제재내용 공개안

1. 금융회사명 : 수협은행

2. 제재조치일 : 2019. 11. 26.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 2건, 개선사항 14건

4. 제재대상사실

가. 경영유의사항

(1) IT자체감사업무 독립성 강화

은행 IT부서에 대한 자체감사업무는 △△그룹과 ▽▽▽▽본부가 각각 수행토록 하고 있으나,

△△그룹은 자체감사자가 감사대상 업무인 감리, 리스크관리 등의 업무를 함께 수행하고 있어 동 업무에 대한 직무가 분리되지 않았고, 자체감사업무에 대한 통제 및 자체감사자의 업무성과 평가절차에 감사대상업무를 수행하는 □□□□팀장 및 ◇◇◇◇부장이 포함되어 있으며,

▽▽▽▽본부도 자체감사자가 감사대상 업무인 IT외주인력 보안관리, 사이버보안관제센터 유지관리, 중요단말기 관리 등의 업무를 함께 수행하고 있어 동 업무에 대한 직무가 분리되지 않았고, 자체감사업무에 대한 통제 및 자체감사자의 업무성과 평가절차에 감사대상업무를 수행하는 ◈◈◈◈팀장이 포함되어 있으며, 자체감사 관련 내규가 마련되어 있지 않는 등 IT자체감사 업무체계가 미흡하므로,

IT부서 자체감사업무에 대한 내규 및 관리체계를 정비하여 자체감사자가 감사 대상 업무를 함께 수행하지 않도록 직무를 분리하고, 자체감사업무에 대해

서는 CIO·CISO가 직접 통제토록 하며, 자체감사자에 대한 업무성과 평가 시 감사대상 업무 수행조직의 부서장 등은 평가에서 배제하는 등 IT자체감사업무의 독립성을 강화하시기 바람

(2) IT업무 연속성 계획의 실효성 강화

재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 총 00개 단위업무 중 00개 업무를 핵심업무로 선정하였으나,

전사적 업무 영향도에 대한 분석·평가를 실시하지 않아 ㅇㅇ그룹에서 선정한 핵심업무(00개)가 전사적 업무 영향도를 반영하지 않고 있으며, 핵심업무 중 00개 업무에 대한 재해복구시스템이 구축되지 않아 주전산센터 재해 발생 시 일부 핵심업무 및 중요업무가 중단될 우려가 있으므로,

향후 전사적 업무 영향도 분석·평가 결과를 검토·반영하여 IT업무 연속성 계획을 수립하는 절차를 마련하는 한편, 핵심업무 관련 재해복구시스템 구축계획을 조속히 수립하여 수행하는 등 업무 연속성 계획의 실효성을 확보하시기 바람

나. 개선사항

(1) IT투자비용 대비 효과분석 미흡

IT자본예산 투자사업에 대하여 사업완료 후 6개월 이후부터 IT투자비용 대비 효과분석을 실시(최근 0년간 0건)하고 있으나,

효과분석 대상 및 시기 등을 구체적으로 내규에 명시하고 있지 않아 중요사업에 대한 효과분석 누락 등 업무 실효성이 저하될 소지가 있으므로,

앞으로 IT투자비용 대비 효과분석의 대상 및 시기 등을 구체적으로 내규에 명문화하는 등 개선하시기 바람

(2) 노후PC 불용처리절차 미흡

내용연수가 경과된 노후PC의 불용처리 시, 정보유출 방지 등을 위하여 데이터저장장치(HDD 등)는 PC에서 분리·송부하고 폐기전문업체를 통해 물리적으로 파기(파쇄)하고 있으나,

PC의 데이터저장장치(HDD 등) 일련번호 등을 관리하고 있지 않아 제출된 데이터저장장치(HDD 등)의 원본 진위여부를 확인할 수 없어 임의의 데이터저장장치 제출 등으로 정보유출 우려가 있으므로,

앞으로 노후PC 불용처리 시 최초 지급된 PC의 데이터저장장치(HDD 등) 원본 진위여부를 확인할 수 있도록 업무를 개선하시기 바람

(3) 전산감리 실효성 미흡

내규에 전산감리 대상사업 기준을 마련하고 있으나,

감리대상을 사업금액 규모로만 판단하여 감리실적이 저조하고 감리예산을 사전에 확보하고 있지 않는 등 전산감리의 실효성이 저하될 우려가 있으므로,

앞으로 실효성있는 전산감리가 시행될 수 있도록 감리대상 기준인 사업금액 기준을 적정하게 조정하거나 사업 추진 시 내부협의회 사전심의 단계에서 감리 필요성을 검토하도록 내규를 개선하는 한편, 감리예산을 전년도에 확보할 수 있도록 관련 업무를 개선하시기 바람

(4) 정보처리시스템 폐기 절차 불합리

정보처리시스템 폐기 시, ㉠㉠그룹은 현업 부서와 업무협의를 통해 서비스 종료 관련 업무*를 처리하고 있으나,

* 시스템 유지보수 계약 정리 등

정보처리시스템 폐기에 관한 표준화된 업무처리 절차가 마련되어 있지 않고, ㉠㉠그룹과 ㉡㉡㉡㉡본부 간 정보공유가 이루어지지 않아 일부 사용 종료된 홈페이지의 불필요한 시스템 접속 및 에러메세지 등을 제한없이 노출한 사례가 있으므로,

앞으로 정보처리시스템 폐기 시, 조치필요사항*에 대한 업무처리 절차를 마련하고 ㉠㉠그룹과 ㉡㉡㉡㉡본부 간 정보공유 강화방안을 수립·운용하는 등 정보처리시스템 폐기 절차를 개선하시기 바람

* 시스템 접속 차단, 주요 데이터 이관·백업·삭제 확인, 정보보호시스템 관련 정책 변경 등

(5) 일괄작업 관리통제 미흡

내규에 일괄작업관리자(Job Scheduler)의 임무 등을 규정하고 ⛝⛝⛝⛝시스템을 운영하여 일괄작업을 통제하고 있으나,

일괄작업 처리결과를 관리하지 않아 일부 작업이 반복적으로 오류가 발생하고 있는 등 사고발생 우려가 있으므로,

앞으로 주기적으로 일괄작업 처리결과를 점검하여 동일한 오류가 지속·반복적으로 발생하는 프로그램에 대해 신속한 조치*를 실시하는 등 관련 업무 및 시스템을 개선하여 일괄작업의 관리통제를 개선하시기 바람

* 에러발생현황 통보, 개선 가능여부 조사 및 조치요구 등

(6) 프로그램 등록관리 절차 미흡

내규에 따라 프로그램 등록관리 업무를 수행하고 있으나,

프로그램 긴급변경 시 긴급변경 적용대상*이 명확하지 않고 긴급적용 시행시 필요한 「◆◆◆ 매뉴얼」도 마련되어 있지 않으며, 운영시스템 이관 시 소스코드 검사 등 중요사항에 대한 사전점검을 실시하지 않고 있어 프로그램 변경 오류 등으로 인한 사고발생 우려가 있으므로,

* 대고객서비스 중단 및 중대한 오류 등

앞으로 구체적인 긴급변경 적용대상 업무 선정기준을 마련하여 이를 포함한 「◆◆◆ 매뉴얼」을 제정하는 등 관련 업무절차를 마련하고, 운영시스템 이관 시 사전점검* 기능을 형상관리시스템에 추가하는 등 관련 업무를 개선하시기 바람

* 소스코드 인스펙션, 하드코딩 검출, 테스트 커버리지 등

(7) 테스트데이터 변환 절차 미흡

프로그램 테스트를 위해 주민등록번호 등 개인정보가 포함된 데이터는 테스트데이터 변환시스템을 사용하여 변환하고 있으나,

테스트 담당자(개발자)가 개인정보가 포함된 데이터(DB컬럼 등)를 직접 선택하여 수동으로 변환하고 있어 고의 또는 과실에 의해 데이터가 누락될 우려가 있으므로,

앞으로 개인정보가 포함된 데이터(DB 컬럼 등)는 메타데이터시스템 등을 통하여 통합관리하고, 테스트데이터 변환 시 동 통합관리시스템과 테스트데이터 변환시스템이 자동 연동되어 변환될 수 있도록 관련 절차를 개선하시기 바람

(8) IP주소 관리 미흡

IP주소 관리정책을 기반으로 네트워크를 분리하여 IP주소를 사용하고 있으나,

일부 외부직원이 내부직원용 IP주소 대역을 사용하고 개발서버와 운영서버가 동일한 IP주소 대역에서 운영되는 등 IP주소 관리가 미흡하므로

앞으로 외부직원은 외부직원 전용 IP주소 대역을 사용하고 개발서버와 운영서버 등 업무특성별로 IP주소 대역을 분리하여 운영하시기 바람

(9) 단말기 통신망 관리 절차 미흡

「□□□□□□□법」제000조의0에 따라 수협은행은 ◈◈◈ 및 ◈◈ 전산시스템의 위탁운영 및 관리업무를 수행하고 있으나,

검사착수일 현재 수협은행 및 ◈◈◈, ◈◈의 단말기가 동일한 통신망을 사용하고 있어 단말기 간 비인가 통신에 의한 정보유출 등 사고발생의 우려가 있으므로,

앞으로 법인별 단말기 통신망을 분리하거나 단말기 간 비인가 통신 등을 차단할 수 있는 통제방안을 마련하여 이행하시기 바람

(10) 무선통신망 차단시스템 관리 미흡

모바일앱 개발 및 테스트 등을 위해 무선통신망을 구축하고 비인가 무선망 사용을 통제하기 위하여 무선침입방지시스템(WIPS*)를 구축·운영하고 있으나,

* Wireless Intrusion Prevention System

무선침입방지시스템 노후화로 최신 무선통신 규격에 대한 탐지·차단기능이 제공되지 않아 비인가 무선기기 사용 및 내부시스템 침해사고 등이 발생할 우려가 있으므로

앞으로 보안기능이 강화된 무선침입방지시스템을 구축하여 무선통신망에 대한 보안성 관리를 개선하시기 바람

(11) ◈◈▣ PC 관리통제 미흡

업무용 PC 등 전산기기는 ◒◒◒◒시스템에 등록하여 관리하고 있으나,

◒◒◒◒시스템에서 ◈◈▣ PC를 식별할 수 없으며, 스마트뱅킹 앱 개발 등의 목적으로 사용중인 ◈◈▣ PC에 보안솔루션*이 설치되지 않은 상태에서 외부통신망(ADSL) 환경에서 사용되는 등 정보자산 관리 및 보안통제가 미흡하므로,

* 매체제어솔루션, 네트워크접근통제시스템(NAC), 바이러스 백신 프로그램 등

앞으로 ◈◈▣ PC 등 ◒◒◒◒시스템에서 식별되지 않는 전산기기에 대한 자산관리를 실시하고, ◈◈▣ PC 등에 대해서 내부정보 유출 및 악성코드 유입 등을 막을 수 있는 보안솔루션을 설치·운용하시기 바람

(12) ▽△◎시스템 운영 미흡

2016.12월 수협중앙회의 ◕◕◕◕부문을 분리하여 수협은행으로 조직을 운영하고 있으나,

양사가 사용하는 ▽△◎시스템을 분리하지 않아 양사 간 공동사용 중인 메신저시스템 등을 통해 별도의 통제절차 없이 은행에서 ◈◈◈로 고객정보가 유출될 우려가 있으므로

앞으로 은행과 ◈◈◈ 간 ▽△◎시스템을 분리하여 구축 및 운용하는 등 ▽△◎시스템 운영을 개선하시기 바람

(13) 이상거래탐지시스템(FDS) 운영 절차 미흡

전자금융사고 예방을 위해 전자금융거래 중 이상거래를 탐지하는 이상거래탐지시스템(FDS*)를 구축·운용하고 있으나,

* Fraud Detection System

FDS시스템 내 이상거래를 탐지하기 위한 정책(00개) 중 00개의 경우 FDS 시스템 구축 이후 검사착수일까지 탐지건수가 전혀 없는 등 이상거래 추출기준의 실효성이 의심되는 상황임에도 추출기준의 적정성 등에 대하여 점검을 실시하지 않고 있으며,

FDS시스템 정책의 등록·변경·삭제에 대한 변경근거 및 책임자 승인 내역과 정책 변경으로 인한 전자금융거래 영향도 분석 등에 대한 상세한 검토절차 등이 마련되어 있지 아니하므로

앞으로 정기적으로 FDS시스템의 운용현황 및 정책의 적정성 등을 유관부서와 공동으로 점검하고, FDS시스템 정책의 등록, 변경 및 삭제에 대한 승인·검토 절차를 마련하는 등 이상거래탐지시스템 운영을 개선하시기 바람

(14) 침입차단시스템 정책 운영 미흡

은행 내부망을 통한 비인가 접속 등 전산실 내 정보처리시스템을 보호하기 위하여 주요 서버 구간별로 침입차단시스템(방화벽)을 구축·운용하고 있으나,

운영 중인 침입차단시스템(방화벽) 총 00대 중 ◇◇◇, ◎◎◎◎ 등 일부 구간 방화벽(00대)의 경우 블랙리스트* 방식으로 운영되고 있어 업무목적 외 불필요한 서비스가 과도하게 접속될 우려가 있으므로

* 위험도가 높은 주요 Well-Known 포트 위주로 차단

앞으로 전산실 내 정보처리시스템을 보호하기 위한 내부 방화벽의 운영방식을 화이트리스트* 방식으로 변경하고, 기 적용된 보안정책을 강화하는 등 관련 시스템 및 통제절차를 개선하시기 바람

* 사전 정의된 정책만 허용되고, 미정의된 정책은 전부 차단