경영유의사항 등 공개안

1. 금융회사명 : 하나캐피탈

2. 조치일 : 2019. 4. 22.

3. 조치내용

대상	내용
기 관	개선사항 4건

4. 조치대상사실

가. 개선사항

(1) IT부문 감사체계 미흡

IT본부 내 IT운영팀 인력 O명을 자체감사자로 선정하고 총 O개 감사항목에 대해 IT부문 자체감사를 수행하고 있으나,

IT부문 자체감사에 대한 수행주기 별 감사항목, 결과보고, 사후관리 등 세부 업무절차가 반영된 내규 또는 지침 등을 마련하지 아니하여

①검사대상기간 중 실시한 감사결과를 감사명령권자(CIO)에게 보고하지 아니하였고, ②시스템 접근통제의 적정성, IT아웃소싱 통제, 고객정보보호 부문 등 정보보호 업무에 대해서는 자체감사를 수행하지 않았으며, ③자체감사자가 IT자체 감사업무 외에 피감업무인 OOO 등의 업무를 겸직 수행하고 있어 자체감사 업무의 독립성이 결여될 우려가 있고, ④IT본부 업무담당자가 일상감사 대상인 총 OOO건 중 OO건에 대해 일상감사를 누락하는 등 IT내부통제가 취약하므로

IT부문 자체감사에 대한 수행주기별 감사항목, 감사방법, 감사결과보고 및 사후관리 절차 등을 포함한 내규 등을 마련하여 IT 및 정보보호 중요업무에 대해 감사를 실시하도록 감사대상 범위를 확대하고, 주기적으로 감사 수행내역의 적정성을 점검하여 그 결과를 CIO에게 보고하는 등 IT부문 자체감사 업무를 개선하시기 바람

(2) 재해복구전환훈련 운영 불합리

내규 「IT서비스 연속성관리 세칙」에 따라 장애 등 비상상황 발생시 시스템 중단시간을 최소화 하는 등 IT서비스의 연속성을 확보할 수 있도록 매년 재해복구전환훈련을 실시하고 있으나,

핵심업무로 지정한 총 OO개 단위업무 중 OOOO, OOOO 등 O개 핵심업무를 제외한 계정계 O개 업무를 대상으로 재해복구전환훈련을 실시하고, 일부 IT직원 및 현업부서가 참여하지 않은 상태로 훈련을 실시하고 있어 비상상황 발생시 실질적인 대응이 곤란하여 고객에게 불편을 초래할 수 있으며

「IT업무연속성 및 비상대응 매뉴얼」에 비상인력의 비상연락망 및 직원별 담당 역할, 백업자료 복구절차, 시스템, 통신망, 최종사용자 컴퓨팅 등 주요 자원에 대한 내용을 포함하지 아니하고, 소산소 등에는 동 매뉴얼을 보관하고 있지 아니하여 비상상황 발생시 신속한 대응이 곤란해질 우려가 있으므로

OOOO 등 OO개 핵심업무에 대해 재해복구전환훈련을 실시하고, 훈련시 IT부서 외에 현업부서가 반드시 참여하도록 하여 IT서비스의 정상가동 여부를 검증하는 한편, 업무연속성 및 비상대응 매뉴얼을 개정하는 등 재해복구전환훈련의 운영을 개선하시기 바람

(3) 전산원장 변경업무 불합리

내규 「어플리케이션 개발 및 운영보안 세칙」등에 따라 장애 또는 오류 발생시 해당 현업부서 부서장이 사전승인 후 전산원장 변경업무 담당자에게 처리를 의뢰하고 있으나,

업무요건 변경, 현업부서 업무담당자 오등록, 프로그램 오류 등의 사유로 변경한 전산원장 변경건수가 총 OOOO건으로 월 평균 OOO건을 상회하고 있어

전산원장 변경업무 담당자에 의한 부당한 변경 또는 오류 등으로 인해 전산장애 및 전자금융사고 등이 발생할 우려가 있으므로

내부통제위원회에서 전산원장 변경을 최소화할 수 있도록 관련 절차를 마련하는 등 전산원장 변경업무를 개선하시기 바람

(4) 백신프로그램 배포관리 미흡

내규 「IT운영보안 세칙」에 따라 바이러스 및 악성코드를 차단하고 내·외부통신망에 위치한 윈도우 서버 및 단말기의 백신 업데이트를 위해 백신관리 서버를 각각 운영하고 있으나,

인터넷망을 통해 다운받은 백신 업데이트 파일에 대해 무결성 검증만 거친 후 내부통신망에 설치된 백신관리 서버로 전송하여 서버 및 단말기에 자동 배포하고 있어, 동 파일이 악성코드 등에 감염된 경우 내부망에 악성코드가 유포될 우려가 있으므로

백신관리 서버에서 자동배포 기능을 차단하고 담당자에 의해 백신 업데이트 파일의 악성코드 감염여부 등을 사전 확인 후 동 파일을 배포하는 등 백신 프로그램 배포 관리 절차를 개선하시기 바람