경영유의사항 등 공개안

1. 금융회사명 : 한국금융투자협회

2. 조치일 : 2020. 5. 22.

3. 조치내용

대 상	내용
기 관	■ 개선사항 12건

4. 조치대상사실

가. 개선사항

(1) IT부문 감사 체계 미흡

「감사규정」에 따라 매년 감사계획을 수립하여 ◎◎실 소속 감사자가 IT업무에 대한 감사를 실시하고 있으나

감사업무편람이 없어 종합감사는 IT업무 전반이 아닌 ○○ 등 특정 분야에 한정하여 실시하고 자체감사를 ▷▷으로 대체하는 한편, 감사결과 지적사항을 내규에 명시되지 않은 '■■'로 해당 부서에 통보하고 있어 IT부문 내부통제가 취약해질 우려가 있으므로

감사항목, 감사주기, 사후관리 등 구체적인 감사업무편람을 마련하여 IT업무 전반에 대해 감사를 실시하고 지적사항은 감사규정에 근거하여 조치할 필요가 있음

(2) 정보처리시스템 성능 분석 미흡

내규「정보기술(IT)업무 관리규정」제21조에 따라 서버, 데이터베이스 등 정보처리시스템 성능을 분석하여 성능관리 보고서를 작성·보고하고 있으나

성능 분석시 CPU, 메모리 등 전산자원의 ◇◇ 등을 분석하지 않고 매월 점검 당시 사용량만 점검·보고하고 있어 정보처리시스템 성능이 ◎◎에 도달하더라도 적절한 시기에 시스템 증설이 이루어지지 않아 장애가 발생할 우려가 있으므로

동 내규에 성능분석 주기를 반영하고 CPU, 메모리 등 전산자원 사용량에 대한 추이분석을 실시하여 보고하는 등 성능관리 절차를 개선하시기 바람

(3) 웹사이트 및 콘텐츠 관리 미흡

내규「정보자산 업무지침」제6조에 의하면 웹사이트 및 콘텐츠를 정기적으로 점검하여 웹사이트 운영이 불필요한 경우 웹사이트를 통·폐합하여야 하나

동 지침에는 점검주기 및 통·폐합 기준이 명시되지 않아 2018년은 점검을 실시하지 않았고, 2016년는 ◎◎ 등 일부 웹사이트 통·폐합을 보고하고도 통·폐합하지 아니하는 등 웹사이트 및 콘텐츠 관리가 미흡하므로

동 지침에 점검주기 및 통·폐합 기준을 명시하고, 불필요한 웹사이트의 통·폐합 결과를 책임자에게 보고하는 등 웹사이트 및 콘텐츠 관리를 강화하시기 바람

(4) 정보처리시스템 운영체제 관리 미흡

전체 정보처리시스템 중 총 ◎◎대는 기술지원이 종료된 운영체제를 사용하고 있어 취약점 보안 및 기능개선 등을 위한 보정작업이 불가하여 신규 취약점을 이용한 해킹 및 악성코드 등에 의한 침해 우려가 있으므로

기술지원이 종료된 운영체제의 전환추진 계획을 수립하고 전환이 이루어지기 전까지 강화된 보안대책을 마련하시기 바람

(5) 취약점 분석·평가 조치이행 및 관리 미흡

시스템 및 홈페이지에 대한 취약점 분석·평가를 매년 실시하여 발견된 취약점에 대한 보완조치 계획 수립 및 취약점을 보완하고 있으나

전체 시스템이 아닌 일부 시스템에 대해 평가 실시후 취약점을 장기간 조치하지 않아 동일한 취약점이 반복적으로 발견되는 한편, 최고경영자에게 조치불가 취약점에 대한 미조치 사유를 보고하지 않고 있어 잔존 취약점으로 인한 사고발생 우려가 있으므로

시스템별 중요도 및 평가대상 선정기준을 마련하고, 조치 가능 취약점이 미조치 되거나 보완조치가 지연되지 않도록 취약점 조치이행 및 보고 절차를 강화하시기 바람

(6) 비상대응 훈련 체계 미흡

비상상황 발생시 IT서비스의 업무연속성 확보를 위해 매년 비상대응 모의훈련을 실시하고 있으나

비상대응매뉴얼에 ◎◎에 대한 복구절차 없이 IT부서 직원이 정보처리시스템 ▷▷여부만 검증하고 있어 비상상황 발생시 신속한 복구가 어려울 수 있으므로

동 매뉴얼에 훈련 참여인력 및 ◎◎ 복구절차를 추가하고 현업 부서 직원이 참가하여 복구자료에 대한 검증을 실시하는 등 비상대응 훈련 참여인력 확대 및 훈련방식을 개선할 필요가 있음

(7) 전산운영위원회 운영 절차 불합리

내규「정보처리시스템 구축 및 운영지침」제6조에 따라 ◎◎ 전결 금액 이상의 IT사업은 전산운영위원회에서 사전에 타당성 검토 및 비용대비 효과분석 결과를 심의·의결한 후 추진하고 있으나

심의·의결 과정에서 논의된 내용을 기록·보관하지 않아 심의·의결 결과에 대한 정당성 확인이 불가하고, 위원이 회의에 참석하지 않고 사후 의결하는 사례가 있어 긴급 추진이 필요한 사업이 적기에 추진되지 못할 우려가 있으므로

심의·의결 과정에서 논의된 내용을 회의록으로 작성·보관하고 긴급 추진이 필요한 사업이 지연되지 않도록 사후 의결을 최소화하는 등 전산운영위원회 운영 절차를 개선할 필요가 있음

(8) 프로그램 인수테스트 업무 불합리

IT부서에서 개발·테스트를 완료한 프로그램은 현업부서 업무 담당자에게 인수테스트를 요청하고 있으나

IT부서에서 인수테스트를 요청하였으나 일부 현업부서에서 인수테스트를 실시하지 않고 ◎◎시스템에 프로그램을 반영하여 프로그램 오류 등으로 인한 전산장애가 발생할 우려가 있으므로

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

(9) 내부정보 유출 방지대책 불합리

전산자료의 유출 등을 방지하기 위해 보안USB 관리시스템, 전자문서암호화, 개인정보검출 솔루션 등을 도입·운영하고 있으나

◎◎는 사용기간 제한없이 책임자 승인 후 지급(사용)함에도 반출자료의 적정성 및 분실현황을 점검을 하지 않고, 인쇄물에 워터마크가 표기되지 않아 내부정보 유출시 사후추적이 곤란해질 우려가 있으므로

◎◎ 등 개인 전산장비 사용을 금지하고 ◎◎ 보유현황 및 반출자료에 대한 점검을 실시하는 한편, 전산자료 출력시 인쇄물에 워터마크가 표시되도록 시스템을 개선하시기 바람

(10) 테스트 데이터 변환·사용 통제절차 불합리

프로그램 개발·테스트시 데이터 정합성 등을 확인하기 위하여 ◎◎를 사용하는 경우 동 정보를 식별할 수 없도록 변환하여 사용하고 있으나

데이터 ◇◇ 등을 포함한 신청절차가 없어 데이터 변환에 대한 책임관계가 불명확하고, 관리자가 수작업으로 ◎◎를 변환·삭제하고 있어 불필요한 정보가 변환 또는 테스트 종료후 삭제되지 않을 우려가 있으므로

데이터 ◇◇ 등을 포함한 신청절차를 마련하고 데이터 변환의 적정성 및 사용시간 만료후 삭제 여부 등에 대해 주기적으로 점검을 실시하는 등 테스트 데이터에 대한 통제를 강화할 필요가 있음

(11) 악성코드 감염 통제방안 미흡

악성코드 감염방지 등을 위해 백신 프로그램을 설치·운영하고 있으나 특정 PC에서 동일한 악성코드가 반복적으로 감염되고 있음에도 ◎◎ 등을 확인하지 않는 등 악성코드 감염 통제방안이 미흡하므로

악성코드 감염 및 치료 활동 등의 절차를 마련하고 매월 보안 점검 수행 시 악성코드 감염현황 및 치료결과를 점검할 필요가 있음

(12) 정보처리시스템 통제절차 미흡

서버 접근통제 솔루션을 도입하여 정보처리시스템 접근시 계정 및 비밀번호외 ◎◎ 등을 통한 추가인증을 수행하고 중요명령어 실행권한은 책임자 승인 후 부여하고 있으나

내부직원에게 사용자 계정을 관리자 계정으로 변경할 수 있는 중요명령어 실행권한을 상시적으로 부여하고 있고, 외주직원이 임의로 중요명령어를 수행하여 정보유출 또는 전산장애 발생 우려가 있으므로

중요명령어 실행권한은 사용기간을 제한하여 부여하고, 중요명령어 실행내역의 적정성 등에 대한 정기점검을 실시하는 등 정보처리시스템 통제를 강화할 필요가 있음