을 상장일부터 30일 이내 처분하지 못하도록 규정하고 있으므로, 회사의 내규를 개선할 필요

* 「인수리스크관리시행세칙」별표1 'IB본부 취득 주식 관리기준'

(7) 보안취약점 분석·평가 사후관리 강화

회사는 내규 「정보보안점검시행세칙」에 의하여 전자금융기반시설의 취약점 분석·평가를 연 1회(홈페이지는 6개월에 1회) 실시하고 발견된 취약점에 대해서는 조치계획을 수립하고 있으나,

검사대상기간 중(2018. 6. 2. ~ 2022. 10. 21.) 총 7회의 전자금융기반시설 및 홈페이지 취약점 분석·평가과정에서 발견된 취약점을 적기에 보완 조치하지 않아* 매년 동일한 유형의 취약점이 발견되고 있는 등 취약점 분석·평가 사후관리가 미흡하게 운영되고 있어 전자금융기반시설 및 홈페이지의 취약점을 이용한 보안 위협이 증가할 우려가 있으므로

* 2019년도 ⓐ개, 2020년도 ⓑ개, 2021년도 ⓒ개 등 총 ⓓ개의 누적된 취약점이 잔존

회사는 미조치 취약점에 대해 업무영향도 및 보안리스크 등을 고려하여 조치가능 여부를 재점검하고, 취약점에 대한 보완조치가 적시에 이행될 수 있도록 관리 방안을 마련하는 등 취약점 분석·평가 사후관리를 강화하시기 바람

(8) 무선통신망 차단시스템 운영 관리 강화

회사는 내규 「인프라보안관리시행세칙」에 따라 비인가 무선통신망 사용을 통제하기 위해 무선침입방지시스템(WIPS) 총 ㉮대*를 설치·운영하고 있으나

* ○○망 ⓐ대, △△△△△망 ⓑ대, ▲▲▲▲▲▲▲▲망 ⓒ대

검사착수일(2022.9.22.) 현재 운영 중인 무선침입방지시스템(WIPS)이 일부 노후화*되어 최근 무선표준**(802.11ac 등)에 대한 탐지·차단 기능을 지원하지 않아 비인가 무선기기 통제에 보안 취약점이 존재하므로

* ○○망 내 무선침입방지시스템 장비 ⓓ대는 모두 2011년에 도입
** 최신 스마트폰, 노트북 등에서는 802.11ac 이상의 표준 무선규격을 지원

회사는 앞으로 무선통신망 운영 시 보안 취약점이 발생하지 않도록 최신 무선 표준 규격의 기술적인 특성 등을 주기적으로 검토하여 무선접속장비(AP) 및 무선침입방지시스템(WIPS)을 개선하는 등 무선통신망 운영·관리를 강화하시기 바람

(9) 전산자료 보호 대책 수립·운용 강화

회사는 고객정보를 활용한 테스트 시 내규 「응용프로그램보안시행세칙」,「암호관리시행세칙」에 따라 고유식별정보 등 민감정보*를 '데이터 변환 솔루션(SQLCanvas)'을 통하여 변환한 후 이용하고, 보안강도 등을 고려하여 암호화 알고리즘을 선정하며, 정보처리시스템의 비밀번호를 일방향 암호화하여 저장하고 있고

* 고유식별정보, 계좌번호, 비밀번호, 고객명, ID, 전화번호 등

내규 「인프라보안시행세칙」 및 「계정관리시행세칙」에 따라 전산자료 접근 및 명령어 통제를 수행하기 위한 접근통제시스템(Petra, DB-Safer)을 구축하여 데이터베이스 접속 및 이용자의 접근권한을 통제하고 있으나,

① 내규상 테스트데이터 변환 시 승인권자가 명시되어 있지 않고 제3자 확인 여부 등을 확인할 수 있는 절차를 내규가 아닌 내부

문서* 등으로 갈음하고 있으며, 검사대상기간 중(2018. 6. 2. ~ 2022. 10. 21.) 테스트데이터 변환 신청 ㉮건 가운데 ㉯건(㉰%)이 신청자(팀장)와 승인권자(팀장)가 동일한 자가승인** 건으로 데이터 변환의 적정성 확인이 미흡할 우려가 있으므로

* '20.10.02. 테스트데이터 변환 통제 시행(개정) 안'

** 테스트데이터 변환 시 IT내부감사자가 2차 승인을 수행하고 있으나, 1차 승인 시 팀장의 경우 데이터 변환 솔루션 내 자가승인이 가능

회사는 앞으로 이용자정보 변환 시 제3자 확인 절차가 강화되도록 데이터 변환 솔루션(SQLCanvas) 시스템 내 승인절차를 개선하고 관련 내규를 마련하시기 바람

② 검사착수일(2022.9.22.) 현재 일부* 정보처리시스템의 비밀번호는 국가기관 등에서 권고된 암호화 방식**보다 보안강도가 낮은 암호화 알고리즘(SHA-1, DES 등)이 적용되어 있어 보안에 취약할 우려가 있으므로

* ○○○, ▲▲▲, △△△ 등 ⓐ개의 운영시스템(Oracle DB)

** 한국인터넷진흥원(KISA)의 '암호 알고리즘 및 키 길이 이용 안내서(2018.12.)'에서 비밀번호 등의 경우 SHA-224/256/384/512 등 해쉬함수 보안강도가 112비트 이상인 암호화 알고리즘 사용을 권장

회사는 정보처리시스템의 비밀번호는 안전한 일방향 알고리즘(SHA-2 등)을 적용하여 암호화하도록 전환계획을 수립·이행하고, 정보처리시스템에 적용된 암호화 알고리즘의 안전성 등이 적정한지 주기적으로 점검하도록 관리체계를 강화하시기 바람

③ 업무부서와 개발담당 일부 직원에게 운영 데이터베이스를 조회·열람할 수 있는 권한을 부여하고 있어 과도한 데이터 조회에 따른 보안상 위협이 발생할 우려가 있으므로

회사는 앞으로 업무부서 및 개발담당 직원에게는 원칙적으로 운영시스템의 데이터베이스 계정 및 데이터 접근권한을 부여하지 않도록 하고 운영 담당 직원에게만 데이터베이스 계정 및 데이터 접근권한을 필요 최소한의 범위에서 부여하도록 관련 절차를 강화하시기 바람

④ DB접근통제 시스템 內 권한내역과 실제 DBMS(데이터베이스 관리시스템) 접근권한이 동기화되어 있지 않는 등 세부적인 권한관리 절차가 미흡하여 비인가자가 권한 없는 정보에 접근할 우려가 있으므로

회사는 접근통제 시스템과 실제 데이터베이스간 접근권한이 동기화될 수 있도록 접근통제시스템(Petra, DB-Safer) 기능을 개선하시기 바람

(10) IT부문 내규 수립 및 외주관리 강화

① 조직개편에 따라 신설된 ▤▤▤▤부(20xx.x월), ▣▣▣▣▣▣부(20xx.x월), ☆☆☆☆☆부(20xx.x월), ▽▽▽▽▽부(20xx.x월)는 마이데이터, 미니스탁 등의 개발·운영 및 DB관리 등 IT업무를 수행하고 있으나,

▣▣▣▣▣▣부는 내·외부 데이터를 활용한 분석 DB관리 업무를 수행하면서 DB 접근통제 절차 및 정책 등을 내규가 아닌 운영매뉴얼로 마련하고 있으며

☆☆☆☆☆본부(▤▤▤▤부, ☆☆☆☆☆부, ▽▽▽▽▽부)는 업무매뉴얼에 IT개발·운영 업무에 대한 사항은 △△본부 소관 내규*를 준수하도록 정하고 있으나

* 개발관리 시행세칙, 변경관리 시행세칙, 외주업체관리 시행세칙

△△본부 소관 내규에서는 위 4개 신설 부서들을 적용 대상으로 규정하고 있지 않아 IT업무 수행에 관한 근거와 권한이 명확하지 않을 우려가 있으므로

▤▤▤▤부, ▣▣▣▣▣▣부, ☆☆☆☆☆부, ▽▽▽▽▽부는 수행 중인 IT부문에 관한 업무절차 및 업무 수행상 필요한 세부사항 등을 내규로 마련하시기 바람

② 회사 내규 「외주업체관리시행세칙」은 시스템 개발·유지보수 등의 외주업무 관리에 대한 기준을 명시하고 있으나

외주업체를 통하지 않고 회사가 직접 구매하는 전산장비, 소프트웨어 등 IT자산 관련 계약 및 검수 절차가 동 시행세칙에 규정되어 내규의 제정목적에 부합하지 않고

IT개발·운영 외주업체인 '◆◆◆◆◆◆'에 대해 서비스품질 요구수준 및 서비스품질 평가기준 등을 포함한 평가표를 구체적으로 정하지 않고 담당팀장이 업무숙련도, 납기준수, 오류유발, 성실도 4개 항목을 객관적 지표 없이 평가하고 있어 평가 결과의 신뢰도가 저하될 우려가 있으므로

회사는 IT자산의 계약 및 검수 절차 등이 내규의 목적에 부합하도록 관련 내규를 정비하고, 차후 ◆◆◆◆◆◆과 IT개발·운영 도급 계약 시 서비스품질 요구수준 및 서비스품질 세부 평가기준 등을 포함한 서비스수준 평가표를 계약서에 포함하시기 바람

(11) 정보처리시스템 운영체제 등 보정작업 강화

내규 「IT운영체제규정」과 「하드웨어시스템설치관리시행세칙」 등에 따라 IT인프라가 응용 시스템을 효과적으로 지원하기 위해 적합한 플랫폼을 제공하여야 하고, 정보처리시스템의 안전한 운영을 위하여 정보처리시스템의 운영체제, 시스템 소프트웨어 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 하여야 하는데도

검사착수일(2022.09.22.) 현재 서버 ㉮대*(총 ㉯대, ㉰%) 및 데이터베이스 ㉱대**(총 ㉲대, ㉳%)가 제조사의 기술지원이 종료된 시스템 소프트웨어를 사용하고 있어 보안패치 및 서비스 업그레이드 등의 지원을 받지 못함에 따라 시스템 오류 및 장애 발생 시 신속한 대응이 어렵고 신규 취약점을 악용한 해킹 및 악성코드 감염 등이 발생할 우려가 있음***

* AIX ⓐ대, LINUX ⓑ대(CentOS ⓒ대, RHEL ⓓ대), SOLARIS ⓔ대, WINDOWS ⓕ대, 기타 ⓖ대

** Altibase ⓗ대, DB2 ⓘ대, MS-SQL ⓙ대, Oracle ⓚ대

*** 매년 'IT 인프라 S/W EOS 보고'를 통해 기술지원종료 운영체제에 대한 업그레이드 또는 교체를 추진 중이나 그 비율이 연 ①% 내외의 수준임

회사는 기술지원이 종료된 시스템 소프트웨어를 업그레이드하거나 제조사와 기술지원 연장계약을 체결하는 등 시스템 소프트웨어 장애발생을 미연에 방지하기 위한 대응방안을 마련할 필요가 있음

(12) 장애관리 업무절차 개선

회사 내규 「IT운영체제규정」과 「장애관리시행세칙」 등에 따라, 회사는 IT부문의 장애 및 보안사고의 체계적인 관리체계를 확립하고 신속한 장애복구와 지속적인 서비스를 제공하기 위하여 장애관리대장에는 정보처리시스템의 장애일시, 장애내용 및 조치사항 등을 상세하게 작성·보관하여야 하는데도

엑셀파일로 관리하고 있는 장애관리대장*에 장애시간, 장애내용, 조치사항, 향후대책, 작성자, 작성일시, 확인자 및 확인일시 등의 내용이 누락되어 있고, ▣▣▣▣▣▣부서의 민원으로 확인된 일부 장애(오류)**가 장애관리대장에 기록되지 않았으며,

* 순번, 발생일자, 제목, 장애/오류 구분, 관련부서, 관련팀, 장애원인, 유발자만 기록

** 해외주식 액면병합 종목 업무처리 오류(▣▣▣▣▣부-2020-0624), 서버자동주문 오류(▣▣▣▣▣부-2020-1366), 해외주식배당옵션 신청 오류(▣▣▣▣▣부-2021-1700)

장애보고서는 회사 내규 「장애관리시행세칙」“별지 제1호 서식“을 준수하여 작성·관리되어야 함에도 이를 준수하지 않은 양식을 일부* 사용함에 따라 작성자, 확인자의 서명이 확인되지 않으며, “별지 제1호 서식”에 IT자체감사자에게 제출한 일자와 IT자체감사자의 접수 확인 서명, 보고선(보고받은 자) 정보 등이 기록·관리되지 않고 있음

* MTS 고객 바이오 인증 지연 보고(2020.03.25.), 온라인 매체 고객 접속 지연 오류 보고(2020.09.03.) 등 6건

회사는 장애상황기록부 및 장애보고서 서식을 개정하고 장애관리 시스템을 구축하여 장애별로 누락되는 정보가 없도록 철저히 기록·관리하며, 타 부서를 통해 확인된 장애에 대해서도 관리하는 등 장애관리 업무절차를 개선할 필요가 있음

(13) 정보시스템 감리수행 절차 강화

전산운영위원회는 정보시스템의 안전성 확보를 위해 전자금융업무 등 대고객 서비스와 관련된 외부주문과 투자규모가 50억원 이상의 정보화 사업은 감리 시행의 필요성을 검토하여 감리를 시행하여야 하나

감리 시행의 필요성을 검토하지 않고 사업을 추진하고 있어 정보시스템의 효율성 및 안전성 확보에 문제가 발생할 우려가 있으므로

회사는 감리 시행 여부에 대한 검토 결과를 사업 품의 문서에 포함하여 사업을 추진토록 하는 등 감리업무 처리 절차를 개선할 필요가 있음

(14) 시스템 개발·유지보수 업무절차 강화

회사는 아래 ①~⑥과 같이 정보처리시스템 개발·유지보수 업무 수행절차를 불합리하게 운영하고 있으므로 회사는 관련 업무절차와 시스템을 개선할 필요가 있음

① 일괄작업 프로그램 오류 원인을 유형별로 분석·관리하지 않고 있어 일괄작업 시 유사한 원인으로 인해 반복적으로 오류가 발생할 우려가 있음

② 업무요건 충족 여부에 대한 개발요청 부서의 인수테스트 없이도 변경된 프로그램의 운영시스템 반영이 가능하여 개발요건 미충족으로 인한 오류가 발생할 우려가 있음

③ 테스트 항목, 결과서 등 개발 관련 산출물을 업무담당자 단말기에만 보관하고 있어 오류 발생시 테스트 수행 여부의 객관적인 검증이 어려움

④ 시스템 관리자 外 개발자에게도 시스템 중단 등을 일으킬 수 있는 중요명령어 실행권한을 부여하고 있어 명령어 오입력 등 조작 실수로 인한 전산오류가 발생할 우려가 있음

⑤ 형상관리 시스템을 사용하지 않고 운영시스템에서 프로그램을 반출하고 있어 개발자 착오 등으로 불필요하거나 구버전의 프로그램이 운영시스템으로 이관될 우려가 있음

⑥ 주식 매매 등 전자금융거래 프로그램도 ☆☆☆☆부서 확인 없이 개발자 등이 보안성 검증을 실시하고 있음

(15) IT아웃소싱 업무통제 강화

회사는 IT업무 전반을 IT아웃소싱 업체에 위탁·운영(Total Outsourcing)하고 운영·개발 등 중요 업무별로 관리책임자를 지정하고 있으나

중요 업무에 대한 상시 보고 체계가 미흡하여 위탁·운영 업무에 대한 업무절차를 미준수하는 등으로 인해 장애가 발생할 우려가 있으므로

회사는 위탁·운영 업무처리 절차 준수 여부에 대해 점검을 실시하는 한편, 업무별 상시감시 체계를 마련·운용할 필요가 있음