제재내용 공개안

1. 금융기관명 : NH선물㈜

2. 제재조치일 : 2024. 7. 30.

3. 조치 내용

대상	내용
기 관	경영유의사항 1건, 개선사항 3건

4. 조치대상사실

가. 경영유의사항

(1). IT감사 및 IT자체감사 업무 강화

(가) IT부문 특별감사 실시 필요

회사 내규「감사위원회직무 규정」에 따르면 특별감사는 특정사안에 대하여 감사위원회*의 재량에 따라 ①감사위원회가 필요하다고 인정하는 경우, ②대표이사의 요청이 있는 경우, ③감독기관의 지시가 있는 경우 비정기적으로 실시해야 한다.

* 사외이사(비상임) 3인으로 구성

하지만 2020.1.1.부터 2023.9.1.까지 회사의 장애관리대장에 등록된 70건의 장애 중 15건(21.4%)의 1등급 장애가 발생하였음에도 동 사실이 감사위원 및 대표이사 등에게 보고되지 않는 등의 사유로 특별감사가 실시되지 않았다.

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

(나) IT감사인의 자격요건 준수 필요

회사 내규 「감사위원회직무 규정」의 '감사인의 자격'에 감사인 임명원칙과 임명 불가자 등에 대하여 규정하고 있다.

하지만 2020.1.1.부터 2023.9.1.까지 감사보조조직이 실시한 총 4회의 종합감사에서 IT 관련 학력 또는 경력이 없는 감사인이 IT부문 감사를 수행한 사실이 있다.

<조치할 사항>
따라서 회사는 IT감사인의 자격요건을 상세화하여 내규에 반영하고, 동 자격요건을 갖춘 IT감사 전문인력을 감사보조조직에 확보하여 IT부문 감사 업무를 운영하시기 바랍니다.

(다) IT부문 자체감사의 실효성 확보 필요

IT부서 자체감사요원(OO팀 직원 1명)을 지정하여 IT 및 정보보호 부문에 대한 자체감사 업무를 수행하고 있다.

하지만 IT부서 자체감사요원이 IT부문 업무(90%)를 겸직하고 있어 자체감사 업무의 독립성 확보가 곤란하며, IT자체감사 점검항목이 대부분 통계 또는 형식 준수 여부만 확인하는 수준으로 시행되고 있어 IT 자체감사의 실효성이 부족한 상황이다.

<조치할 사항>
따라서 회사는 IT 및 정보보호 업무에 대한 IT부서 자체감사요원의 지정, 자체감사 실시기준 등을 내규에 반영하고, IT자체감사 업무편람을 마련하는 등 IT자체감사의 실효성을 확보하여 운영하시기 바랍니다.

나. 개선사항

(1) 프로그램 변경 절차 강화

NH선물㈜는 내규 「IT변경관리 준칙」 및 형상관리시스템(OOOOO) 등을 통해 프로그램 변경·통제 절차를 마련하여 운영하고 있으나 아래와 같이 프로그램 변경·통제 절차를 강화할 필요가 있다.

(가) 프로그램 테스트 절차 개선

프로그램 변경과 관련하여 내규에 단순 테스트 절차*만 수립되어 있고 구체적인 테스트 시나리오 작성 기준이 마련되어 있지 않으며, 프로그램 테스트 시 내규에 현업 부서의 확인을 받는 절차가 미흡하여 테스트 및 테스트 결과의 적정성 검토가 미흡할 우려가 있다.

* 단위 테스트, 결합 테스트, 과부하 및 성능 테스트, 사용자 승인 테스트

<조치할 사항>
따라서 회사는 프로그램 테스트가 적정하게 이뤄지도록 테스트 시나리오 기준 등*을 마련하고, 담당 부서장 및 현업부서의 확인을 거쳐 최종적으로 형상관리 시스템에 등록 후 배포하도록 절차를 개선하시기 바랍니다.

* 개발 시 테스트 시나리오 범위 수립 후 테스트 데이터 변환 시 변환항목, 사용목적 등을 기재하여 테스트가 적정하게 완료되었는지 검토 등

(나) 형상관리시스템 관련 내규 개선

형상관리시스템(OOOOO)에 대해 단순 개발자·관리자·사용자 가이드만 관리하여 운영하고 내규에는 형상관리시스템 적용절차·범위를 마련하지 않아 프로그램 변경 시 형상관리시스템 적용을 누락할 우려가 있고,

전자금융거래와 관련된 중요 프로그램 소스코드에 대하여 형상관리시스템 내 개발시스템 소스코드와 운영시스템 소스코드 전후 비교 등 간단한 분석은 진행하고 있으나, 보안 취약점 제거 등 세부적인 분석을 수행하지 않아 소스코드 관리가 미흡할 우려가 있다.

<조치할 사항>
따라서 프로그램 개발, 테스트 및 배포 등을 위한 형상관리시스템 적용범위·절차 관련 내규를 제정하고, 소스코드 정밀 분석을 위한 별도 방안을 마련하여 정보계(FEP/HTS), 계정계(원장), 클라이언트(HTS) 등 중요 프로그램의 요구사항 관리 및 변경통제를 강화하시기 바랍니다.

(다) 최종 검증 수행절차 마련

테스트가 완료된 전자금융거래와 관련된 중요 프로그램에 대하여 변경승인 절차 등만 마련하고 운영시스템 배포 전 운영시스템과 동일한 인프라 환경을 마련하여 최종 검증을 수행하지 않아 장애가 발생할 우려가 있다.

<조치할 사항>
따라서 장애 발생 최소화를 위해 변경된 프로그램을 운영시스템으로 최종 반영 전 별도 검증 가능한 인프라 환경을 구축 후 사전에 소스코드 취약점 등을 점검하여 프로그램 변경통제 절차를 강화하시기 바랍니다.

(2) 전산원장 통제 절차 강화

NH선물㈜는 내규「변경관리 준칙」에 의하여 전산원장의 변경·통제 절차를 수립하여 운영하고 있으나 아래와 같이 전산원장 통제 절차를 개선할 필요가 있다.

(가) 전산원장 변경 시 통제대상 판단 세부기준 마련

변경 통제의 대상이 되는 전산원장의 기준을 정하고 있지 아니하여 전산원장 변경업무가 금전거래 정보·고객정보 등과 무관한 일반 데이터 정정업무 및 시스템 변경업무와 미분리되어 운영되는 등 중요정보에 대한 관리 효율성이 저하되는 측면이 있다.

<조치할 사항>
따라서 회사는 변경 통제의 대상이 되는 전산원장의 세부기준을 내규에 반영하여 일반 데이터 정정·시스템 변경 업무와는 구분하여 운영될 수 있도록 전산원장 통제체계를 개선하시기 바랍니다.

(나) 전산원장 변경관리 절차 전산화

내규「변경관리 준칙」에 따라 전산원장 변경 요청시 동 내규의 '별지서식 1호(원장 변경 요청서)'를 이용한 수기결재를 통해 변경요청·책임자 승인·제3자 검증 등의 절차를 이행하고, 변경완료 이후 적정성 검증 실시내역도 수기로 관리하고 있어서 내규에서 정하고 있는 전산원장 변경절차가 누락되거나 순서대로 이행되지 않을 우려가 있고 실제 회사의 내부감사를 통해 절차 누락 관련 사항이 반복지적*되고 있다.

* 2021년, 2022년 내부종합감사시 '원장변경시 컴플라이언스 팀장의 승인 누락' 지적사항 반복

<조치할 사항>
따라서 전산원장 변경 관련 절차를 전산화하는 등 관리체계를 강화하시기 바랍니다.

(다) 전산원장 변경 관련 사후관리 절차 준수

내규「변경관리 준칙」에서 월별로 '로그내역'과 '프로그램 변경업무 증빙자료'를 통해 주관팀장이 원장변경 내용의 적절성을 확인토록 정하고 있으나, 주관팀장(OO팀장)은 실제 월별 원장변경 건수 등만 파악하고 변경 작업 관련 '로그내역' 및 '프로그램 변경업무 증빙자료' 등 변경작업에 대한 적절성 여부는 확인하지 않는 등 원장변경 관련 사후관리 업무처리가 부적정하게 이루어지고 있다.

<조치할 사항>
따라서 전산원장 등 중요정보의 무결성을 확보할 수 있도록 내규에서 정하고 있는 원장변경 관련 절차를 철저히 준수토록 주의할 필요가 있고, IT감사시 주기적으로 전산원장 변경과 관련한 적정성 여부를 확인할 수 있는 체계를 마련하시기 바랍니다.

(3) 일괄작업 통제 절차 강화

NH선물㈜는 내규「변경관리 준칙」및 일괄작업 관리시스템 등을 통해 일괄작업 프로그램의 등록·변경·삭제 및 실행 등을 통제하고 있으나 아래와 같이 일괄작업 통제 절차를 강화할 필요가 있다.

(가) 일괄작업 서버 분리

모든 정기 일괄작업의 수행을 일괄작업 전용 서버가 아닌 계정계 원장 관련 서버에서 하고 있어 일괄작업 작업 수행과정에서 오류가 발생할 경우 전자금융거래가 지연 또는 중단되는 장애가 발생할 우려가 있다.

<조치할 사항>
따라서 일괄작업 수행이 계정계 원장 관련 서버 등 중요 서버에서 수행되지 않도록 별도 서버를 구축하여 동 서버에서만 일괄작업이 수행되도록 일괄작업의 운영·관리를 강화하시기 바랍니다.

(나) 일괄작업 관리시스템 권한부여 적정성 검토 강화

일괄작업 관리시스템 내에 응용프로그램 개발·운영 담당자에게 일괄작업 등록·삭제가 가능하도록 권한이 부여*되어 있어 일괄작업 담당자 외에도 일괄작업을 등록·삭제할 우려가 있다.

* 일괄작업 관리시스템의 권한관리를 업무담당자 직원단위가 아닌 팀단위(OO팀)로 설정하여 관리

<조치할 사항>
따라서 일괄작업 관리시스템에 대한 권한부여는 일괄작업 등록·삭제 담당자로 제한하여 동 담당자가 책임자의 사전 승인 이후에만 일괄작업 등록·삭제가 가능하도록 관련 절차를 개선하시기 바랍니다.

(다) 일괄작업 관련 오류 유형별 처리절차 마련

일괄작업 수행 결과 동일한 오류가 지속적으로 발생하고 있음에도 오류 유형별 처리 절차가 내규 등에 부재하여 단순 재수행하여 해당 오류를 해결하고 있다.

<조치할 사항>
일괄작업 관련 오류 유형별 처리 절차를 내규 등에 마련하여 일괄작업 수행 결과 동일한 오류가 지속적으로 발생하는 경우 원인분석 및 관련 프로그램 개선 등을 통해 일괄작업의 오류 발생을 최소화시기 바랍니다.

(라) 야간·휴일 일괄작업 오류 관련 기록·관리체제 마련

야간 또는 휴일 일괄작업 수행과정에서 오류가 발생*하는 경우 오류 원인 및 책임자의 확인 여부를 구체적으로 기록·관리하지 않는 등 관리체계가 미흡하다.

* 일괄작업 오류 발생 시 관련 부서(OO팀, OO팀 등)에게 알림 및 문자(SMS) 발송

<조치할 사항>

야간 또는 휴일 일괄작업 오류 등으로 재처리를 하는 경우 오류의 원인 및 책임자 확인 여부가 기록·관리될 수 있도록 관련 절차를 개선하시기 바랍니다.