제재내용 공개안

1. 금융기관명 : 신한투자증권㈜

2. 제재조치일 : 2024. 6. 7.

3. 조치 내용

대상	내용
기 관	경영유의사항 1건, 개선사항 3건

4. 조치대상사실

가. 경영유의사항

(1) IT감사 및 IT자체감사 업무 강화

(가) IT부문 정기감사 생략시 내규 준수 필요

회사 내규 「IT감사지침」에 따라 IT부문* 정기감사는 감사(감사위원회)의 명령을 받아 연 1회 실시함을 원칙으로 하며, 정기감사를 생략하고자 하는 경우 감사(감사위원회)의 승인을 받아야 한다.

* IT감사의 피감부서는 ICT본부 및 정보보호본부에 속해 있는 부서

하지만 감사실은 2020.1.1.부터 2023.9.8.까지 ICT본부와 정보보호본부에 대한 정기감사를 격년 주기로 실시하면서 생략*한 정기감사에 대해 감사(감사위원회)의 승인을 받지 않았다.

* ICT본부(2021년) 및 정보보호본부(2020년 및 2022년) 정기감사 미실시

<조치할 사항>
따라서 회사는 「IT감사지침」의 정기감사 수행주기를 감사운용 현황에 맞도록 개정하거나 IT부문에 대한 정기감사를 생략하는 경우에는 감사(감사위원회)의 승인을 명확히 받는 등 내규를 준수하여 운영하시기 바랍니다.

(나) IT부문 수시감사 강화 필요

회사 내규 「IT감사지침」에 수시감사는 IT 관련사고가 발생하거나, IT 업무 수행에 있어 발생 빈도가 높거나 사고 발생시 위험이 큰 사항들에 대하여 수시로 감사(감사위원회)의 명령을 받아 실시할 수 있다.

하지만 감사실은 2020.1.1.부터 2023.9.8.까지 IT부문에서 ○○건의 전산장애가 발생하였으나, 수시감사를 실시한 사례는 장애 ○건에 대한 수시감사 ○회에 그쳤다.

<조치할 사항>
따라서 회사는 IT부문 사고, 장애 또는 제보사항 등에 대하여 필요시 감사보조조직이 자체적으로 수시감사를 실시할 수 있는 객관적인 기준을 마련하여 내규에 반영하고, 동 기준에 부합하는 사항에 대해서는 수시감사를 실시하는 등 IT부문 수시감사를 강화하여 운영하시기 바랍니다.

(다) IT감사 업무편람 마련 필요

IT감사와 관련하여 감사실은 「IT감사지침」, ICT본부는 「ICT자체감사절차」 및 「ICT자체감사매뉴얼」을 마련*하고 있다.

* 정보보호본부는 「보안점검 관리 절차」 '6. 감사'에 「ICT자체감사절차」를 준용하도록 규정

하지만 감사실, ICT본부 및 정보보호본부는 감사(정기, 일상, 수시 등)시 감사항목, 감사내용, 감사대상, 감사절차, 관련부서 및 관련규정 등의 내용을 포함한 IT감사 관련 업무편람을 마련하고 있지 않아* IT감사인 또는 IT부서 자체감사요원 변경 시 일관된 감사체계를 운용하기에 미흡하다.

* (예시) 감사실(IT감사 업무편람), ICT본부(ICT자체감사 업무편람), 정보보호본부(정보보호자체감사 업무편람)

<조치할 사항>
따라서 회사는 감사보조조직별로 IT감사 관련 업무편람을 마련하고, 신규 시스템 도입 및 업무 변동 등이 있는 경우 관련 업무편람을 개정하는 등 IT감사인 또는 IT부서 자체감사요원 변경 시에도 일관된 감사체계를 유지・운용하시기 바랍니다.

(라) IT자체감사인 지정시 내규 준수 필요

회사 내규 「IT감사지침」에 IT부서 자체감사요원은 IT부문 본부장이 지정하며, 지정사항을 감사담당부서(감사실)에 통보하여야 한다.

하지만 ICT본부 및 정보보호본부는 2020.1.1.부터 2023.9.8.까지의 기간 중 조직개편 및 인사 이동 등으로 IT부서 자체감사요원이 변경되었음에도 감사실에 통보하지 않았다.

<조치할 사항>
따라서 ICT본부 및 정보보호본부는 변경된 IT부서 자체감사요원의 자격(경력)요건 및 감사대상 업무로부터 독립성 등을 감사실이 검증할 수 있도록 감사인 지정사항을 통보하는 등 내규를 준수하여 운영하시기 바랍니다.

(관련부서 : 감사실, ICT본부, 정보보호본부)

나. 개선사항

(1) 프로그램 긴급변경 절차 강화

회사는 내규「ICT응용프로그램유지보수절차」및「ICT시스템변경관리절차」등을 통해 프로그램 변경·통제 절차를 마련하여 프로그램 긴급처리 및 사후관리 등을 운영하고 있으나 아래와 같이 프로그램 긴급변경 절차를 개선할 필요가 있다.

(가) 긴급처리 승인절차 개선

내규에서 긴급처리는 고객서비스에 대한 장애처리, 장애 예방을 위한 긴급한 업무처리의 경우로 제한하였으나 긴급처리 사유 및 작업내용 등에 프로그램 변경 내용과 무관한 내용*을 기재해도 부서장이 승인하는 등 프로그램 긴급 변경 절차를 오남용할 우려가 있다.

* “수정. 반영”, “골드넷 바탕화면” 등

<조치할 사항>
따라서 긴급처리의 목적인 장애 처리 및 예방의 경우에만 이용될 수 있도록 내규에 긴급처리 항목 예시 및 전자금융거래 등 중요 프로그램의 범위 등을 수립하여 구체화하시기 바랍니다.

(나) 중요 프로그램 긴급처리 절차 마련

내규에서 중요 프로그램의 기준을 수립하지 않아 전자금융거래와 관련된 프로그램과 내부 프로그램 오류 수정 등과 같은 대고객서비스와 무관한 프로그램 간의 긴급변경 통제절차가 동일*하므로 중요 프로그램 사후관리가 미흡하다.

* 대고객서비스를 제공하는 전자금융거래 관련 프로그램 등에 대해서는 통제절차를 강화하여 구분 필요

<조치할 사항>
따라서 전자금융거래와 관련된 중요 프로그램 기준을 수립하여 별도의 긴급처리 절차를 마련하는 등 긴급변경 업무처리 통제를 강화하시기 바랍니다.

(관련부서 : ICT본부)

(2) 전산원장 통제 절차 강화

회사는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 변경대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등을 포함한 내규 「ICT데이터관리절차」 및 「원장변경 관련 업무처리 매뉴얼」을 수립·운용하고 있으나 아래와 같이 전산원장 통제 절차를 개선할 필요가 있다.

(가) 중요 원장 지정기준 및 지정 적정성 검토 절차 개선

회사는 중요거래 정보에 대한 무결성 확보 및 금융사고 발생 방지를 위해 ICT 조직과 감사부서가 사전협의하여 '중요 원장'을 지정하고 '중요 원장'의 변경과 관련한 요청은 감사부서에서 검토·승인하는 통제절차를 갖추도록 「원장변경 관련 업무처리 매뉴얼」을 개정(2022.6.20.)하였으며

이에 따라 ○○개 '중요 원장'*을 지정하고 '중요 원장'의 변경 요청시 감사실의 합의를 필히 거치도록 사내에 공지(IT업무게시판, "원장변경관련 업무처리 절차 안내", 2022.10.14.)하여 운영하고 있으나,

* 예수금, 거래내역, 주문·체결, 잔고, 시재, 고객정보에 해당하는 총 ○○개 테이블

관련 내규 등에 '중요 원장' 지정 기준과 '중요 원장' 지정의 적정성을 검토하는 주기 등 세부사항을 정하고 있지 않아 '해외주식 잔고' 등의 주요 거래정보 관련 전산원장이 '중요 원장' 지정시 누락되었으며, 최초 '중요 원장' 선정 이후 추가로 지정이 필요한 테이블 등에 대해 검토를 실시하지 않았다.

* ◇◇◇◇(해외주식 잔고), ◇◇◇◇(해외주식 주문이력) 등

<조치할 사항>

따라서 중요 거래정보를 포함한 전산원장이 내규에서 정한 통제대상에서 누락되지 않도록 '중요 원장'의 지정 기준 및 지정 절차를 세분화하는 등 회사는 '중요 원장' 지정 기준과 지정의 적정성 검토 관련 절차를 개선하여 전산원장 변경통제 절차의 실효성을 제고하시기 바랍니다.

(나) 전산원장 긴급변경의 사후승인 절차 개선

회사는 전산원장 변경 요청시 업무상 긴급상황(예 : 시스템 기능 이상, 또는 고객서비스 시 빠른 안정을 위한 긴급 처리시) 발생의 경우 선 조치 후 원장변경 공문 등*을 첨부하여 사후결재 및 보고하는 절차를 마련하는 등 긴급변경 사유 및 내역에 대한 적정성을 사후적으로 검증토록 하고 있으나

* 현업 요청에 의한 변경시 : 현업의 요청공문, ICT 자체 요청에 의한 변경시 : 원장변경 사유 보고서·장애보고서·오류조치보고서 등

전산원장 변경관리 시스템(◇◇◇) 상 내규에서 정하고 있는 요청 공문 등의 첨부 여부와 상관없이 사후결재 상신이 가능하여 실제 원장 변경 공문 첨부가 누락되었음에도 책임자 사후 승인 및 제3자 확인 결재를 진행하는 등 긴급변경의 세부사유 확인을 적시에 미실시한 사례*가 있다.

* 회사는 자체점검(2023.7.27.)을 통해 검사대상 기간 중 원장변경 공문 등이 미 첨부된 ○○건을 확인, '해외주식 주문 체결시 정정확인 수량 오류관련 정정'(2021.10.1.) 건의 경우 원장변경 공문 첨부없이 원장변경 책임자 및 제3자 승인(2021.10.5.)후 자체점검 시정요구에 따라 공문 결재(2023.7.31.)

<조치할 사항>
전산원장 변경의 사전·사후 승인시 긴급변경의 세부사유* 등을 적시에 확인 가능하도록 내규에서 정하고 있는 절차를 통해서만 승인이 이루어지게 하는 등 시스템을 개선하여 실질적인 검증업무가 실시될 수 있도록 전산원장의 통제 절차를 강화하시기 바랍니다.

* 전산원장 변경관리 시스템 상의 안건 이름, 업무 목적, 작업에 사용된 SQL구문의 확인만으로는 긴급변경과 관련한 당위성·적정성을 검증하기 어려움

(관련부서 : ICT본부)

(3) 일괄작업 운영 및 사후관리 강화

회사는 내규 「ICT전산실운영관리절차」에 일괄작업 관리 절차를 마련하고 일괄작업 통합관리솔루션(◇◇◇◇) 및 일괄작업 자동화솔루션(◇◇◇◇)을 통해 일괄작업의 수행 등을 기록·관리하고 사용자 권한을 그룹 단위로 관리하고 있으나 아래와 같이 일괄작업 운영 및 사후관리 절차를 개선할 필요가 있다.

(가) 일괄작업 운영시스템 권한부여 적정성 검토 강화

일괄작업 자동화솔루션(◇◇◇)상 전산실 운영에 대한 외부주문직원이 관리자 그룹과 동일한 권한*을 가지고 있어 외부주문직원을 통해 관련 책임자 승인 없이 일괄작업이 등록·실행·삭제될 우려가 있다.

* ◇◇◇◇상 사용자 권한을 AdminGroup(신한투자증권, 신한DS 관리자), UpdateGroup(전산실 운영에 대한 신한DS 직원) 및 BrowseGroup(View) 총 3그룹으로 관리하고 있으나, AdminGroup과 UpdateGroup의 권한이 All로 동일하게 부여

<조치할 사항>
따라서 일괄작업 운영 관련 시스템 권한부여 내역을 재점검하여 업무상 필요 범위 외로 부여된 권한은 모두 회수하고 이후 주기적으로 일괄작업 운영시스템 권한의 적정성에 대한 점검을 강화하시기 바랍니다.

(나) 일괄작업 운영관리(모니터링) 절차 개선

정기적으로 수행하는 일괄작업의 개별 작업 단위(Job)별로 관련 담당자가 수행시간 임계치를 설정하여 임계치를 초과하는 일괄작업의 경우 알림 발생 등을 통해 담당자가 재수행 등의 조치를 하고 있으나,

최근 평균 수행시간이 주기적으로 임계치에 근접하는 등 임계치를 초과하여 오류 발생 우려가 있는 일괄작업에 대해 원인분석 절차가 마련되어 있지 않는 등 일괄작업에 대한 운영관리가 일부 미흡하다.

<조치할 사항>
따라서 평균 수행시간이 임계치에 근접하는 등 오류 발생 위험도가 높은 일괄작업에 대한 구분 기준을 내규 등에 수립하고 동 기준에 따라 고위험 일괄작업으로 분류되는 경우 원인분석 및 수행 결과의 적정성을 점검하도록 일괄작업의 모니터링 절차를 강화하시기 바랍니다.

(다) 일괄작업 사후관리 절차 개선

내부업무처리 시스템 '◇◇◇'을 통해 일괄작업*을 수행하는 경우 일괄작업 통합관리솔루션(◇◇◇◇)을 거치지 않고 수행되어 오류 발생 시 책임자 확인 절차가 시스템상 강제화되지 않는 등 일괄작업의 사후관리가 미흡하다.

* 일괄작업 자동화솔루션(◇◇◇◇)을 통해 수행하는 정기적인 일괄작업이 아닌 담당 부서의 요구사항이 있는 경우에만 수행하는 일괄작업(On-Demand 일괄작업)

<조치할 사항>

따라서 회사는 내부업무처리 시스템을 통해 수행되는 일괄작업에서 오류가 발생하는 경우 책임자의 확인 절차가 강제화 되도록 관련 시스템을 개선하시기 바랍니다.

(관련부서 : ICT기획운영부)