경영유의사항 등 공시

1. 금융회사명 : 삼성증권㈜

2. 조치일 : 2022. 12. 1.

3. 조치내용

대상	내용
기관	○ 경영유의사항 10건 ○ 개선사항 16건

4. 조치대상사실

가. 경영유의사항

(1) 사내 정보교류차단 예외승인 업무절차 강화

□ 삼성증권㈜ 내규「xxxxxx지침」제x-x조에 따르면, 사내 정보교류차단 예외승인은 정보를 제공할 상당한 이유가 있고, 제공하는 정보를 업무상 필요한 최소한의 범위로 한정하는 등 요건을 모두 충족하는 경우에만 가능함에도 2017년~2021.1월 기간 중 총 xxxx건의 정보교류차단 예외를 승인하였는 바,

○ 동 절차가 형해화 될 우려가 있으므로 향후 요건충족 여부를 면밀히 검토하는 등 사내 정보교류 관련 업무절차를 강화할 필요가 있음

(2) 정보교류 차단 관련 점검절차 강화

□ 삼성증권㈜ 내규「xxxxxx지침」제x-x조에 따라 준법감시인은 사내 정보차단 부문 간 또는 계열회사와의 정보를 교류하는 경우에는 관련 유지기록을 확인·점검하여야 함에도

○ 정보차단 부서 간 보안 예외 승인을 받은 외부저장매체를 통한 정보 교류, 계열회사와 외부회의를 통한 정보교류 등을 모니터링 하는 절차가 미흡하므로 이를 개선할 필요가 있음

(3) 이해상충 방지 등을 위한 통신내용 유지·관리 필요

□ 삼성증권㈜ 준법감시팀은 임직원의 이해상충 방지 및 정보교류 차단 의무 준수여부 등을 확인하기 위해 녹취, 전자메일 등 통신내용을 보관하고 적정성을 점검하고 있으나,

○ 2019.4월 내규「xxxxxx지침」개정으로 통신기록 보관범위가 축소됨에 따라 임직원의 이행상충 및 불법행위 등에 대한 사후점검이 어려울 소지가 있으므로, 향후 통신기록 보관부서, 보관대상 및 보관기간의 확대 등을 전면 재검토할 필요가 있음

(4) 이사회 내 소위원회의 합리적 운영 필요

□ 삼성증권㈜ 감사위원회 위원 3인 중 2인이 위험관리위원회와 내부거래위원회 위원을 겸직한 사실이 있는 바,

○ 향후 감사위원의 직무전념성 강화 등을 위해 일정 수 이상의 소위원회 겸직을 제한하는 등 합리적 운영방안을 마련할 필요가 있음

(5) 임직원 자기매매 관련 내부통제 강화

□ 삼성증권㈜ 영업부서 직원이 가족, 지인 등 타인명의 계좌를 통해 자기 계산으로 주식을 매매하였음에도 이를 고객의 정당한 주문 요청에 따라 매매를 체결한 것으로 처리하는 등의 위법행위(x명)가 발생하였는 바,

○ 향후 영업부서 임직원이 관련 법규를 준수할 수 있도록 정기적으로 가족계좌의 주문내역에 대해 자금출처를 확인하는 등 모니터링을 강화할 필요가 있음

(6) 내부감사 업무절차 강화

□ 삼성증권㈜ 내규 「xxxxxxx규정」에 의하면, 감사결과 위법·부당사항 또는 개선이 요구되는 사항을 발견한 때에는 담당부서에 개선 등의 처분을 요구하여야 함에도, 2019년 IB부문 내부감사시 지적된 '재산상 이익제공 입력 누락 과다' 등에 대한 사후보완이 미흡한 사례가 발생하였으므로,

○ 향후에는 내부감사결과 지적사항에 대한 사후처리가 철저히 이루어지도록 관련 업무절차를 강화할 필요가 있음

(7) 사모펀드 위험등급 평가 및 분류기준 등 정비 필요

□ 'xxxxxxx사모부동산투자신탁 제xx호' 등 xx개 사모펀드의 위험등급을 명확한 근거 없이 운용사보다 낮게 평가하였고, 투자대상 및 전략 등이 유사한 펀드의 유형을 다르게 분류한 사례가 발생하였는 바,

○ 향후에는 투자자에게 정확하고 일관성 있게 안내가 가능하도록 사모펀드의 위험등급 및 유형 분류기준을 정비하는 한편, 관련 통제절차를 강화할 필요가 있음

(8) 미매각 인수증권에 대한 리스크관리 강화 필요

□ 재매각 목적으로 취득한 수익증권의 미매각 규모가 증가하고 있음에도 내규(「xxxxxx준칙」)를 개정하여 처분기한 확대 및 보유기간 연장 승인권자 하향 등 처분절차를 완화하였는 바,

○ 향후 미매각 수익증권 관련 모니터링 및 리스크관리 절차를 강화할 필요가 있음

(9) 전략북의 합리적 운영 필요

□ 전략북은 정책펀드 및 관계사·유관기관 투자자산 등을 보유할 목적으로 설정된 것임에도 IB부문의 미매각 인수증권 및 PI투자자산이 이전되는 등 당초 취지와 달리 운영되고 있는 바,

○ 향후 전략북의 성격에 맞지 않는 자산 편입사례 등이 발생하지 않도록 운영취지를 명확히 하는 등 관련 업무절차를 강화할 필요가 있음

(10) 투자자재산의 채권 매매시 주문기록 유지·보관 업무절차 강화

□ 삼성증권㈜ 내규 「xxxxxxxxxx지침」 제x조에 따라 주문 및 체결 내역 통지와 관련하여 전송한 전자메일, 메신저 등은 출력 또는 파일변환하여 편철하거나 부서 파일서버에 보관하여야 함에도

○ xxx팀 및 xx팀은 채권 매매와 관련한 메신저 기록을 직원 PC에 보관하고 부서 파일서버 등에는 보관하고 있지 않아 채권 매매와 관련한 중요정보의 누락이 발생할 경우 법규준수 여부에 대한 점검이 어려울 수 있으므로,

○ 향후 투자일임재산 및 신탁재산의 채권 거래와 관련한 거래체결 과정 전반의 적정성을 검증할 수 있도록 관련 업무절차를 강화할 필요가 있음

나. 개선사항

(1) 정보교류 차단을 우회할 수 있는 PC 등에 대한 통제 강화

□ 삼성증권㈜ 내규 「xxxx지침」 제xx조, 제xx조는 PC에 보안프로그램을 설치하지 않는 등 회사의 보안체계를 우회하거나 무력화하는 행위를 금지하고 있음에도

○ 정보교류 차단을 우회하기 위해 회사의 보안프로그램이 미설치된 PC를 이용하여 회사 내부망에 접속하는 행위가 발생하는 등 정보보안상의 취약점이 있으므로 관련 통제절차를 마련할 필요가 있음

(2) 장기 외근자에 대한 근태관리 절차 마련

□ 삼성증권㈜는 내규 「xx지침」에 따라 근무시간, 휴게시간, 출근 및 결근 등에 대한 기준과 절차를 마련하여 관리하고 있으나, 장기 외근자에 대하여는 별도의 근태관리 기준이 없어 소속 부서장의 구두지시만으로 장기간 사외근무가 가능하도록 운영되는 등 근태 기록 관리가 미흡하므로,

○ 향후에는 전산으로 인사팀에 통보하는 절차를 신설하는 등 관련 근태관리 기준과 절차를 마련할 필요가 있음

(3) 파생결합증권 중도상환업무 처리 개선

□ 삼성증권㈜ 내규 「xxxxxxxxxx준칙」 제x-x조 등은 파생결합증권 발행시 중도상환 기준*을 정하고, 이를 위해 매영업일 파생결합증권 평가금액을 공시하도록 규정하고 있음에도

* 예) ELS의 경우 중도상환결정일 후 1영업일에 공시되는 평가금액의 95%이상

○ 일부 ELS에 대하여는 별도 기준에 따라 평가금액을 산정함에 따라 내부기준에 미달하여 상환한 사례가 발견되었고, DLS의 경우 평가금액 등을 수기로 관리하고 있어 공시금액 및 환매가격의 오류가 발생하였는 바,

○ 향후에는 환매정책 및 기준 등에 따라 정확한 가격으로 환매될 수 있도록 관련 절차를 개선할 필요가 있음

(4) 신용공여 이자율 산정근거 명확화

□ 삼성증권㈜ 내규 「xxxxxxxx규준」은 신용공여 이자율 산정 시 목표이익률(금리구성 요소)은 경영목표, 업계 평균 이익률 등을 감안하여 합리적으로 책정하도록 규정하고 있으나,

○ 경영목표 등의 감안 여부를 기록하지 않고 목표이익률을 산출하고 있는 바, 향후에는 동 이익률 관련 사항을 문서화하는 등 산출 근거를 명확히 할 필요가 있음

(5) IT부문 감사체계 미흡

□ 삼성증권㈜ 내규 「xxxxx규정」, 「xxxxxxx규정」 등에 따라 매년 감사계획을 수립하여 IT부서의 IT업무에 대해서는 감사실 정기감사 및 IT부서 자체감사를 실시하고 있으나,

○ 정보보호 부서의 정보보호업무에 대해서는 정기감사 및 자체감사를 실시하지 않고 있으며, IT업무 감사 시 전산장애 재발방지 대책의 적정성 등에 대해서는 점검하고 있지 않아 유사원인으로 인한 장애가 반복적으로 발생할 우려가 있으므로

○ 정보보호 부서에 대한 정기감사 및 자체감사를 실시토록 하고 전산장애 대책의 적정성에 대해서도 감사활동을 강화할 필요가 있음

(6) IT부문 내규 관리 강화

□ 전자금융거래의 안정성을 위해 IT부문 관련 200개의 내규를 제정하여 운영하고 있으나

○ 전자금융거래법 등 관련 법령이 내규에 누락되거나 다르게 기술되어 있는 부분*이 있어 임직원이 관련 법령을 위반할 소지가 있으므로

* 「전자금융거래법」제8조(오류의 정정 등), 제24조(약관의 명시와 변경통지 등), 「전자금융 감독규정」 제32조(내부사용자 비밀번호 관리) 등

○ 전자금융거래법 등 관련 법령과 IT부문 내규 간의 상호 정합성을 재정비 하는 등 IT부문 내규 관리를 개선할 필요가 있음

(7) 사용자 비밀번호 관리 강화

□ 내규 「xxxxxxx지침」에 따라 내부 사용자가 사용하는 정보처리시스템의 비밀번호를 안전한 알고리즘(SHA256 등)으로 암호화하고 있으나

○ 일부(녹음청취시스템)시스템의 비밀번호에 대해서는 국가에서 권고하는 보안강도에 미달하는 알고리즘(SHA1)이 적용되어있어 해킹 등에 의해 비밀번호가 노출될 우려가 있으므로

○ 안전한 알고리즘(SHA256 등)을 이용하여 비밀번호를 암호화하는 등 비밀번호 암호화 대책을 마련할 필요가 있음

(8) 일괄작업 통제 강화

□ 일괄작업(BATCH) 프로그램은 책임자의 승인을 득한 작업요청서에 근거하여 일괄작업을 수행토록 통제하고 있으나,

○ 일괄작업 프로그램 수행 권한 및 수행결과에 대한 접근권한의 적정성 점검이 되지 않아 권한 없는 사용자 작업에 의해 오류가

발생할 소지가 있고, 오류발생 시 원인 분석이 미흡하여 동일한 전산장애가 발생할 우려가 있으므로

○ 일괄작업 프로그램 수행 및 수행결과에 대한 접근권한을 재점검하여 업무 관련자만 접근할 수 있도록 하고 동일 원인으로 인한 오류 발생을 최소화하기 위해 발생한 오류원인을 체계적으로 분석하는 등 일괄작업에 대한 통제를 강화할 필요가 있음

(9) 프로그램 인수테스트 강화

□ IT부서에서 개발·테스트를 완료한 프로그램은 현업부서 업무담당자에게 인수테스트를 요청하고 있으나

○ 인수테스트 업무 절차가 없어 일부 현업부서에서 인수테스트를 실시하지 않고 운영시스템에 프로그램을 반영하는 사례가 있어 프로그램 오류 등으로 인한 전산장애가 발생할 우려가 있으므로

○ 인수테스트 요청절차, 운영시스템 반영 전 부서장 승인 등을 포함한 인수테스트 업무 절차를 마련하는 등 프로그램 인수테스트 업무 처리 절차를 개선할 필요가 있음

(10) 이상거래탐지시스템(FDS) 운영 강화

□ 전자금융사고 예방을 위해 전자금융거래 중 이상거래를 탐지하는 이상거래탐지시스템(FDS)을 구축·운용하고 있으나

○ 이상거래탐지 차단 정책 등록·변경 시 책임자 승인 및 영향도

분석을 수행하지 않아 검증되지 않은 차단정책으로 인해 이상 거래로 오인식되거나, 거래가 차단되어 예상치 않은 장애가 발생할 소지가 있으므로

○ 정책 등록·변경 시 정책 적용에 대한 영향도 분석을 실시하고, 책임자 승인 절차를 시스템에 반영하는 등 운영 절차를 강화할 필요가 있음

(11) 기술지원 종료 운영체제 사용 및 노후 장비 관리 강화

□ 정보처리시스템 총 xxx대는 제조사의 기술지원이 종료된 운영체제가 설치되어 있거나 노후 장비로,

○ 기술지원이 종료된 운영체제에 대한 신규 취약점 보완 및 기능 개선 등을 위한 보정(patch) 작업이 곤란하여 미보완 취약점을 이용한 해킹, 악성코드 감염 등 침해사고가 발생하거나 노후된 장비로 인한 장애 발생 가능성이 있으므로

○ 기술지원이 종료되었거나 노후된 장비의 구체적인 전환계획을 수립하고 전환 전까지 보완대책을 마련·운용할 필요가 있음

(12) 정보처리시스템 성능관리 강화

□ 정보처리시스템(서버, DB, 네트워크, 보안 등)에 대한 성능 관리 및 장애 예방을 위하여 성능관리솔루션을 도입하고 CPU, 메모리, 백업 용량 등 시스템의 상태를 실시간으로 모니터링하며 매월 정기적으로 이용도 등을 분석을 하고 있으나

○ 임계치를 초과하였음에도 원인을 분석하지 않고 증설 검토를 수행하지 않는 경우가 있고, 증설 검토 기준이 없어 CPU 증설 직후에도 임계치를 초과하는 등 정보처리시스템 증설 업무가 체계적으로 관리되지 않으며

○ 동일 장애 유형이 상이한 기준(Warning, Info 등)으로 등록되고, 알림 메시지가 현행화되어 있지 않는 등 장애 발생 시 적시 대응이 어려울 소지가 있으므로

○ 월 운영보고 시 임계치를 초과하는 경우 원인을 분석하여 증설 필요 여부를 검토하고, 증설 검토 기준을 재정립하여 매뉴얼에 추가하는 한편

○ 실시간 모니터링 알람 시스템의 대상 이벤트를 일제 점검하여 메시지 수준을 통일하고 내용을 현행화하는 등 정보처리시스템 성능관리 체계를 강화할 필요가 있음

(13) 정보처리시스템 가용성 관리 강화

□ 프로그램 변경 시 정보처리시스템에 대한 가용성 확보를 위해 자체 수요예측을 하여 최대 처리 용량을 산정하고 있으나

○ 자체 수요 예측 후 산정한 최대처리용량이 실제 접속자 수보다 낮게 예측되는 사례가 있어 이용자 접속 과다로 인한 업무 처리가 지연될 우려가 있으므로

○ 전자금융 업무 관련 프로그램 변경 시 정보처리시스템에 대한 가용성 확보를 위한 자체 수요예측 산정 방식을 개선하고,

○ 공모주 청약 등 일반 업무와 실시간 거래가 필요한 주문·체결 업무가 동일한 정보처리시스템에서 수행되어 공모주 청약 등 일반 업무에 다수 이용자가 접속할 경우 실시간 거래가 필요한 주문·체결 업무에 영향을 미칠 수 있으므로

○ 일반 업무의 부하로 인해 주문·체결 업무에 영향을 주지 않도록 동시 접속 인원수를 통제하거나, 일반 업무와 주문·체결 업무를 분리하는 등 정보처리시스템의 가용성을 보장할 수 있는 방안을 마련할 필요가 있음

(14) 정보처리시스템 접근 계정 관리 미흡

□ 정보처리시스템 접근 계정 정기점검을 정기적으로 수행하고 공용계정 발급 시 보안부서 승인 절차를 마련하고 있으나

○ 정기점검 주기가 반기로 길고 공용계정의 적정성은 정기적으로 점검하고 있지 않으며 인사이동 시 명확한 계정 회수 절차가 정립되지 않아 불필요 계정이 장기간 잔존할 가능성이 높으므로

○ 공용계정을 포함한 접근 계정 정기점검을 단축하여 실시하고 인사이동 시 계정 회수 절차를 명확히 마련하는 등 정보처리시스템 접근 계정 관리를 강화할 필요가 있음

(15) 중요단말기 지정·통제 방식 불합리

□ 삼성증권㈜ 내규 「xxxxxxx지침」에 따라 서버, DBMS 등 정보처리시스템에 직접 접근하는 단말기는 중요단말기로 지정하여 해당 업무 이외의 용도로는 사용할 수 없도록 하고 그룹웨어 접속을 차단하는 등 강화된 보안 정책을 적용하여 관리하고 있으나

○ 단순 데이터 조회를 목적으로 정보처리시스템에 직접 접근하는 현업 부서의 일부 단말기(xx대)를 중요단말기로 지정하지 않았으며, 중요단말기에서 내부 업무 시스템 접속이 가능한 경우가 있는 등 중요단말기 운용 및 통제가 내규와 부합하지 않으므로

○ 단순 데이터 조회를 목적으로 정보처리시스템에 대한 직접 접속하는 단말기는 내규를 준수하여 중요단말기로 지정하고 중요단말기에서의 내부 업무용 시스템 접속을 차단하는 등 중요단말기 통제를 강화할 필요가 있음

(16) 외부 인터넷 접속 통제 불합리

□ 내부 업무용 단말기에 대한 인터넷 접근 예외 적용 시 업무 연관성을 고려하여 정보보호위원회 승인 후 접속을 허용하고 있으나

○ 기 승인된 사이트의 경우 추가적인 정보보호위원회 승인 절차 없이 보안부서의 승인만을 득한 후 접속을 허용하고 있어 업무 연관성이 없는 업무에 대해서도 접근이 허용될 가능성이 있으므로

○ 인터넷 접근 예외 허용 내역을 점검하여 기 승인된 사이트에 대한 예외 허용 부서를 명시하는 한편, 정보보호위원회의 인터넷 접근 예외 승인 시 예외 허용 부서를 명시하여 승인하고 예외 허용 부서의 추가가 필요한 경우 정보보호위원회 승인을 통해 추가하는 등 내부 업무용 단말기의 인터넷 접근 통제를 강화할 필요가 있음