경영유의사항 등 공개안

1. 금융기관명 : 유안타증권㈜

2. 조치일 : 2025. 9. 24.

3. 조치내용

제재대상	제재내용
기 관	경영유의사항 3건, 개선사항 13건

4. 조치대상사실

가. 경영유의사항

(1) 대체투자업무의 리스크관리 정교화 필요

A부서는 대체투자 업무와 관련하여 각 투자 사업장의 평가등급을 3단계로 분류하고 있으나, 각 단계별 구분 기준이 단순하고 구체적이지 않으므로

각 사업장의 사업성에 영향을 미칠 수 있는 다양한 리스크요인*을 평가등급 구분 기준에 반영하고 평가등급을 세분화하는 등 대체투자업무와 관련된 리스크관리를 정교화할 필요가 있음

* 투자물건의 종류, 준공율, 분양율, 만기연장 횟수, 수분양자 계약취소율, 시공사 신용등급, 지역별 낙찰가율, 신탁사 책임준공여부 등

(2) SPC 자금관리 업무 관련 내부통제 강화

SPC의 업무수탁자에게 자금집행 요청 시 담당자의 개인메일을 이용하거나 상위 직급자 확인 절차를 생략하는 경우가 있고

일부 자금집행의 경우 자금집행증빙이 보관되지 않거나 미비하고, 사전에 계획되지 않거나 통상적이지 않은 용역자문계약을 체결하는 경우에도 별도의 절차 없이 자금이 집행되는 등 체계적 관리가 미흡한 바, SPC 자산관리자로서 수행하는 업무에 대한 내부통제를 강화할 필요가 있음

(3) IT부문 수시감사 및 IT부서 자체감사 강화

회사는 내규「감사위원회 직무규정」및「IT감사지침」등에 따라 IT부문에 대한 수시감사를 실시토록 정하고 있음에도,

객관적인 수시감사 실시기준을 마련하지 않아 감독기관의 요청에 따른 수시감사 외에는 자체적으로 수시감사를 실시하지 않았고,

「IT감사지침」내 정보보호업무 자체감사 관련 내용을 반영하지 않았고, 정보보호업무에 대한 IT 자체감사자를 지정하지 않았으며, 그 결과 동 업무에 대한 자체감사 업무를 실시하지 않고 있으므로

IT부문 수시감사와 관련한 객관적인 실시기준과 정보보호업무에 대한 IT 자체감사자 지정, 자체감사 실시기준, 감사항목, 실시방법을 포함한 감사 매뉴얼 등을 마련하고, 동 기준에 따라 감사업무를 실시하는 등 IT부문의 내부통제 체계를 강화할 필요가 있음

나. 개선사항

(1) IT업무 수의계약 절차 미흡

회사는 내규「IT업무 계약지침」에 따라 IT 업무에 해당하는 계약을 체결하고자 할 때에는 경쟁입찰에 의한 거래상대방 선정을 원칙으로 하며, 계약담당부서장은 계약금액이 X억원 이상의 수의계약을 체결하는 경우 IT운영위원회 승인을 받도록 절차를 마련하고 있으나,

검사대상기간(2020.1.1.~2023.8.1.) 중 계약금액 X억원 이상의 수의계약 XX건을 수의계약으로 추진하는 타당성에 대한 IT운영위원회의 승인 없이 사업 내용에 대한 승인만 득하여 계약을 체결한 사실이 있으므로

앞으로 IT운영위원회를 통한 IT 사업타당성 검토 및 비용 대비 기대효과 분석시 세부 사업별 계약 방안을 포함하여 심의하는 절차를 마련하거나, 계약금액 X억원 이상의 수의계약으로 추진하는 타당성에 대해 심의하는 절차를 마련하시기 바람

(2) 정보시스템 구축사업 감리기준 수립·운용 절차 미흡

회사는 내규 「정보시스템 감리지침」에 따라 IT관련 정보화 사업을 추진할 때 위험요소를 최소화하고 정보시스템의 안정성 및 효율성을 확보하기 위해 IT운영위원회 심의 기준 이상의 정보시스템 구축사업은 감리를 수행하고 있으나,

외부 감리는 투자금액과 상관없이 사업의 성격, 규모, 난이도 등을 고려하여 시행 여부를 결정하여야 하는데도, 내규상 내·외부 감리 대상 기준을 별도로 구분하고 있지 않는 등 외부감리 시행 여부에 대한 구체적인 판단기준이 없어 외부 감리 실시 여부에 대한 사전검토 없이 사업을 추진하고 있으며

검사대상기간(2020.1.1.~2023.8.1.) 중 실시한 XX건의 감리를 외부 감리 없이 모두 IT본부 자체감사인 1명이 일괄로 실시함에 따라 사업 종료 이후 사후적으로 감리가 실시된 사례가 있는 등 감리의 실효성이 저해될 우려가 있으므로

고객정보 처리 또는 금융거래 및 거래정보 제공에 미치는 영향도 등을 고려하여 내규 「정보시스템 감리지침」에 외부감리 기준을 마련하고, 동 기준에 따라 외부 감리 시행 여부를 검토한 후 동 검토 결과(감리 수행 또는 미수행 사유)를 사업 품의(계약) 결재 문서에 기재토록 하는 절차를 지침에 반영하여 정보처리시스템의 안전성 및 효율성을 확보할 수 있도록 개선하시기 바람

(3) 프로그램 개발·운용 절차 미흡

회사는 내규 「IT업무 개발지침」에 따라 프로그램 개발, 테스트 등의 절차를 규정하고 전산개발관리시스템 및 형상관리시스템을 이용하여 프로그램 변경·통제 절차를 운영하고 있으나,

(가) 프로그램 변경 관련 테스트 결과서 작성 시 테스트 시나리오 체크리스트 이외에 프로그램 정상 작동 여부에 대한 결과화면 등의 첨부가 필수적이지 않아 테스트 결과의 적정성 검토가 미흡할 우려가 있으므로

전산개발관리시스템을 통해 프로그램 변경 시 테스트 결과화면 첨부가 누락되지 않도록 관련 절차를 개선하시기 바람

(나) 장애·오류가 발생하는 등 긴급을 요하는 경우 프로그램 긴급 변경 절차를 거치고 있으나, 절차상 사후결재 기한이 정해져 있지 않아 관련 책임자 승인이 누락될 우려가 있으므로

긴급 변경 절차를 통한 프로그램 변경 시에는 책임자 결재가 누락될 우려가 없도록 사후결재 기한을 내규 등 업무절차에 반영하시기 바람

(다) 외부주문 직원을 포함한 프로그램 개발자에게 수정된 소스코드를 운영시스템으로 이행할 수 있는 이행관리시스템 권한이 부여되어 있어 프로그램 담당자가 직접 수정된 프로그램을 운영시스템에 반영할 우려가 있으므로

외부주문 직원을 포함한 프로그램 개발자가 직접 운영시스템에 변경된 프로그램을 이행할 수 없도록 관련 이행관리시스템 등의 권한관리를 강화하시기 바람

(4) 일괄작업 사후관리 등 미흡

회사는 내규 「야간일상작업 처리절차」에 따라 일괄작업 수행 시 IT관리시스템을 통해 요청 후 일괄작업관리시스템에서 책임자가 승인하여 처리하고, 오류발생 시 오류처리 절차에 따라 작업을 재수행하며

평균 수행시간이 위험 기준을 초과하는 일괄작업에 대해서는 담당자가 검토결과서를 작성하고 관리자 승인을 받도록 하고 있으나,

(가) 검사대상기간(2020.1.1.~2023.8.1.) 중 위험기준을 초과한 일괄작업 XXX건 중 XXX건에 대해서는 검토 결과서 작성을 누락하는 등 사후관리가 미흡하여 전산장애가 발생할 우려가 있으므로

평균 수행시간이 위험 기준을 초과하여 오류 발생 위험이 있는 일괄작업에 대해 검토 결과서 작성을 생략하지 않도록 하고, 주기적으로 일괄작업 수행 결과를 점검하여 오류 발생 위험이 있는 일괄작업 프로그램을 신속히 개선하는 등 사후관리를 강화하시기 바람

(나) 일괄작업 수행 과정에서 오류가 발생하여 이를 재수행하는 경우 책임자에게 유선 등으로 보고 후 처리하고 있으나 책임자가 동 처리내역을 사후적으로 승인하는 절차가 마련되어 있지 않아 오류가 발생한 일괄작업에 대해 책임자 보고가 누락될 우려가 있으므로

야간 또는 휴일 오류 등으로 일괄작업을 재수행하는 경우 해당 책임자가 오류 원인 및 재수행 이후 정상 완료 여부 등을 사후적으로 승인할 수 있도록 관련 절차를 개선하시기 바람

(5) 프로그램 보안성 검증 절차 미흡

회사는 내규 「개발보안 지침」에 따라 보안성 검토가 필요한 개발 건에 대해서는 보안성 검증을 수행하고 어플리케이션 개발자는 프로그램 개발 시 「개발 보안 가이드라인」에 따라 소스코드 점검을 수행하고 있으나,

개발부서에서 프로그램 변경 시 보안성 검증 수행 필요 여부에 대한 정보보호본부와 합의 절차가 구축되어 있지 않으며, 정보보호부서에서 프로그램 보안성 검증 수행 이력을 별도로 관리하고 있어 개발부서에서 전자금융거래 관련 프로그램 변경 시 정보보호부서에 보안성 검증 요청을 누락할 우려가 있으므로

전자금융거래와 관련성이 높은 매매·파생·이체업무 및 이용자 정보를 처리하는 프로그램 변경 건에 대해서는 정보보호본부에서 프로그램 보안성 검증을 실시하거나 개발부서에서 직접 보안성 검증 수행 시에는 보안성 검증이 누락되지 않도록 정보보호본부 합의 결재 후 변경된 프로그램이 운영시스템에 반영되도록 관련 절차 및 시스템을 개선하시기 바람

(6) 업무지속성 확보방안 운용 미흡

회사는 내규 「금융전산분야 현장조치행동매뉴얼」 등에 따라 주요 통신회선 및 전산장비 등을 이중화하고 재해복구센터를 구축·운영하는 등 업무지속성 확보방안을 수립하여 시행하고 있으나,

주전산센터 및 재해복구센터 모두 단일 통신사업자의 시설에 구축하고 MTS·HTS 등 주요 대고객 전자금융거래 서비스 제공을 위한 통신회선(이하 “대고객 통신회선”)도 동 통신사업자의 회선으로만 구축함에 따라

동 통신사업자의 장애 발생 시 모든 대고객 전자금융거래 서비스의 제공이 불가하고, 재해복구센터 전환에 따른 비상대책 운영도 불가능해지는 등 업무지속성 확보방안의 실효성이 저해될 우려가 있으므로

특정 통신사업자의 장애 발생에 따른 비상대책 시나리오를 점검하여 대고객 통신회선의 통신사업자를 이원화하는 등 대고객 전자금융거래 서비스 제공의 안정성을 제고하고, 이에 따라 관련 비상대책을 개선하여 시행하시기 바람

(7) 이상금융거래탐지시스템 운영 미흡

회사는 증가하는 전자금융사고에 대한 대응수준 강화를 위하여 XXXX년 중 이상금융거래탐지시스템(이하 “FDS”)을 구축하고 XXXX년 중 고도화를 통해 이용자 로그인, 공동인증서 발급, 이체 내역 등의 정보를 조합하여 이상거래를 탐지하고 고위험 시나리오에 대해 사전차단 정책을 운영하고 있으나,

FDS와 관련한 규정·지침·절차 등을 마련하고 있지 않아 탐지정책·운영기준 등이 체계적으로 관리되지 못할 우려가 있고, 실제로 FDS 개발 업체의 유지보수 중단(서비스 종료) 이후 추가계약 등 향후 운영방안을 마련하지 않아 탐지·차단 정책을 신규로 적용하거나 변경이 되지 않고 있으며, XXXX년 고도화 이후 지금까지 정책의 추가·변경 등 운영실적이 전무하고, 오탐률이 높다는 이유로 XXXX년 중 사전 차단 정책을 해제하는 등 FDS로서의 실질적인 기능을 하지 못하고 있으므로

이상금융거래를 적시에 인지하여 신속히 대응할 수 있도록 이상금융거래의 기준, FDS 운영의 주체, 업무처리절차 및 기타 운영 방침 등을 마련하여 시행하는 등 전자금융사고에 대한 대응체계를 강화하시기 바람

(8) 기술지원 종료 운영체제 사용에 따른 보안통제 미흡

회사는 내규 「IT기기관리지침」 등에 따라 서버·통신장비 등 정보처리시스템에 대하여 필요시 보정작업을 실시하고 있으며 IT본부 중장기 계획을 통해 노후 정보처리시스템을 단계적으로 교체하는 계획을 수립하여 추진하고 있으나,

검사종료일(2023.8.1) 현재 회사가 가동 중인 서버 중 일부에서 제조사 기술지원이 종료된 운영체제(OS)를 사용하고 있어 운영체제에 대한 신규 취약점 보완 및 기능개선 등을 위한 보정(patch) 작업이 곤란하여 미보완 취약점을 이용한 해킹, 악성코드 감염 등 침해사고가 발생할 우려가 있으므로

장애발생을 미연에 방지하기 위해 기술지원 종료 도래 여부를 주기적으로 점검하고, 연간 업무계획 및 예산 수립 시 노후장비 교체, 운영체제 업그레이드, 제조사 기술지원 연장 계약 체결 등의 방안 이행이 사전에 반영될 수 있도록 절차를 개선하시기 바람

(9) 전자금융기반시설 안전성 관리 미흡

회사는 내규 「보안사고 예방 및 대응 지침」에 따라 침해사고 내부정보 유출사고 예방을 위해 전자금융서비스를 운영하는 주요 정보시스템 취약점 점검, 침해사고 및 악성 이메일 탐지·대응 훈련계획을 수립하여 서버해킹, 악성코드 및 서비스 거부에 대한 침해사고 대응훈련을 수행하고 있으나,

취약점 점검 대상을 선정하는 기준 및 절차 등이 명확하게 구분되어 있지 않아 취약점 분석·평가 담당자가 주요 전자금융거래 관련 시스템들을 누락할 우려가 있고, 2020년~2022년 기간 중 전자금융기반시설 취약점 분석·평가 시 XX건의 동일한 취약점 항목이 지속적으로 발견되고 있는 등 취약점 보완이 적기에 이루어지지 않고 있으므로

전자금융기반시설 취약점 분석·평가 대상 및 범위를 선정하기 위한 기준을 마련하여 관리하고, 매년 지속적으로 발견되는 취약점 항목은 보완 방안을 마련하여 관리하는 등 전자금융기반시설 취약점 점검체계를 강화하시기 바람

(10) 해킹 등 전자적 침해행위 방지대책 미흡

회사는 내규 「정보보호 규정」 등에 따라 ㉮ 등을 설치·운영하고, ㉯를 이용하여 보호하고 있으나,

보안시스템별 주요정책 변경 시 정보보호 주관부서장의 승인 없이 정보보안 담당자의 확인만 실시하고 있으며, 정책의 적정성 여부 또한 주기적으로 검토하지 않는 등 전자적 침해행위 방지를 위한 업무절차가 미흡하므로

정보보호시스템의 주요 정책 변경 시 정보보호 주관부서장의 승인을 득하는 전자결재 등의 공식적인 확인 절차를 갖추고, 주기적으로 ㉮ 정책 타당성 검토를 진행하는 등 침해행위 방지를 위한 업무절차를 개선하시기 바람

(11) 자체 보안성 심의 절차 미흡

회사는 내규 「개발보안 지침」에 따라 자체 보안성 심의를 포함한 보안성 점검 등의 정책·기준을 수립하여 신규 전자금융 서비스 제공 시 안정성 확보를 위해 자체 보안성 심의를 수행하고 있으나,

자체 보안성 심의 대상인 신규 전자금융 서비스 기준 및 전산시스템 개발 시 보안성 점검 대상과 자체 보안성 심의 대상이 명확하게 정의되지 않아 신규 서비스 오픈 또는 기능 추가 시 보안성 심의 보고가 누락될 우려가 있으므로

신규 전자금융 서비스에 대해 자체 보안성 심의가 누락되지 않도록 내규에 전자금융 서비스 기준을 세분화하여 수립하고, 전산시스템 개발 시 보안성 심의 여부를 담당자가 인지할 수 있도록 보안성 점검 대상 항목과 자체 보안성 심의 절차를 구분하여 보안성 심의 체계를 개선하시기 바람

(12) 무선침입방지시스템 및 중요단말기 운용·관리 미흡

회사는 내규 「사용자 인증 및 접근통제 지침」 및 「시스템 보안관리 지침」에 따라 비인가 무선통신망 사용을 통제하기 위해 주요시설에는 ㉮를 설치·운영하고, ㉯ 등 보안통제를 적용하는 등 매월 운용상태를 점검하고 있으나,

(가) 주요시설의 정의와 무선통신망 차단을 위한 운영기준·절차 등이 마련되어 있지 않아 전산시스템의 직접접속이 가능한 개발실 등의 신규 구축 시 ㉮의 설치를 누락하거나 무선신호세기가 약하게 설정되어 실질적인 무선통신망 차단이 미이행될 우려가 있으므로

내규에 주요시설의 정의 및 무선통신망 차단 운영기준·절차 등을 마련하고, 주요시설 내 비인가 무선통신망의 사용이 차단되도록 적정한 무선신호세기를 설정·운용하는 등 무선통신망의 보안통제를 강화하시기 바람

(나) 서버·DB접근제어시스템을 통해 정보처리시스템에 접속하는 일부 업무망 단말기가 중요단말기로 지정·관리되지 않아 보안점검 대상에서 누락될 우려가 있으므로

정보시스템 및 정보보호시스템을 접속하는 PC가 보안점검에서 누락되지 않도록 중요단말기 지정 기준·대상 등을 내규에 반영하고, 중요단말기 및 서버 등 내부 IP 관리 체계를 정비하여 중요단말기 관리를 개선하시기 바람

(13) 이용자 정보 관리 및 조회·출력 통제절차 미흡

회사는 내규 「개인정보보호 지침」에 따라 업무처리시스템(통합단말)에서 고객정보 조회·출력 시 마스킹 처리 및 결재권자의 승인을 통해 화면 권한을 부여하고 개인정보 파일 유출 방지를 위해 매월 정보처리시스템 담당자에게 개인정보 검출 여부를 확인하는 등 이용자 정보를 관리 및 점검하고 있으나,

정보처리시스템 개발·운영 시 개인정보 마스킹 처리가 필요한 화면 적정성을 점검하는 절차가 미흡하여 마스킹 처리를 누락할 우려가 있고, 업무처리시스템 내에 고객정보가 조회 가능한 화면에 대한 권한부여 체계가 미흡하여 업무상 불필요한 화면 조회 또는 임의조작 등 오남용의 우려가 있으므로

정보처리시스템 개발·운영 시 개인정보 마스킹 처리를 누락하지 않도록 업무절차와 시스템을 개선하고, 화면 접근권한 범위를 재정비하여 점검하는 등 이용자 정보 관리 및 조회·출력 절차를 강화하시기 바람