경영유의사항 등 공시

1. 금융기관명 : 미래에셋증권㈜

2. 제재조치일 : 2024. 11. 26.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 6건 개선사항 13건

4. 제재대상사실

가. 경영유의사항

(1) 정보교류 차단대상 설정 기준 합리화

금융투자업자의 정보교류 차단의무 이행을 위해 미공개 중요정보 등의 접근 가능성이 있는 업무 부문을 정보교류차단대상으로 설정하여 교류기록 유지 등 통제 절차를 마련 및 운영하고 있으나,

기업금융업무를 수행하는 부문 중 ■사업부만을 정보교류 차단대상으로 설정하고 ■사업부는 제외하고 있어, 기업금융업무와 기타업무 간 부적절한 정보교류가 일어날 우려가 있으므로 해당 사업부를 정보교류 차단대상에 포함시키는 등 설정 기준을 합리적이고 일관적으로 운영할 필요

(2) 공매도 관련 독립거래단위의 독립적 운영 강화

미래에셋증권㈜은 동일 부서 내 다수의 독립거래단위 운영 시 일부 소속 직원이 복수의 독립거래단위에 속하는 등 직무 분장이 명확하지 않고 일부 독립거래단위에 대한 매매목적 및 전략에 대한 문서화가 미비하므로,

공매도 운영 부서 소속직원에 대한 업무분장을 명확히 하고 독립거래단위별 매매목적(전략)을 관련 내규에 명시하는 등 독립거래단위의 독립적 운영을 강화할 필요

(3) 미결제위험 예방을 위한 환매조건부거래 중개 관련 업무절차 보완 필요

미래에셋증권㈜은 국내·외 거래당사자간 국내 상장주식 환매조건부거래(이하 'RP거래'라 함) 체결 및 이행을 지원(계좌개설, 매매 주문접수, 주식·자금이체 등)하는 업무를 수행하는 과정에서

RP거래 매수자인 ■측의 재무상황 및 주식확보 여부 확인 등 투자중개업자로서 거래상대방 결제불이행 가능성 분석, 방지를 위한 역할이 미흡한 것으로 파악되는바, 향후 미결제위험 예방을 위한 RP거래 중개 업무 프로세스 보완·강화 등 실효성 있는 투자자 보호 절차를 충실히 마련하여 이행할 필요

(4) 해외주식 권리업무 처리절차 강화

미래에셋증권㈜은 해외주식 권리변동 처리와 관련하여 수기작업에 따른 업무착오를 방지하기 위해 다음과 같이 전산시스템 활용도 등을 제고할 필요

■팀은 해외주식 병합(분할), 해외주식운영팀은 거래정지 등 관련부서 간 처리결과를 메신저, 유선 등으로 공유하고 있어, 정보전달 지연, 착오 등의 우려가 있으므로 각 부서에 전산시스템 조회 권한을 확대하는 한편,

해외주식 병합(분할) 등 권리변동에 대하여 예탁결제원의 배정 처리 이전에 고객 잔고수량에 미리 반영하는 경우 엑셀 수기 작업을 통해 검증하고 있어 계산 착오 등의 우려가 있으므로 전산시스템을 통해 확인하는 등 처리절차 강화 필요

(5) 금융사고 보고 절차 및 감사업무 독립성 등 강화 필요

금융기관은 「금융기관검사및제재에관한규정」에 따라 소속 임직원이 위법·부당행위를 함으로써 당해 금융기관 또는 금융거래자에게 손실을 초래하는 경우 등에는 감독원장에게 즉시 보고해야 하는데도

미래에셋증권 ■는 2022.2.7.~2022.3.4 기간 중 실시한 자체감사를 통해 ■지점 직원의 「자본시장과 금융투자업에 관한 법률」, 「특정경제범죄 가중처벌 등의 관한 법률」(이하 '특정경제범죄법') 등의 법규 위반사실을 확인하고, 사안을 중대하다고 판단하여 자체감사 기간 중에 신속히 면직 조치를 하였음에도 동 사실이 대외에 알려질 경우 회사의 평판 등 경영상 위험을 우려하여 검사착수일까지 금융감독원에 금융사고로 보고하지 않았고, 전체 감사결과를 회사의 감사위원회에 보고하지 않는 등 감사업무를 소홀히 한 사실이 있으며,

2023.6.15.~2023.7.26. 기간 중 실시한 자체감사를 통해 ▣▣▣▣▣▣ 직원의 「형법」, 「특정경제범죄법」 등의 법규 위반사실을 확인하고, 사안을 중대하다고 판단하여 면직 조치를 하였음에도 검사착수일까지 금융감독원에 금융사고로 보고하지 않았고, 회사의 감사위원회에서 민·형사상 조치를 검토하라는 요청이 있었음에도 후속 조치를 소홀히 하는 등 감사 업무를 독립적으로 수행하지 않은 사실이 있는바

향후에는 관련 규정에 따라 금융사고 보고사항이 적시에 이루어질 수 있도록 임직원에 대한 교육, 내규 및 관련 절차를 강화하고, 금융사고 보고의 지연 및 누락여부를 정기적으로 점검하여 감사위원회에 보고하는 절차를 마련하는 등 사후점검 프로세스를 강화하는 한편, 감사위원회 산하 감사보조조직이 경영진으로부터 독립성을 확보하여 공정하고 투명한 감사업무가 이루어질 수 있도록 인적구성·업무체계 등을 강화할 필요가 있음

(6) IT부문 감사체계 제고 방안 강구

IT부문은 내규 「전산컴플라이언스지침지침」 등에 따라 IT부문에서 제공하는 정보기술업무에 대하여 자체감사를 실시하고 있으나

IT부문 외 5개 본부는 정보기술 및 정보보호 업무에 대한 자체감사를 수행하지 아니하여 일상적인 업무처리 수행과 그 결과의 적정성에 대한 점검이 이루어지지 않으므로

위 5개 본부는 자체감사자 지정방안을 마련하고 부서별 업무 특성에 맞는 점검항목 및 점검방식 등에 대한 세부 감사 매뉴얼 등을 마련하여 자체감사를 실시하시기 바람

나. 개선사항

(1) 신용공여 금리 적용 및 산정 업무 개선

영업점계좌의 경우, 신용공여 기간별로 금리를 차등하여 단기간 이용시 할인금리를 적용하고 있는 반면, 비대면계좌의 경우는 이용기간에 무관하게 최고금리를 적용하고 있으므로, 이용채널에 따라 불합리한 차별이 없도록 비대면계좌에 대해서도 이용기간 별로 차등금리를 적용하여 운영하는 한편

「금융투자업자의 대출금리 산정 모범규준」에 따라 내부심사위원회를 거쳐 이자율을 산정하고 있으나, 아래와 같은 일부 불합리한 부분에 대해 개선 필요

① ‘신용프리미엄’은 대출자산에 대한 예상손실을 반영하여 합리적으로 부과하여야 하나, 동 자산에 대한 예상손실을 ‘0’으로 인식해 대손충당금을 전혀 쌓지 않고 있음에도 고객에게 최고 4.5%p까지 부과하고 있으므로, 회사가 인식하는 예상손실을 초과하여 고객에게 부과하지 않도록 개선할 필요

② ‘업무원가’는 신용공여 업무와 관련하여 직·간접적으로 발생하는 제반비용만을 포함하여야 하나, 예금보험료 등 관련없는 비용이 포함되어 있으므로, 실제 신용공여 업무와 무관한 비용이 고객에게 부과되지 않도록 개선할 필요

③ ‘목표이익률’은 회사의 경영목표 등을 반영해 미리 설정하여 일관성 있게 적용하여야 하나, 명확한 근거없이 일괄 4%p를 적용하고 있으므로, 합리적인 목표이익률 설정기준을 마련할 필요

한편, 이자율 산정을 위한 내부심사위원회 운영기준 등을 내규로 문서화하고 있지 않고, 회의록 등 논의내용 기록·유지 과정 없이 담당 팀장(부서장) 선에서 금리가 결정되고 있으므로, 심사위원회 운영기준 등을 내규에 명문화하고, 심사위원장을 임원급으로 격상하여 운영하는 등 위원회 운영을 강화할 필요

(2) 비대면 투자일임계약 체결시 업무절차 개선

투자일임업자는 비대면 투자일임계약 체결시 영상통화로 설명의무를 이행하여야 하나, 회사 판매직원이 영상통화로 상품내용을 설명하는 과정에서 외부 영향으로 영상통화가 일부 비정상적으로 중단되는 사례가 발생하고 있으므로

녹화중단 가능 상황 발생시 팝업 알람 설치, 영상통화 종료시 통화시간과 실제 녹화시간을 비교·확인할 수 있는 시스템 구축 등 업무절차를 개선할 필요

(3) IT 비상대책 수립·운용 미흡

(가) 회사 내규 「전산업무규정」에 따르면, 회사는 핵심업무를 비롯한 중요 업무에 대해 데이터 및 프로그램 백업시스템을 재해복구센터에 구축하고, 재해 발생 시 정상가동이 가능하도록 운영 및 관리하여야 하는데도

주전산센터 내의 서버 및 회선 등의 사용현황 대비 재해복구센터 서버 용량 및 회선 등이 일부 부족하여 재해발생 시 재해복구센터로 전환 운영하더라도 전자금융거래 업무의 지연 또는 중단이 우려되므로

주전산센터의 정보처리시스템의 자원 사용 현황 및 추이 분석 등을 통해 재해복구센터 서버 및 회선 등에 필요한 적정 용량을 정기적으로 산정하여 필요한 자원을 추가하거나 미사용 자원의 배분을 실시하는 등 재해복구센터 운용·관리를 강화할 필요가 있음

(나) 회사 내규 「전산업무규정규정」에 따라 IT비상대책의 실효성 확보를 위하여 연 1회 이상 재해복구전환훈련을 실시하고 있으나,

2018.11.14. ~ 2022.12.16. 중 실시한 8차례의 훈련에서 해외주식 및 해외파생 주문 등을 수행하는 해외주문FEP 시스템을 해외주문 중계기관과 연결하지 않고 훈련을 실시하여 재해복구센터와 해외주문 중계기관 간 전용선이 확보되지 않은 사실을 인지하지 못하였고, 이에 따라 재해발생 시 재해복구센터로 전환하더라도 영국, 독일 등 일부 해외 전자금융거래의 중단될 수 있으므로

해외주문 중계기관(또는 거래소)과 연계훈련을 실시하는 등 재해복구전환훈련을 실효성 있게 실시할 필요가 있음

(4) IT계약업무 절차 불합리

회사는 내규 「물품 및 용역의 구매 관리규정」 및 「IT구매관리지침」 등에 따라 IT구매계약 업무를 수행하고 있으나,

회사의 전반적인 물품구매에 관한 상위 규정 「물품 및 용역의 구매 관리규정」에 발주와 동시에 납품이 가능한 물품의 구매 등의 경우 계약서 작성을 생략할 수 있도록 규정하고 있어 중요도가 높은 IT자산을 구매하는 경우에도 동 규정을 근거로 계약서 작성을 생략하는 사례가 있어 추후 계약조건 관리가 어렵고 당사자 간 사후분쟁이 발생할 우려가 있으므로

내규를 개정하여 IT자산 구매 시 발주와 동시에 납품이 가능한 경우에도 계약서를 작성하도록 업무절차를 마련하시기 바람

(5) 정보처리시스템 감리 기준 수립·운용 미흡

회사 내규 「정보처리시스템 감리지침」에 따라 정보처리시스템의 안전성 등을 확보하기 위하여 투자금액(H/W, S/W 구입비용 제외)이 30억원 이상인 정보처리시스템 구축사업은 내부 감리를 시행하여야 하고, 사업의 성격, 규모, 난이도 등에 따라 외부 감리 시행이 필요하다고 판단되는 경우 외부 감리를 시행토록 하고 있으나

내부 감리 시행 기준 금액이 지나치게 높아 감리를 시행한 사례가 없고 외부 감리 시행 여부에 대한 구체적인 판단기준이 없어 외부 감리 실시 여부에 대한 사전검토 없이 사업을 추진하고 있으며, IT업무를 수행하고 있는 디지털 부문 등의 타 부서는 동 지침의 적용을 받지 않아 정보처리시스템 효율성 및 안전성 확보에 문제가 발생할 우려가 있으므로

정보처리시스템 효율성 및 안전성을 실효성 있게 확보하기 위한 내부 감리실시 시행 기준 금액을 낮추고, 외부 감리 실시 시행에 대한 세부적인 기준을 마련할 필요가 있으며, 「정보처리시스템 감리지침」의 적용 범위를 개선하여 IT업무를 수행하는 디지털 부문 등의 정보처리시스템 구축사업에도 적용하여 운영할 필요가 있음

(6) 전산장애 사후처리 운영 미흡

내규 「금융소비자 보호기준」에 따라 트레이딩매체 담당 부서는 전산장애 보상처리시 금융소비자 보호 민원 주관부서와 사전협의하고 처리 결과를 통보해야 하고

민원 주관부서는 공정한 민원 처리 및 합리적인 보상을 위하여 청구 금액이 5억원 이상이면서 일정부분 손해배상책임이 존재할 것으로 판단되는 민원은 내부통제소위원회에서 심의하여야 하는데도

트레이딩매체 담당 부서인 ■팀은 민원 주관부서인 ■팀에 전산장애 발생시 사전협의 및 처리결과 통보여부를 기록·관리하지 않아 보상처리에 대한 적정성 확인이 곤란하고,

민원 주관부서인 ■팀도 일부 전산장애 관련 민원에 대해 내부통제소위원회에 상정하지 않아 해당 민원에 대한 공정한 처리 및 합리적인 보상이 어려울 수 있으므로

■팀은 전산장애 발생시 금융분쟁조정팀과의 사전협의 및 처리결과에 대한 기록·보관이 누락되지 않도록 하고, 관련 내용을 담당 본부장에게 주기적으로 보고토록 하는 절차를 마련하고

■팀은 내부통제소위원회 심의 대상에 대한 기준을 보강하여 「금융소비자 보호기준」에 반영하고, 금융소비자보호 총괄책임자는 전산장애 관련 민원에 대한 내부통제소위원회 심의 여부와 민원 및 보상처리 상황 등을 점검할 수 있는 절차를 개선할 필요가 있음

(7) 시스템 개발·유지보수 업무절차 미흡

(가) 회사 내규 「시스템운영지침」에 따라 일괄작업(batch) 프로그램은 책임자의 승인을 득한 작업의뢰서에 근거하여 일괄작업을 수행토록 통제하고 있으나, 오류 프로그램을 수정 재실행하는 경우 책임자 확인이 시스템상 강제화되어 있지 않아 일괄작업 프로그램에서 반복적으로 오류가 발생할 우려가 있으므로

일괄작업 수행과정에서 오류가 발생하는 경우 작업을 중단하고 해당 업무 책임자가 오류 발생원인 및 오류 수정사항을 확인 후 재실행토록 하고,

주기적으로 일괄작업 오류명세(오류 유형별 분석·관리 현황 포함)에 대한 점검을 시행하여 점검 결과의 적정성을 본부장에게 보고하는 절차를 마련하는 등 일괄작업 프로그램에 대한 관리통제를 강화하시기 바람

(나) 회사 내규 「전산업무개발지침」에 따라 프로그램 개발 의뢰 부서는 요구한 개발요건이 충족되었는지에 대한 인수 테스트를 완료한 후 운영시스템 적용을 개발부서에 요청하고 있으나

개발부서는 프로그램 개발 의뢰 부서가 작성한 인수테스트 시나리오, 수행한 인수테스트 결과문서를 등록하지 않거나 인수테스트 결과 적정 여부에 대한 개발 의뢰 부서의 회신이 없는 프로그램을 운영시스템에 적용할 수 있어 충분한 테스트가 완료되지 않은 상태의 프로그램 오류로 인해 전산장애가 발생할 우려가 있으므로

변경된 프로그램을 운영시스템에 적용하기 전 개발의뢰부서의 개발요청서에 기반한 테스트 항목 및 테스트 결과문서에 대한 책임자 승인이 강제화되도록 절차 또는 시스템을 개선하시기 바람

(다) 회사 내규 「서버보안 관리지침」에 따라 정보처리시스템 기동/종료 등 시스템 가동에 영향을 미치는 주요 명령어는 업무중요도에 따라 통제하고 있으나

전산자료 삭제 등을 포함한 일부 명령어는 책임자 사전승인 없이 실행이 가능하여 운영 서버에서 불필요한 명령어 실행 등으로 인한 전산사고가 발생할 우려가 있으므로

관리자, 시스템담당자, 일반사용자를 포함하여 전 임직원을 대상으로 서버 및 데이터베이스의 중요 명령어 실행 권한을 점검하는 한편, 서버·데이터베이스의 중요 명령어 통제범위를 확대하여 책임자의 작업계획서 사전 승인 후에만 실행이 가능토록 관련 시스템을 개선하고

■팀은 주기적으로 정보처리시스템에서의 중요명령어 차단 여부 및 중요 명령어 수행 내역의 적정성을 점검하여 정보보호최고책임자(CISO)에게 보고하는 절차를 마련하여 정보처리시스템 중요작업에 대한 통제를 강화하시기 바람

(라) 회사 내규 「정보보호 규정」에 따라 MTS 등을 포함한 모바일 앱은 앱 위·변조 방지, 키패드 보안, 통신구간 암호화 등 보안대책을 적용하고 있으나

모바일 앱 배포용 단말기를 운용하고 있지 않아 악성코드 감염 등으로 인한 보안사고가 발생할 우려가 있으므로

앱스토어 등 배포시 필요한 사이트만 접속을 허용한 모바일 앱 배포용 단말기를 지정·운용하고, 앱 배포 후 배포프로그램 등 관련 자료를 즉시 삭제하고 자료 삭제여부에 대한 점검을 주기적으로 실시하여 ■팀에게 통보하는 등의 절차를 마련하는 등 모바일 앱 개발 및 배포 환경에 대한 통제를 강화하시기 바람

(마) 회사 내규 「개발 및 응용보안 관리지침」에 따라 운영업무담당자는 프로그램 변경 계획 수립시 보안담당자에게 요청하여 보안성 검토를 실시하여야 하나

IT부문 및 ■본부를 제외한 나머지 개발업무를 수행하고 있는 부서는 자체 보안성 검토 절차를 수립하지 아니하여 전자금융거래 관련 프로그램에 대한 자체 보안성 검증이 누락되어 전자금융거래용 프로그램이 보안 취약성을 내포하는 경우 보안사고가 발생할 우려가 있으므로

■부문을 포함한 모든 개발업무를 수행하는 부서에서 개발한 주문, 자금 이체 등 전자금융거래와 관련성이 높거나, 이용자 정보를 처리하는 프로그램에 대해서는 ■본부에서 자체 보안성 검증을 실시하거나,

개발 부서에서 직접 보안성 검증을 실시하는 경우에는 보안성 검증 결과에 대한 ■본부 합의 후 변경된 프로그램이 운영시스템에 반영(단, 휴일, 장애발생시에는 제외)되도록 관련 절차 및 시스템을 개선하시기 바람

(8) 전산자료 보호대책 수립·운용 미흡

(가) 회사 내규 「전산운영실 및 통신망 관리지침」, 「네트워크보안 관리지침」에 따라 운영 서버에 대한 비인가 접근을 원천 차단하고 개발 및 테스트 서버의 장애 또는 보안 취약점이 운영 서버로 전이되지 않도록 운영·개발·테스트 서버 유형별로 네트워크를 분리·구축하고 업무용 단말기에 대한 네트워크 IP 부여 기준을 수립하고 있으나,

단말기에 부여된 네트워크 IP을 기준으로 접근 가능한 서버 또는 데이터베이스의 계정을 관리하지 않아 해당 단말기가 중요 단말기로 지정이 누락될 우려가 있고, 업무용 단말기와 동일한 IP대역을 사용할 경우 IP대역별 보안정책 적용 시 업무와 상관없이 보안정책이 완화될 우려가 있으므로

모든 단말기에 대해 회사가 정한 '네트워크 IP 부여 기준'의 준수여부를 점검하여 동 기준을 준수토록하고, 서버 또는 데이터베이스 유형별(운영, 테스트, 개발 등) 계정 발급시 정보처리시스템에 직접 접속하는 단말기가 중요 단말기로의 지정이 누락되지 않도록 정보보안팀과 합의 절차를 마련하는 한편, 정보보안팀은 정보처리시스템 접속이 가능한 단말기에 대한 주기적인 점검을 실시하여 단말기에 대한 보안통제를 강화하시기 바람

(나) 회사 내규 「개발 및 응용보안 관리지침」에 따라 운영시스템의 실제 데이터를 테스트 및 개발 용도로 사용할 때에는 중요데이터는 변환하여 사용하도록 하고 있으나,

'데이터 변환 솔루션(SQLCanvas)'을 통하여 고유식별정보 등 민감정보를 테스트 및 개발 시스템으로 변환·이관하는 과정에서 데이터 변환을 수행하는 담당책임자 승인 이외에 정보보안부서 또는 내부감사자와 같은 추가적인 확인 절차와 사용 목적이 종료된 테스트 데이터의 삭제 여부를 확인하는 절차가 내규에 마련되어 있지 않아 데이터 변환 수행의 적정성 확인 및 사후관리가 미흡할 우려가 있으므로

데이터 변환 신청시 이용목적, 사용자, 사용기간, 승인권자, 폐기 절차 등이 포함된 절차와 변환 대상 항목을 내규에 반영하고, 운영시스템 데이터를 테스트 및 개발 시스템으로 변환·이관 시 추가적인 확인 절차가 강화되도록 변환 요청 부서의 책임자, 데이터베이스 관리부서의 책임자, 정보보호부서 책임자의 사전승인 시에만 이용자 정보 변환이 가능토록 시스템을 개선하고

테스트 및 개발 시스템에 변환되지 않은 이용자 정보 저장여부를 주기적으로 점검하여 미변환 이용자 정보가 있는 경우 즉시 삭제하는 등 테스트 데이터에 대한 통제를 강화하시기 바람

(다) 회사 내규 「PC보안 관리지침」에 따라 단말기에 중요정보(고객정보 및 내부중요정보)를 보관하지 않도록 하고, 불가피하게 단말기에 보관할 필요가 있는 경우 해당 정보를 암호화하여 관리하기 위해 문서암호화시스템(DRM) 솔루션 등 정보보호시스템을 설치·운영하고 있으며, 중요정보의 외부반출 시 담당팀장의 검토와 승인을 받도록 절차를 마련하고 있으나,

■팀은 암호화문서에 대한 복호화 승인권자 등 통제 절차를 규정에 반영하지 않았고, 문서 복호화 자가승인 권한 보유자의 적정성에 대해 분기 1회 점검하고 있으나 업무상 무관한 문서를 복호화 하거나 직전 분기 복호화 수행 건수가 저조하여 자가승인 권한의 필요성이 낮은 직원에 대하여도 충분한 검토 없이 복호화 자가승인 권한을 재부여하는 등 자가승인 권한 부여의 적정성 검토 및 사후관리가 미흡하여 암호화 해제된 내부자료 등이 외부로 유출될 우려가 있으므로

문서복호화시스템 사전·자가승인 대상 기준, 승인권자, 승인 절차 및 자가승인 권한 재부여 기준과 담당직원이 자가승인한 문서 복호화 수행내역을 담당 부서장이 사후 승인하여 주기적으로 자가승인 관련 내용을 정보보호부서에 전달하도록 절차를 마련하고 문서보안 통제 절차 준수 여부를 주기적으로 점검하여 문서보안시스템에 대한 통제 절차를 강화하시기 바람

(9) 취약점 분석·평가 사후관리 미흡

회사 내규 「보안점검 관리지침」에 따라 전자금융기반시설 및 홈페이지의 취약점 분석·평가를 연 1회(홈페이지는 6개월에 1회) 실시하고 발견된 취약점에 대해서는 조치계획을 수립·이행하고 있으나,

취약점 분석·평가 시 발견된 취약점과 관련하여 영향도 분석 등 세부 처리 절차를 마련하고 있지 않으며, 발견된 취약점을 적기에 보완조치하지 않아 매년 동일한 유형의 취약점이 발견되고 있으며, 일부 취약점의 경우 최초 조치 계획이 이행되지 않았더라도 그 사유에 대한 검토 없이 조치 계획의 이행을 장기간 연장하는 등 사후관리가 적정하게 이루어지지 않을 우려가 있으므로

취약점 분석·평가 결과 식별된 취약점에 대해서는 취약점 조치 관리 주관부서에서 업무 영향도 평가를 수행하여 조치 가능 여부를 빠짐없이 검토하고, 조치가 어려운 취약점은 조치에 준하는 보완통제를 적용하고,

조치계획에 대해서 주기적으로 이행현황 및 미조치 사유 등을 분석·평가하고, 그 결과를 ■본부와 협의하여 식별된 취약점의 조치 이행이 적시에 이루어질 수 있도록 관련 절차를 개선하시기 바람

(10) 무선통신망 차단시스템 운영·관리 미흡

회사 내규 「네트워크보안 관리지침」에 따라 비인가 무선통신망 사용을 통제하기 위해 무선침입방지시스템(WIPS) 총 54대를 설치·운영하고 있으며, 정보처리시스템에 대한 접근통제 시스템을 운영하여 비인가자에 대한 통제를 실시하고 있으나,

운영 중인 무선침입방지시스템(WIPS)이 일부 노후화 되어 최근 무선표준(Wi-Fi 5 등)에 대한 탐지·차단 기능을 지원하지 못하는 등 비인가 무선기기 통제에 보안 취약점이 존재하므로

무선통신망 운영 시 보안 취약점이 발생하지 않도록 최신 무선 표준 규격의 기술적인 특성을 반영하여 무선침입방지시스템(WIPS)을 개선하는 등 무선통신망 운영·관리를 강화하시기 바람

(11) 정보보호 내규 수립·운용 미흡

(가) 회사 내규 「정보보호 규정」, 「보안시스템 관리지침」, 「서버보안 관리지침」 등 14개의 규정·관리지침에 따라 정보보호관리체계를 수립·운용하고 있으며 업무환경 및 관련 법령의 변화에 따라 정보보호 규정의 타당성을 연 1회 정기적으로 관련 팀과 협의하여 검토하고 있으나,

망분리, 클라우드컴퓨팅서비스 이용절차 등에 대한 보고 문서를 기준으로 운용함에 따라 체계적인 업무 수행이 미흡할 우려가 있으므로

망분리, 클라우드컴퓨팅서비스 이용절차 등을 내규에 반영하고 앞으로 전자금융 관련 법규의 개정 내용을 신속히 파악하여 내규에 반영할 수 있도록 소관부서가 철저히 검토하시기 바람

(나) 회사 내규 「보안점검 관리지침」에 따라 전자금융거래를 위하여 서비스를 신규로 오픈하거나 회사의 중요정보를 취급하는 프로젝트 등의 경우 안전한 전자금융거래를 위하여 자체 보안성심의를 실시하도록 하고 있으나,

자체 보안성심의 요청·수행 시점이 절차상 구체적으로 마련되어 있지 않고 신규 전자금융업무 수행 이외에 인증절차 추가·삭제·변경 등 보안에 중요한 영향을 미치는 사항에 대해 자체 보안성심의를 수행해야 한다는 내용이 내규 등 절차상 마련되어 있지 않아 보안상 중요한 사항에 대해 자체 보안성심의가 누락되어 보안 위협이 증가할 우려가 있으므로

자체 보안성심의 요청·수행 시점을 구체적으로 내규에 마련하고, 전자금융거래의 인증절차 추가·삭제·변경 등 보안에 중요한 영향을 미치는 사항에 대해서도 자체 보안성심의를 수행하도록 하도록 관련 내규를 강화하시기 바람

(12) 신용정보전산시스템 내부통제 미흡

회사 내규 「신용정보 관리 및 보호에 관한 규정」에 따라 신용정보전산시스템에 대한 불법적 접근이나 입력된 정보의 변경·훼손·파괴 등을 방지하기 위하여 기술적·물리적·관리적 보안대책을 수립·시행하도록 하고 있고, 개인신용정보처리 관련 프로그램 변경 시 프로그램 개발 프로세스(ITSM)과 형상관리시스템(RIMS)에 의한 통제절차를 실시하고 있으나,

프로그램 개발자가 이용자 인증·식별 등 중요 프로그램을 변경하는 과정에서 프로그램 개발 프로세스(ITSM) 및 형상관리시스템(RIMS)에 의한 통제절차를 우회하여 프로그램을 운영시스템에 반영하는 경우 이를 사전에 방지하기 위한 모니터링 체계가 마련되어 있지 않는 등 신용정보전산시스템에 대한 보안 대책이 일부 미흡할 우려가 있으므로

개인신용정보처리 관련 중요 프로그램 개발·변경 시 프로그램 통제절차를 우회할 수 없도록 관련 내부통제 절차를 마련하고 형상감사기능을 통하여 주기적으로 점검하는 등 모니터링 체계를 강화하시기 바람

(13) 정보처리시스템 운영체제 등 보정작업 미흡

회사 내규 「변경관리지침」에 따라 시스템 운영체제(OS), 시스템 S/W 버전, DBMS의 버전 등에 대한 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 변경 작업을 하여야 하는데도

검사착수일 기준 서버 242대, 데이터베이스 120대 및 정보보호시스템 50대가 제조사의 기술지원이 종료된 시스템 소프트웨어를 사용하고 있어 보안패치 및 서비스 업그레이드 등의 지원을 받지 못하여 시스템 오류 및 장애 발생 시 신속한 대응이 어렵고 신규 취약점을 악용한 해킹 및 악성코드 감염 등이 발생할 우려가 있으므로

기술지원이 종료된 시스템 소프트웨어를 업그레이드하거나 제조사와 기술지원 연장 계약을 체결하는 등 시스템 소프트웨어로 인한 장애발생을 미연에 방지하기 위해 업그레이드 또는 교체 추진에 대한 이행계획을 주기적으로 마련하고, 조치 결과를 정기적으로 점검하여 완료하지 못한 경우 그 사유를 남기고 연관 부서의 확인서를 받는 등 관리를 강화하시기 바람