경영유의사항 등 공개안

1. 금융기관명 : (주)비바리퍼블리카

2. 조치일 : 2021. 3. 29.

3. 조치내용

대상	내용
기 관	경영유의사항 2건, 개선사항 13건

4. 조치대상사실

가. 경영유의사항

(1) 전자금융 및 IT부문 업무 내부통제 강화

회사는 '선불전자지급수단 발행 및 관리업' 및 '전자지급결제대행업(PG)' 등 전자금융업을 영위하고 있으나,

전자금융 및 관련 IT부문 업무에 대한 적정성, 준법성을 주기적으로 점검하는 준법감시·감사기능 등 내부통제 체계가 미흡하여 전자금융 및 IT부문 업무 전반에 걸쳐 미흡사항이 발견되고 있으므로

앞으로 전자금융 및 IT업무에 대한 적정성, 준법성을 주기적으로 점검할 수 있도록 감사 기능(IT포함)을 신설하고, 자체점검 항목 등을 마련하여 준법감시 기능을 강화하는 등 내부통제 체계를 강화할 필요가 있음

(2) 신규 영업행위 사전 준법성검토 강화

회사는 OO 앱을 통해 전자금융업(선불, PG 등) 이외에도 계좌 및 카드 통합 조회, 대출 맞춤추천 등 부가·제휴서비스를 제공하는 등 총 OO개 이상의 금융서비스를 영위하고 있으나,

신규 금융서비스를 출시하기 이전에 신규 영업행위 시 전자금융거래법 및 타 법률 위반 소지에 대한 사전 준법성 검토를 실시하는 내부통제체계가 갖추어져 있지 않아 신규 영업행위에 대한 충분한 사전 법률리스크 검토 없이 금융서비스를 출시하여 관련 법률을 준수하지 못할 우려가 있으므로

앞으로 신규 영업행위를 수행할 경우 이용자 권익보호, 사전 준법성 검토 등을 종합적으로 검토한 후에 서비스가 출시될 수 있도록 관련 내규 및 절차를 마련하는 등 내부통제 체계를 강화할 필요가 있음

나. 개선사항

(1) 선불전자지급수단 처리절차 불합리

선불전자지급수단(이하 'OO머니')을 발행하면서 간편송금, 간편결제, 더치페이 등 다양한 전자금융서비스를 OO머니로 제공하고 있으나,

기존 OO머니(앱)를 통한 간편송금 방식 이외 RCS* 기반 문자메시지를 통한 간편송금 서비스(계좌간 직접 송금서비스)의 경우 거래기록을 확인할 수 있는 OO 앱 메뉴('OO머니 거래내역')에서 출금·송금 내역 등이 조회되지 않아 거래기록 확인이 어려우며

* RCS(Rich Communication Suite) : 기존 통신사 문자메시지에 카카오톡과 같이 그룹채팅, 읽음확인 등 모바일 메신저 기능을 추가한 채팅서비스

계좌간 직접 송금서비스를 통해 충전잔액 이상의 금액을 송금하는 경우 송금 후 기존 충전잔액을 자동 재충전하고 있는 등 이용자의 의사와 관계없이 송금 전 충전잔액을 유지시키는 불합리한 처리방식으로 운영하고 있으므로

앞으로 이용자의 OO머니 사용내역(입금, 송금, 충전, 결제 등)을 통합 조회할 수 있도록 관련 시스템을 개선하고, 계좌간 직접 송금서비스의 경우 송금 후 기존 충전잔액을 자동 재충전하는 절차를 개선할 필요가 있음

(2) 본인인증절차 변경 보안성검토 미흡

내규 「OOOO규정」 제25조(OOOOOOO)에 의하면 이용자를 대상으로 신규 전자금융업무를 수행하거나 제휴서비스를 제공하는 경우 자체 보안성심의를 실시하여야 하나,

본인인증절차 변경 등 보안에 중요한 영향을 미치는 사항에 대해 보안리스크 평가 및 정보보호위원회의 심의·의결 없이 임의로 변경을 허용함에 따라 이에 기인한 전자금융사고가 최근 발생한 사실이 있으므로

앞으로 본인인증절차 변경 등 보안에 중요한 영향을 미치는 변경사항을 정의·분류하고, 동 사항은 보안성 검토 실시 후 정보보호위원회 심의·의결을 거치도록 관련 내규 및 절차를 마련할 필요가 있음

(3) 정보처리시스템 장애관리·통제 미흡

시스템 장애관리를 위하여 내규를 마련하고 장애 개요(장애시간, 장애시스템, 장애현상 등), 원인 분석 내용, 조치 결과, 재발 방지 대책 등의 내용을 포함하는 보고서를 작성토록 하고 있으나,

OOOO.OO.OO.부터 OOOO.OO.OO.까지 발생한 장애 건에 대하여 작성된 장애상황기록부 내용을 확인한 결과, 장애 개요, 원인 분석 내용, 조치 결과, 재발 방지 대책 중 일부 항목을 누락하여 작성하는 등 장애상황 기록·관리가 미흡하고,

OOOO.OO.OO. 'OOO OOO OO 프로그램 오류' 장애가 발생하여 프로그램 오류를 즉시 수정 조치하였으나, 오류로 인한 피해고객에 대한 전수조사 실시 등 영향도 분석과 장애조치의 적정성 사후점검 절차 등이 없어 장애처리에 대한 사후관리가 미흡하므로

앞으로 자체 장애등급·분류기준을 적용하고 장애상황기록부 작성내용을 누락 없이 기록·관리하도록 하며 장애처리 시 영향도 분석을 실시하는 등 장애처리 업무를 강화하고, 장애처리 종료 후 재발방지 대책 이행 등을 정기적으로 점검하는 등 장애관리 업무를 체계적으로 관리할 필요가 있음

(4) 고객센터 본인확인절차 불합리

이상금융거래탐지시스템(FDS)을 통해 부정의심 거래가 탐지되는 경우 이용자 계정을 즉시 차단하고 있으나,

동 계정 차단 후 이용자에게 관련 사실을 통지하지 않아 이용자가 계정 차단여부를 인지하기 어려우며,

이용자는 계정차단 해제를 위해 고객센터 상담채널을 통한 본인확인 시 촬영사진 확인 방식을 통해 본인확인 과정을 거치고 있어 단기간 내 다수 민원 발생이라는 문제 외

촬영사진 임의조작 등 위·변조에 취약한 문제점이 발생할 우려가 있으므로

앞으로 이용자 계정 차단 후 고객통지 절차를 추가하고, 이용자 계정 차단 해제 요청 시 자동화된 비대면 본인인증시스템을 구축하는 등 본인확인절차를 개선할 필요가 있음

(5) 전자금융기반시설 취약점 분석·평가 관리 미흡

① 매년 전자금융기반시설을 대상으로 자체전담평가반 또는 외부전문기관을 통해 취약점 분석·평가를 실시하였으나,

검사실시기간(OOOO.O.OO.부터 OOOO.O.O.까지) 중 OOOO 홈페이지에서 홈페이지 이용자의 OOOO OO를 확인할 수 있는 취약점이 발견되었고, OOOO 홈페이지에 내재된 OOOO 취약점으로 인해 홈페이지 OOO 및 OOO OOO이 확인되었으며,

OO O, OOO 홈페이지 등 웹서버에서 운영에 불필요한 파일, OO OO 암호화 알고리즘, OOO, OOO, OO OOOO 등이 발견되어 웹 페이지의 위·변조에 악용되거나 비공개 정보가 노출될 우려가 있으므로

앞으로 발견된 취약점을 신속히 제거하고 취약점 분석·평가 시 회사의 특성(어플리케이션, 인프라)을 고려한 취약점 분석항목 도출 등 취약점 분석·평가 관련 개선방안을 마련하는 한편, 공개용 웹서버의 보안 강화를 위해 OOOO 도입, OOOOO OOO 등 종합적인 대책을 수립할 필요가 있음

② 취약점 분석·평가 시 발견된 취약점이 조치가 불가한 경우 대표이사의 승인을 받아 위험 수용으로 처리하고 있으나,

위험 수용한 OOOOOO시스템 취약점(OOOO년)의 경우 비인가자가 OOOOOO으로 서버의 OOOO 파일을 호출하여 OOO 정보를 열람할 수 있는 취약점임에도 위험 수용으로 처리하였으며,

OOOO년 위험 수용한 서버 취약점의 경우 OOOO시스템 우회 시 시스템 중요정보 유출·삭제 등이 가능하여 사고위험이 높은 취약점임에도 위험 수용으로 처리하고 있으므로

앞으로 보안 취약점의 위험 수용시 위험 수용을 최소화하되 불가피하게 위험 수용 시에는 보완조치에 준하는 통제를 적용할 필요가 있음

(6) 문서파일·전산자료 반출통제 미흡

① 이용자 정보를 처리하는 내부업무시스템의 안전한 운영을 위해 접근통제, 신종 악성코드 감염 방지를 위한 차세대 방화벽 운영 등 보안대책을 적용하고 있으나,

내부업무시스템 고객정보의 외부 반출 시에는 OOOO 등이 일정 건(OO건) 이상 검출된 경우에만 책임자 사전 승인을 하고 있고, 내부업무시스템 접속화면에 대한 OOOO를 허용하고 있어 고객정보 등 전산자료 반출에 대한 사전 승인이 무력화될 위험이 있으므로

앞으로 고객정보 반출 시 검출건수와 상관없이 반출업무 담당자가 적정성을 검증하고 책임자 승인 후에만 반출하도록 하는 한편, 내부업무시스템에서 고객정보 조회 시 OOOO 방지 기능을 적용할 필요가 있음

② 인터넷 단말기로 반출된 고객정보의 경우 업무목적 달성 이후에도 해당 파일의 삭제여부를 확인하지 않고 있으며,

내부업무시스템에서 고객정보를 과다하게 반출한 직원에 대한 OO절차가 마련되어 있지 않고, 인터넷 단말기 내 회사의 각종 문서파일에 대해서는 인터넷을 통한 반출 차단 등 통제가 미흡하여 고객정보, 회사 중요 문서 등이 외부로 유출될 우려가 있으므로

앞으로 인터넷 단말기에 저장된 이용자 정보는 해당 업무목적이 달성된 이후에는 즉시 삭제하도록 하고 과다 반출자에 대한 OO절차를 마련하는 한편, 이용자 정보·회사 중요문서 등의 유출방지를 위한 보완대책을 마련할 필요가 있음

(7) 접근통제시스템 운영·관리 미흡

① 침입차단시스템의 보안규칙을 설정하면서 프로토콜 등 기능 및 서비스 포트번호를 특정하여 운영하고 있으나,

내부 정보처리시스템의 OOO OOOO 또는 외부인터넷 등에 대해 OOO OOOO를 특정하지 않고 네트워크 대역으로 접속을 허용하여 인가되지 않은 접속 및 통신이 발생할 우려가 있으므로

앞으로 침입차단시스템 보안규칙 설정시 기능 및 서비스 포트번호 뿐만 아니라 OOO OOOO와 OOO OOOO도 특정하여 적용할 필요가 있음

② 회사의 내부통신망 및 단말기를 통한 이용자 정보 유출에 대한 대응을 위해 고객정보유출방지시스템을 운영하고 있으나,

회사의 업무용으로 OOOOO(OO)을 사용하면서 동 메일시스템에는 고객정보유출방지시스템을 구축하지 않아 발송 메일의 첨부파일 및 본문을 통해 고객정보가 인가되지 않은 자에게 전송될 우려가 있으므로

앞으로 업무용 OOOOO(OO)에 대해 고객정보유출방지시스템을 도입하여 적용할 필요가 있음

③ 서버 접근통제시스템 및 DB접근통제시스템을 도입하여 운영하고 있으나,

OOO는 통제시스템의 운영체제 로그인 정책을 우회하여 서버에 로그인 후 다른 서버에 직접 로그인할 수 있도록 허용하였고, OOOO OOO OO의 경우 DB접근통제시스템을 통하지 않고 OOOO의 직접 로그인을 허용하고 있으므로

앞으로 서버 및 DBMS에 대한 접근통제시스템 규칙을 누락 없이 적용하고 서버 간 우회 접속을 금지할 필요가 있음

(8) 전자금융보조업자 재무건전성 및 품질수준 평가 관리절차 미흡

전자금융업자는 전자금융보조업자에 대한 재무건전성 및 서비스 품질수준을 연 1회 이상 평가하고 그 결과를 금융감독원에 보고하여야 하나,

OOOOO OOOO OOOO 이외의 전자금융보조업자에 대한 재무건전성 및 서비스 품질수준 평가를 실시하지 않았고, 보고 대상 전자금융보조업자의 재무건전성 및 서비스 품질수준 평가결과 보고를 누락하였으므로

앞으로 전자금융보조업자 내부 분류기준과 전자금융보조업자의 재무건전성 및 서비스 품질수준 평가절차를 내규에 반영하여 전자금융보조업자 평가를 강화하고, 보고일 기준 작성대상에 해당되는 전자금융보조업자에 대한 평가 결과를 보고하는 등 관리절차를 개선할 필요가 있음

(9) 자체 보안성심의 절차 미흡

① 신규 전자금융업무를 수행하거나 제휴서비스를 제공하는 경우 자체 보안성심의를 진행하고 있으나,

자체 보안성심의를 전자금융 서비스 개시 이후에 실시하는 등 안전성이 확보되지

않은 상태에서 서비스를 제공하는 사례가 확인되고 있으므로

앞으로 자체 보안성 심의 완료 후 서비스를 개시하고, 자체 보안성심의 실시 판단 기준과 운영절차를 내규에 반영하는 등 운영·관리절차를 개선할 필요가 있음

② 내규 「OOOO규정」에 자체 보안성심의 내용을 반영하고 있으나 하위규정인 지침 또는 절차서 등에 자체 보안성심의 실시 판단 기준과 세부 운영절차를 별도로 마련하고 있지 않아

업무 담당자가 자체 보안성심의를 요청하지 않을 경우 자체 보안성심의가 누락될 우려가 있으며, 자체 보안성심의 완료 후 금융감독원에 보고가 지연되는 사례가 다수 확인되고 있으므로

앞으로 신규 전자금융업무와 관련된 자체 보안성심의 결과보고가 누락되거나 지연되지 않도록 내규개정 등 관리를 강화할 필요가 있음

(10) 전자금융거래 약관 불합리

회사의 전자금융거래 약관에 이용자가 분쟁처리를 요청하는 경우에는 손해배상 등 분쟁처리에 대한 조사 또는 처리결과를 15일 이내에 이용자에게 알리도록 규정하고 있으며, 착오송금의 경우, 이용자가 이를 인지한 후 회사에 분쟁처리를 요청하면 회사가 이용자를 대신하여 착오 송금된 은행에 착오송금 분쟁을 신청하고 있으나,

이용자에 대한 착오송금 처리결과 회신에 통상 O주 ~ O주 정도가 소요되고 있어 약관에 따른 분쟁처리 기한 준수가 곤란하므로

앞으로 착오송금 관련 이용자 회신, 처리기한 적시 등 관련 분쟁처리 절차를 전자금융거래 이용약관에 반영하는 등 이용자 보호를 강화할 필요가 있음

(11) 비상계획 및 모의훈련 운영 불합리

비상상황 시 업무지속성을 확보하기 위해 내규 「업무지속성 확보방안(BCP) 및 재난복구 비상대책(DRP)」을 마련하고 이에 따라 연 O회 비상대응훈련을 실시하고 있으나,

하드웨어 고장, 일부 정보시스템 장애, 전력공급 중단 등 다양한 비상상황 발생에 대비한 재해복구 훈련을 실시하지 않았고,

위기관리TF 인적구성에 관한 최신상황이 적정히 관리되지 않아 OOOO 및 OOOO OO OOO 직원이 O명 이상 포함되어 있는 등 실제 비상상황 발생시 시스템 복구 등 상황판단의 어려움과 해당 담당자의 신속한 대응에 차질이 발생할 우려가 있으므로

앞으로 위기관리TF 변경사항을 최신화하여 관리하고 자산별 장애조치 방법을 포함한 다양한 비상상황 시나리오를 개발하여 상황별 대응능력을 제고할 수 있도록 비상대응훈련을 개선할 필요가 있음

(12) 정보처리시스템 성능관리 불합리

정보처리시스템 장애예방 및 성능 최적화를 위하여 내규「OOO OO지침」제14조에 따라 OO별로 정보시스템의 사용현황 및 추이 분석을 수행하고 있고 정보처리시스템의 OOO, OOO·OOO 사용량이 임계치(OO%)를 넘는 경우 시스템 담당자에게 알려주도록 운영하고 있으나,

분석 내용상 OO O OOOO 수치 현황·추이에 대한 모니터링 외에 포함되어야 할 분석·평가결과 내용을 포함하지 않아 이벤트 실시, 신규 서비스 오픈 등 장애 발생이 가능한 상황에 대해 예비 용량 확보 등이 적절하게 수행되었는지 확인하기 어려우므로

앞으로 정기적으로 인프라 성능과 사용량 추이, 이상 징후 발생에 대한 원인 등을 종합 분석하여 결과를 정기적으로 보고하도록 개선할 필요가 있음

(13) 프로그램 및 일괄작업 관리 통제 불합리

① 내규「OOOO규정」제5조에 따라 프로그램 등록·변경시 개발, 테스트 및 배포 등의 절차를 규정하고 형상관리프로그램을 이용하여 프로그램 요구사항 관리 및 변경 통제 절차를 운영하고 책임자 승인을 수행하고 있으나,

대부분의 프로그램 등록·변경을 승인하는 프로젝트 책임자를 일반적인 관리직책을 가진 자가 아니라 해당프로그램 담당 개발자 외 다른 팀원으로 지정하여 책임관계가 모호하며 프로그램 간 연계 오류 및 협업 부서의 개발 요구사항에 대한 총괄적인 검증 및 통제관리가 미흡하고

제3자에 의한 프로그램 내용 정당성 검증 수행 시 일부 프로그램은 자동화된 툴(tool)을 통해 보안성 검증 등을 수행하고 있으나,

자동화된 검증 이외에는 검증 담당자가 수동으로 검증을 진행하고 있어 검증 수준 및 정확성의 차이가 발생할 우려가 있으므로

앞으로 기존 프로젝트 책임자가 아닌 실질적인 관리책임을 수행할 자를 지정하여 프로그램 등록·변경을 승인토록 개선하고, 제3자에 의한 프로그램 내용 정당성 검증에 대해 자동화 검증 범위를 확대하거나 보안성 검증 수행 체크리스트 등을 통해 검증 담당자마다 검증수준을 유사하게 운영토록 개선할 필요가 있음

② 내규「OOOO규정」제6조에 따라 일괄작업(batch) 등록·변경시 절차를 규정하고 OOOOOOOOOO 관리시스템을 이용하여 일괄작업 등록하여 관리하고 있으나,

일괄작업을 수행하기 전 책임자 승인을 서면으로 수행하고 OOOOOOOOOO에 등록하여 관리하고 있어 사후 승인하거나 승인이 누락되는 등 통제가 미흡하므로

앞으로 일괄작업 승인을 시스템을 통해 사전에 수행하도록 개선하여 사후승인하거나 승인을 누락하지 않고 일괄작업이 수행될 수 있도록 일괄작업의 통제를 강화할 필요가 있음