경영유의사항 · 개선사항 공개

1. 금융기관명 : 카카오뱅크

2. 제재조치일 : 2023. 3. 30.

3. 조치내용

대 상	내 용
기 관	경영유의사항 2건, 개선사항 4건

4. 조치대상사실

가. 경영유의사항

(1) 비상대책 등의 수립·운용 강화

① 내규에 따라 ■■팀은 전사 업무영향분석(BIA)을 통해 단위업무를 도출하고 ☆☆☆☆☆☆팀의 적정성 검토를 받아 핵심업무를 선정하고 있으나

업무영향분석(BIA) 수행 시 부서 간 사전협의 절차가 미흡하여 전사 업무연속성계획과 IT업무연속성계획이 상이하게 관리되고 있고, 핵심업무 선정 과정에서의 보고체계가 미비하여 책임소재가 불분명할 우려가 있으며

실시간으로 처리되는 대고객 서비스에 대한 중요도 분석이 다소 미흡하여 일부 전자금융서비스의 복구목표시간(RTO)을 다소 길게 측정하고 있으므로

업무영향분석(BIA) 수행 시 업무부서와 IT부서가 협의를 통해 핵심업무를 선정·보고하는 등 공식적으로 합의·검토하는 절차를 마련하고, 실시간으로 처리되는 대고객 서비스의 복구목표시간(RTO)을 적정수준으로 산정하도록 관련 절차 및 기준 등을 재정비하시기 바람

② 내규에 따라 비상시 업무지속성 확보를 위해 별도의 내규를 마련하여 지침 및 매뉴얼 등에 반영하고 있으나

파업 시 필수 IT인력 확보 방안이 다소 미흡하고 비상대책위원회 등 임직원 비상연락망과 재해복구센터 전환을 위한 작업절차가 일부 누락되어 있으며,

전자금융사고 보고 절차와 재해복구 관련 매뉴얼의 배포 절차가 기술되어 있지 않고, 복구목표시간(RTO) 기준을 지침과 매뉴얼 간 상이하게 정의하는 등 비상대책 관련 내규가 다소 미흡하므로

비상대책 관련 내규에 파업 등 다양한 상황별 대응절차를 구체화하여 마련하고 ▲▲▲ 설정변경 등 누락된 작업절차를 보완하는 한편, 전자금융사고 보고 절차와 매뉴얼 배포 절차를 규정화하고 상이하게 관리되는 복구목표시간을 지침과 매뉴얼 간 동일하게 운영할 수 있도록 관련 내규를 재정비하시기 바람

(2) 제3자 서비스 관련 운영리스크 관리 강화

제3자와 제휴 및 업무 위·수탁 계약 등을 체결하여 ○○○○등의 주요 서비스를 고객에게 제공하고 있으나,

제휴 및 위·수탁 계약을 체결한 제3자의 전산시스템에 장애 및 재해 등으로 인해 은행의 전자금융거래 서비스가 중단될 경우, 회사의 주요 전자금융거래 서비스를 지속하기 위한 업무 대체수단이 마련되어 있지 않는 등 제3자와의 제휴 및 위·수탁 업무에 대한 업무지속성이 담보되어 있지 않으므로

제휴 및 위·수탁 업무에 대한 제3자 리스크를 식별하여 업무 대체수단을 확보하고 제3자와의 제휴 및 업무 위·수탁 시 업무 대체수단 등 리스크를 평가하는 절차를 마련하는 등 제3자 서비스 관련 운영리스크 관리를 강화하시기 바람

나. 개선사항

(1) 재해복구 전환훈련 불합리

내규에 따라 화재, 지진 등 재해 발생 시 업무지속성 확보 방안의 실효성을 검증하기 위하여 재해복구 전환훈련을 연1회 실시하고 있으나

조회성 업무에 대해서만 제한적으로 훈련을 실시하고 ◇◇◇를 포함한 대외기관들과의 연계 훈련을 수행하지 않고 있어 비상상황 발생시 신속한 대응이 어려울 우려가 있으며

훈련결과 분석 시 ■■■■시스템은 정상복구 여부만 확인하고 훈련 결과에 관한 증빙자료를 확보하지 않고 있어 복구훈련의 실효성이 담보되기 어려우므로

대외기관과의 연계, 데이터의 등록·변경이 수반되는 시나리오를 마련하여 재해복구 전환훈련을 실시하고, 훈련 상세결과에 관한 증빙자료를 확보하는 등 재해복구 전환훈련의 실효성을 제고하시기 바람

(2) 전산장비 장애 및 오류관리 업무 불합리

① 내규에 따라 오류인지, 보고, 등급산정 및 조치 등 오류관리에 관한 제반사항을 수립·운용하고 있으나,

전산장애·오류 발생 시 대응해야 할 총괄조직 및 담당자의 역할, 직무 분장 및 상세 대응 절차 등을 구체적으로 규정하지 아니하여 역할 및 직무가 명확하지 않고 책임소재 파악이 어려우며,

관련 내규의 핵심업무표가 상이하고, 내규 등에 전자금융사고 대응 프로세스가 포함되어 있지 않아 전자금융사고 발생 시 신속한 보고가 이루어지지 않을 우려가 있으므로

오류·장애 관련 내규에 전산장애·오류에 대한 총괄 조직 및 소관업무, 담당자 등을 정의하여 직무분장을 명확히 하고, 전자금융사고 대응 프로세스를 추가하며, 오류·장애 관련 내규 내 핵심업무를 재정리하는 등 오류·장애 관련 내규 및 절차를 재정비하시기 바람

② 전산장비의 장애·오류 등으로 인한 서비스 중단에 대비하여 주요 전산장비를 이중화 구성하고 있으나,

Active(운영)-Standby(대기) 방식으로 이중화 구성을 하는 경우, 신규 시스템 구축과정에서 전환 테스트를 수행한 이후 별도의 전환 테스트를 수행하지 않아 비상 상황 시 원활하게 전환되지 않을 우려가 있으므로

주요 전산장비의 전환 테스트가 주기적으로 이루어질 수 있도록 관련 내규에 반영하고, 정기적으로 전환 여부를 검증하여 전산장비 업무지속성을 확보하시기 바람

(3) 네트워크 보안대책 불합리

① 내규에 따라 정보처리시스템의 특성과 필요한 보호대책의 수준을 고려하여 네트워크를 구성·운용하고 있으나,

△△△△△△ 등 네트워크 관련 시스템의 비정상 트래픽에 대한 접근통제가 일부 미흡하여 ●●●●●의 접속이 간헐적으로 지연되는 등 네트워크 정책 설정 미흡으로 ●●●●● 서비스가 원활하게 제공되지 않을 우려가 있으므로

앞으로 비정상 트래픽에 대한 접근통제 정책을 강화하고 네트워크 구간에서 병목현상이 발생하지 않도록 네트워크 장비의 경로설정 정책을 점검하는 등 ●●●●● 서비스가 원활히 제공될 수 있도록 네트워크 구간에 대한 보안대책을 개선하시기 바람

② 내규에 따라 △△△△△△ 등 네트워크 관련 시스템을 도입하여 ◎◎◎ 정책 변경 절차를 통해 인가받은 서비스에 대해서만 접근을 허용하는 등 네트워크 접근통제 정책을 수립·운용하고 있으나,

◎◎◎ 정책 변경 신청 시 해당 서비스가 재해복구센터에도 적용이 필요한지 여부 등을 사전에 확인하는 절차가 마련되어 있지 않아 실제 재해 상황 발생 시 재해복구센터 ◎◎◎ 정책 누락으로 인하여 신속한 서비스 전환에 어려움이 발생할 수 있으므로

앞으로 ◎◎◎ 정책 변경 신청 시 재해복구센터 적용 필요성을 사전에 확인할 수 있는 절차를 마련하고, 네트워크 보안대책 관련 업무절차를 개선하시기 바람

(4) 전산자료 소산매체 관리 불합리

내규에 따라 전산센터 소실 등 비상상황 발생 시 전산자료의 신속한 복구 등을 위하여 주기적으로 전산자료를 백업·소산하고 백업 및 소산자료에 대한 적정성 등을 검증하고 있으나,

소산된 매체를 재해복구센터 사무실 내 내화금고에 보관하고 있어 인가되지 않은 외부주문 인력 등이 백업자료에 접근할 우려가 있고, 적절한 항온항습 시설, 소화설비 등이 다소 미흡하여 소산매체의 적정수명을 보장하지 못할 우려가 있으므로

소산매체가 보관된 내화금고를 출입 통제장치 및 적절한 항온항습 시설, 소화설비 등이 마련된 별도의 장소에 보관하고, 소산업무 담당자 등 인가된 직원만 출입할 수 있도록 통제하는 등 전산자료 소산매체 관리를 강화하시기 바람