경영유의사항 등 공개안

1. 금융기관명 : ㈜카카오뱅크

2. 제재조치일 : 2022. 7. 25.

3. 제재조치내용

제재 대상	제재 내용
기관	• 경영유의사항 18건
	• 개선사항 26건

4. 제재대상사실

가. 경영유의사항

(1) 고객 앞 은행의 중요한 의사표시 안내 시 메시지 내용 검증 강화

○ 대출과 관련한 중요한 의사표시를 고객에게 안내하기 전에 메시지 내용의 오류 여부 등에 대한 검증 프로세스가 부재하여

'18.2.20.(최초 상품출시일) ~ '☆☆.☆.☆☆. 기간 중 대출약정 직후 고객에게 발송(LMS)한 '대출 약정내용' 상 기준금리 적용에 대한 내용을 오안내*하는 등 고객 통지사항에 대한 검증절차가 없으므로

* 전월세보증금대출의 기준금리는 2영업일 전의 은행연합회 고시 신규취급액 기준 COFIX(6개월) 금리이나 실행 당일자의 COFIX(6개월) 금리가 적용된다고 안내

중요한 의사표시 내용*은 ☆☆☆☆부의 사전검증 절차를 마련하는 등 대고객 통지서비스를 강화할 필요가 있음

* 기한전의 채무변제(기한의 이익 상실) 독촉, 상계 · 질권(저당권) 실행 통지 등

(2) 금융소비자보호 모범규준을 반영한 소비자 권익보호 미흡

○ 「금융소비자 보호 모범규준('20.1.1. 개정 시행)」*에 따라 은행은 소비자 피해예방은 물론 금융소비자 권익 확대를 도모하여야 하는데도

* ① CEO가 소비자 보호에 관심을 갖도록 하고, 소비자보호 총괄책임자(CCO)의 독립성 및 권한을 강화 ② '금융소비자 중심 경영인증제' 도입을 통한 금융소비자실태평가 실효성 제고 ③ 소비자의 권리 · 부담사항을 수시 · 정기적으로 고지 ④ 휴면 · 장기 미청구 금융재산 발생의 예방·감축을 위한 절차·기준 마련

여신업무 관련 채무관계자에 대한 권리·부담사항 등의 정보제공 부실*로 소비자 피해 사례가 발생하고 있는데도 관련 사례가 ★★팀 등 관련부서에 전파되지 않고 있으므로

* 은행의 중요한 의사표시가 배달증명부 내용증명 우편이 아닌 LMS로 발송, 전월세보증금대출 기준금리 적용 고객 앞 오안내, 후불교통카드 소액연체 고객 앞 통지서비스 미흡 등

원활한 소비자보호 업무 수행을 위해 소비자보호 실무인력을 충분히 확보하고, 중대한 소비자 피해 우려 등의 경우 그 결과를 대표이사에게 보고하는 등의 개선방안을 마련할 필요가 있음

(3) 계열사 등과의 거래시 내부통제 절차 미흡

○ 내규「이사회규정」제11조 등에 의하면 주요주주 등과의 거래 시 이사회 사전 결의를 받아 거래의 내용과 절차의 공정성을 확보하여야 하는데도

주요주주 등과의 거래 시 이사회 사전 결의를 거치지 않았거나(▽건), 거래상대방별 연간 거래가능 금액을 연 1회 사전 승인을 받고 동 금액 내에서 이루어지는 거래에 대해서는 거래의 내용에 관계없이 별도로 이사회 사전 결의를 받지 않은 사례가 있어* 이해상충 발생 가능성이 높은 거래 등에 대한 이사회 차원의 적정성 검토가 충실히 이루어지기 어려운 상황이므로

* 검사대상기간 중 주요주주 등과의 거래 ▽▽▽건 중 동 사전 포괄승인으로 이사회 결의를 실시한 건은 ▽▽건(▽▽.▽%)

앞으로는 주요주주 등과의 거래 시 이사회에서 개별 거래의 내용과 절차의 공정성 등을 사전에 충실히 검토할 수 있도록 관련 업무 프로세스를 강화할 필요가 있음

(4) 자체감사 기능 및 감사조직 운영 강화

㈎ 내부감사 계획 수립 철저

○ 은행은 내규「감사규정」제6조 등에 따라 종합검사, 부문감사, 특별감사, 상시감사 등을 실시할 수 있으나, 내부 감사인력 부족 등의 사유로 대부분의 감사를 특정 테마에 대한 부문감사 형태로만 실시하고 개별 조직 업무 전반에 대한 종합감사는 거의 실시하지 않아* 일부 부서에서 조직적인 비위 행위가 발생한 사례**가 있으므로

* 2017년 영업 개시 이후 종합감사 실시 사례는 ▼건(▼▼▼▼.▼월, ▼▼▼▼팀)

** 2017년 이후 팀 고유의 업무에 대한 내부감사가 이루어지지 않았던 ○○팀의 경우 ○○○○.○○월 팀 업무와 관련한 자산횡령 등으로 상당수 팀원이 징계(면직~견책)를 받은 바 있음

앞으로는 특정 업무에 대한 감사공백이 장기간 발생하지 않도록 내부감사 계획을 철저히 수립할 필요가 있음

㈏ 상시감사 업무 실효성 제고

○ 은행은 내규「감사업무지침」제47조 등에 따라 전산시스템 등을 활용한 상시감사를 실시*하고 있으나, 검사대상기간 중 상시감사 결과가 시정·개선 등으로 이어진 사례가 매우 적은(◁건) 등 이상거래 추출의 유효성이 부족하고, 이상거래 의심 건에 대한 확인 기한도 정해져 있지 않아 비정상적인 업무 수행에 대한 즉각적인 대응이 이루어지지 않을 우려도 존재하므로

* 검사기준일 현재 ◁◁개의 상시감사 항목(차주외 제3자 대출원리금 상환 등) 운영중

상시감사 항목별 유효성 점검 등을 통해 실효성을 제고*하는 한편, 이상거래 의심 건에 대한 즉각적인 사유 확인이 가능하도록 관련 프로세스를 강화할 필요가 있음

* 장기간 이상거래 의심 건이 추출되지 않는 항목이거나, 이상거래 의심 건은 추출되나 실제 이상거래로 이어지는 경우가 미미한 항목 등은 유효성 점검을 통한 개선이 필요

㈐ 내부감사 사후관리 철저

○ 내규「감사규정」제20조 등에 의하면 ●●팀은 자체 감사를 통해 수감부서에 필요한 조치를 실시하고 이에 대한 정리 결과를 보고받아 관리하여야 하는데도, 수감부서가 ●●팀 지적사항에 대한 정리 결과를 정해진 기일 내에 회신하지 않은 사례가 다수 확인*되었으며, 정리가 지연된 건에 대한 ●●팀의 관리도 소홀하게 이루어지고 있으므로

* 검사대상기간 동안 사후관리가 필요한 지적 건 중 ◁◁.◁%가 지연정리(◁◁◁건 중 ◁◁건)

앞으로는 지적사항에 대한 정리가 신속히 이루어질 수 있도록 사후관리 프로세스를 강화할 필요가 있음

㈑ 감사위원회의 감사보조조직 장에 대한 통제 강화

○ 내규「감사위원회규정」등에 의하면 감사위원회는 효율적인 업무수행을 위해 팀 단위의 감사보조조직을 둘 수 있고, 동 감사보조조직의 장은 감사위원회를 보좌하며 감사위원회로부터 위임받은 감사업무 등을 수행하고 있으나

감사보조조직의 장이 조직 내 팀원으로부터 동료평가만 받고 감사위원회로부터는 평가 등의 통제를 받지 않고 있어 충실한 감사위원회 보좌 역할 및 감사업무 수행이 이루어지지 않을 소지가 있으므로

감사보조조직의 장으로서의 역할 및 직무 등을 반영한 성과평가 등이 이루어질 수 있도록 관련 제도를 정비할 필요

(5) 이사회 및 소위원회 운영절차 철저

○ 이사회 및 소속 위원회 운영과 관련하여 아래와 같이 미흡한 점이 있으므로 이사회 및 소속 위원회가 본연의 기능을 충실히 수행할 수 있도록 관련 업무 프로세스를 강화할 필요가 있음

㈎ 이사회 및 소속 위원회 안건 제공 충실

○ 이사회 및 소속 위원회 내규*에 의하면 각 회의 안건 등을 회의 개최일 3일 전까지 위원들에게 배포하도록 되어있는데도 회의 개최 전 촉박하게 배포한 사례**가 다수 있는 등 경영상 중요한 의사결정과 관련하여 사전 검토시간이 충분히 보장되지 않는 우려가 있으므로

* 「이사회규정」 제10조, 「보수위원회규정」 제5조 등

** 검사대상기간 중 '회의 개최일 ~ 안건 송부일'이 3일 미만인 건 : 이사회 ◀◀건, 운영위원회 ◀◀건, 보수위원회 ◀건, 임원후보추천위원회 ◀건 등

위원들이 회의 개최 전 안건 검토를 충분히 할 수 있도록 회의 안건 송부 기한을 재검토하고 불가피한 사유가 아니라면 이를 단축하지 않도록 운영할 필요가 있음

㈏ 이사회 및 소속 위원회 의사록 작성 철저

○ 이사회 및 소속 위원회 내규*에 의하면 회의 안건, 경과의 요령 및 결과 등을 의사록에 충실히 기재하고 참석 위원들의 기명날인 또는 서명을 받아 보관하여야 하는데도

* 「이사회규정」 제16조, 「보수위원회규정」 제10조 등

의사록에 위원들의 발언 내용이 기재되어 있지 않은 경우가 상당수 확인되었으며 일부 위원의 기명날인 또는 서명 관리가 특별한 사유 없이 장기간 지연되는 사례*도 있는 등 의사결정 과정에 대한 기록·관리가 전반적으로 미흡하므로

* (예시) 2021년 제2차, 제3차 임원후보추천위원회 등

앞으로는 위원들의 발언내용 등을 의사록에 충실히 반영하고 위원들의 서명관리도 철저히 하여 회의체 운영의 투명성과 책임성을 제고할 필요가 있음

(6) 사외이사 후보군 관리 및 평가절차 미흡

㈎ 사외이사 후보군 관리 미흡

○ 사외이사 후보를 추천 시 ◎◎팀이 관리하고 있는 사외이사 후보군에 편입될 후보를 대부분 지원부서인 동 부서가 추천하고, 외부자문기관 등에 의한 추천을 전혀 활용하지 않고 있으므로

사외이사 후보군의 추천 경로를 다양화하고, 후보군 현황을 주기적으로 점검하는 등 후보군 관리를 강화할 필요가 있음

㈏ 사외이사 평가절차 미흡

○ 사외이사 평가* 시 이사회 발언기록 등에 근거한 지원부서 평가가 미흡**하고, 지배구조 연차보고서 상 사외이사의 평가결과가 일부 사실과 다르게*** 기록되었으므로

* 자기평가, 상호평가, 지원부서 평가의 3가지 방식으로 수행

** 이사회 발언기록 등을 참고한 평가가 이루어지지 않았으므로 해당 기록 등을 참고하여 평가에 객관성을 기할 필요

*** 사외이사의 평가결과가 5점 만점 기준 4~5점임에도 불구하고, 모든 사외이사가 '전 부문에서 최고 수준을 득점'한 것으로 기재

앞으로는 사외이사 평가가 정확히 이루어지고, 평가결과의 신뢰성을 높일 수 있도록 사외이사 평가절차를 개선하고, 평가결과에 대한 공시의 정확성을 제고할 필요가 있음

(7) 합리적인 성과평가기준 및 보수체계 설계·운영 미흡

㈎ 합리적인 성과평가지표 설정 및 성과급 지급률 결정 필요

○ 임원별 업무 범위 및 역할이 상이함에도 특별한 사유 없이 대다수 임원*에 대해 대표이사와 동일한 성과평가지표에 따라 평가하고 있으며, 임원에 대한 실제 보수 결정 시 보수위원회가 사전에 정해놓은 평가등급별 성과급 지급률과 무관하게 대표이사가 임원별 최종 보수지급률을 결정하여 성과평가 결과와 실제 성과보수가 연동되지 않으므로

* 최고기술책임자(CTO), 최고서비스책임자(CSO), 최고비지니스책임자(CBO), 정보보호최고책임자(CISO) 등

임원별 업무 등을 감안하여 성과평가지표를 재설정하는 한편, 불합리한 보수지급률 조정이 발생하지 않도록 하여 관련 업무 절차를 개선하여 성과평가 결과와 실제 성과보수간 연동성을 강화할 필요가 있음

㈏ 성과평가기준 상 내부통제 부문 강화

○ 내규 「보수위원회규정」, 「내부통제위원회규정」 등에 의하면 은행은 임직원이 과도한 위험을 부담하지 아니하도록 보상체계를 마련하고 내부통제 점검 결과 등을 임직원 평가에 반영하여야 하나 임직원 성과평가기준상 법규준수 등 내부통제와 직접적으로 관련된 항목이 포함되어 있지 않으므로

성과평가기준에 내부통제기준 준수와 관련한 평가 항목을 추가하는 등 평가보상 체계가 내부통제기준 준수 유인으로서의 기능할 수 있도록 유의하시기 바람

㈐ 성과평가지표 및 보상기준의 수립의 적시성 강화

○ 매년 보수위원회의 임원 성과평가지표 및 보상기준 등의 결정이 지연(통상 6월 이후)*되어 연초부터 약 6개월간 성과평가지표 및 보상기준이 없는 문제점이 있으므로

* 임원 성과평가기준 보수위원회 결의 시점 : 2019년도 2019.目.目目. , 2020년도 2020.目.目. 등

앞으로는 임원에 대한 성과평가지표 및 보상기준이 적시(예 : 1분기 내)에 수립될 수 있도록 절차를 개선하는 등 관련 업무를 철저히 하시기 바람

㈑ 보상 결정 과정의 투명성 확보

○ 2019.3월 임직원에게 주식매수선택권을 부여 과정에서 보수위원회의 사전심의, 이사회·감사위원회의 주주총회 상정 안건 검토, 준법감시인 사전심의, 일상감사 등 중요한 내부 의사결정 절차가 불충분·불투명하게 이루어졌으므로*

* 1) 보수위원회 : 보수위원회 안건에 주식매수선택권 부여기준, 조건 등에 대한 판단 근거가 기재되어 있지 않으며, 위원회 의사록에도 관련 내용을 논의한 기록이 부재
2) 이사회·감사위원회 : 주주총회 개최 전 이사회·감사위원회의 주주총회 안건 검토 시 실제 주주총회 안건과 상이한 안건(주식매수선택권 부여에 관한 상세내용 등 부재)으로 논의가 진행
3) 준법감시·일상감사 : 주주총회, 이사회 및 소위원회 안건 부의 등의 내부결재를 진행하면서 안건 세부 내용이 제외된 문서로 준법감시인 사전심의 및 일상감사 등이 이루어짐

앞으로는 보상과 관련한 의사결정 시 관련 위원회 및 조직에 필요한 정보를 충분히 제공하고, 구체적인 논의 내용 등을 투명하게 기록하는 등 관련 업무를 철저히 할 필요가 있음

㈐ 성과보수의 장기성과와의 연계 강화

○ 내규「보수위원회규정」등에 의하면 은행은 임원의 성과보수 중 상당부분을 주식 또는 주식연계상품 등 장기성과와 연동될 수 있는 형태로 지급할 수 있고, 개인의 업무에서 손실이 발생한 경우 지급 미확정 부분은 실현된 손실규모를 반영하여 재산정할 수 있다고 규정하고 있으나

은행은 임원에 대한 이연된 성과보수 지급 시 임원 중 사내이사에 대해서는 주가에 연계하는 방식 등으로 이연된 성과보수를 장기성과와 연계하여 지급하고 있으나, 그 외 임원*에 대해서는 주가 연계하거나 이연기간 중 손실발생 규모를 반영하는 등의 절차가 충실히 이루어지지 않고 있으므로**

* 최고기술책임자(CTO), 정보보호최고책임자(CISO) 등

** 보수위원회 차원에서 임원의 이연된 성과보수 지급 시 손실 발생규모 등을 검토한 기록이 남아 있지 않음

앞으로는 임원에 대한 성과보수가 은행의 장기성과와 충실히 연계되어 지급될 수 있도록 보수위원회에서 관련 논의를 별도로 실시하고, 이에 대한 기록을 유지하시기 바람

(8) 자체 징계 및 포상 업무 수행 미흡

㈎ 자체 징계 업무의 합리성·투명성 제고

○ 검사대상기간 중 직원의 위규행위와 관련하여 ●●팀에서 내부감사 결과를 바탕으로 징계를 요구한 건들에 대하여 인사위원회 또는 대표이사가 대부분 요구양정 대비 감경하여 조치*하고 있으나

* 검사대상기간 중 ●●팀의 요구양정이 '주의' 이상인 건 중 인사위원회 또는 대표이사가 감경한 건은 ●●%(●●건 중 ●●건)

합리적이지 않은 사유('부서의 인력부족' 등)를 감경 사유로 적용하거나, 인사위원회 안건·회의록, 대표이사 결재문서에 징계수준 판단 근거, 감경 적용 사유 등이 남아 있지 않은 사례가 확인 되었으므로

앞으로는 자체 징계 시 관련 규정 등에 근거하여 합리적이고 명확한 사유가 있을 경우에만 감경을 적용하고, 징계수준 판단 근거, 논의 내용 등을 기록으로 충실히 남기는 등 징계 절차의 투명성을 강화할 필요가 있음

㈏ 징계 수준 결정의 적정성·일관성 제고

○ 임직원의 금융관련 법령 위반 사항에 대해서도 특별한 사유 없이 내규상 징계가 아닌 '주의환기'로 조치한 사례가 있어 징계조치의 관대화에 따른 임직원들의 법규준수 의식 저하 우려가 존재하므로

징계 양정 판단을 위한 내부 기준 마련 등을 통해 징계 수준 결정의 적정성 및 일관성을 제고할 필요가 있음

㈐ 합리적인 포상 제도 운영 필요

○ 은행은 상시적으로 업무성과가 우수한 직원들에게 포상을 실시하고 있으나, 포상 부여 기준 및 자격 요건 등이 마련되어 있지 않아 포상 제도가 다소 불합리하게 운영된 사례가 있으므로*

* 우수한 성과로 포상을 받은 조직이 이듬해 자산횡령 등으로 징계를 받거나, 담당업무와 관련한 징계 조치 후 포상을 부여한 사례 등

포상 제도가 내부통제 중심의 조직문화 정착에 기여할 수 있도록 포상 부여 기준 및 자격 요건을 마련하는 등 관련 업무 절차를 강화할 필요가 있음

(9) 고문계약 체결 업무 미흡

○ 은행은 ▥▥▥▥.▥▥.▥▥. 사내이사직을 사임한 임원과 고문 계약을 체결하면서 고문 계약의 필요성 검토 및 계약 체결과 관련한 필수적인 내부통제 절차(준법감시인 사전심의, 일상감사 등)를 이행하지 않았으며, 계약 체결 이후에도 고문 내역에 대한 사후관리 등을 실시하지 않은 사실이 있으므로

고문제도와 관련한 내규상 운영 근거를 마련하는 한편, 고문 계약 필요시 사전에 필요성·업무범위 등에 대한 검토를 실시하고 실제 고문 내역에 대한 기록관리·평가 등도 실시하는 등 관련 업무를 보다 철저히 할 필요가 있음

(10) 외환송금 퇴결 관련 금융소비자보호 미흡

○ 은행은 금융소비자의 권익 증진을 위해 금융소비자보호를 위한 경영방침을 정하고 이를 공식적인 문서로 표명하는 노력을 기울이고 있으나, 고객의 해외송금*(▨▨▨ ▨▨▨▨)의 퇴결과 관련하여

* ▨▨은행 자회사인 ▨▨▨▨▨▨▨▨▨▨의 결제망을 통해 송금처리, 동 위탁계약을 통해 미국, 캐나다, 프랑스, 독일, 스페인 등 총 19개 국가에 송금 가능

외화송금 퇴결 시 고객의 정보정정(수신자 계좌번호 등) 요청이 불가한 가운데,

고객(송금인)의 계좌에 퇴결금액이 원화로 재입금되어 환차손이 발생*할 수 있으며, 내규에 따른 송금수수료**는 고객에게 반환하지 않아 고객은 금전적인 손실이 발생한 것으로 인지할 가능성이 있으므로

* 예) 1만불 상당의 1천만원을 송금하였으나, 2일후 퇴결시점의 환율을 적용하여 송금계좌에 990만원 입금
** [송금수수료, 할인정책無] 송금액 5천불이하: 5천원(정액), 송금액 5천불초과: 1만원(정액)

금융소비자보호 및 민원예방 차원에서 퇴결금액 입금 시 우대환율을 적용하여 환차손 발생을 최소화하고, 송금수수료 일부를 반환*하는 등의 운영기준을 마련하여 관련 내부규정을 정비하는 한편, 중장기적으로는 외화계좌를 통한 퇴결금액 입금 등 환차손을 방지하는 방안을 검토할 필요가 있음

* 송금수수료와 은행의 실제비용(지급비용 1,500원 등)간의 차이

(11) ●●팀의 IT부문에 대한 감사활동 강화 필요

○ 내규 「감사규정」에 IT감사를 통해 정보기술 부문의 안전성·건전성을 평가하도록 하고 종합감사, 부문감사, 특별감사 및 일상감사 등의 방법으로 감사를 실시하도록 규정하고 있으나,

관련 내규에 종합감사에 대한 실시주기가 정의되어 있지 않고, 검사대상 기간 중 IT부문 전반에 대한 종합감사 실시 없이 ◎◎팀 및 ◇◇◇◇팀 대상 테마검사 성격의 부문검사(6회*)만을 실시하고 있으므로,

* IT보안 및 정보보호 실태점검, 개인정보보호 실태점검, 전자금융서비스 장애처리 실태점검 등

인터넷전문은행 특성상 IT업무가 차지하는 비중이 큰 점을 감안하여 IT부문 업무 전반에 대해 실질적인 감사가 이루어질 수 있도록, 관련 내규에 종합감사 실시주기를 반영하여 주기에 따라 종합감사를 실시하는 등 IT부문에 대한 감사활동을 강화하시기 바람

(12) IT자체감사 체계 강화방안 마련

○ IT자체●●팀은 은행의 IT업무를 수행하는 ◎◎팀 및 ◇◇◇◇팀에 대해 자체감사업무를 수행하고 있으나,

IT자체●●팀에서 IT정책 및 내규관리, IT비상계획 수립·관리 등 감사대상 업무를 함께 수행하고, 일일감사·월별감사 등 주기별 감사 없이 반기별 수시감사 형태로만

감사를 실시하고 있으며,

IT자체●●팀 직원에 대한 업무성과 평가시 ◎◎팀 내 다른 팀 직원들을 상호평가자로 지정할 수 있도록 평가체계가 구성되어 있고,

IT자체●●팀의 감사대상 업무를 수행하고 있는 ◆◆◆◆◆팀(IT도입, IT변경관리, 경영업무시스템 개발·운영 등)을 총괄하는 팀장(◆◆◆◆◆팀장)이 감사업무에 대해서도 통할하여 관리하고 있어, 감사업무의 독립성이 훼손될 우려가 있으므로,

IT자체●●팀의 이해상충 소지가 발생하지 않도록 업무를 분리·조정하고, 주기별 감사와 특명감사 등을 확대 실시하는 한편,

IT자체●●팀 감사업무에 대한 보고·통제 체계 개편(1차 조직장인 ◎◎팀장 직접 수행 등), 업무성과 평가체계 변경 등 IT자체감사 체계의 독립성을 확보하시기 바람

(13) 스크래핑 방식 대외기관 연계 서비스의 연속성 제고

○ 대출상품(개인신용대출, 마이너스통장대출, 개인사업자 대출)의 비대면 서비스 제공을 위해 대외기관(▶▶▶▶▶▶, ▶▶▶▶▶▶ 등)에서 제공하는 고객의 소득정보 자료를 스크래핑 방식*으로 수집·처리하고 있으나,

* 웹사이트에서 사용자 대신 정형화된 정보를 자동화하여 추출하는 방식

검사대상 기간 중 발생한 총 ▶▶건의 장애내역 중 동 대외기관(▶▶▶▶▶▶, ▶▶▶▶▶▶ 등)의 화면 구성 변경 등으로 인한 스크래핑서비스 관련 장애가 다수 차지(▶▶건, ▶▶.▶)하는 등 스크래핑서비스 관련 장애가 지속적으로 발생하고 있으므로,

스크래핑서비스의 안정성 제고를 위해, 스크래핑서비스 대상 대외기관에 대한 모니터링을 강화하고,

서비스 장애 시 장애내역 공지, 공공 마이데이터 사업을 통한 단계적 API방식 전환 추진 등 이용자 불편을 최소화할 수 있도록 서비스의 연속성 제고 방안을 수립·운용하시기 바람

(14) 취약점 조치 이행관리 강화

○ 전자금융기반시설 등에 대해 취약점 분석·평가를 정기적으로 실시하고 있고, 취약점 이행조치 결과는 정보보호위원회의 심의·의결을 거쳐 최고경영자에게 보고하고 있으나,

2020년 발견된 취약점에 대한 조치율이 ♤♤.♤%로 저조하고, 다수 취약점*이 차기 점검 기간까지 제거되지 않고 잔존하고 있는 등 취약점 조치 및 제거 이행계획을 기한 내 완료하지 못하고 있고

* 최근 2년간 장기 미조치 상태인 취약점은 ♤♤♤개, 재발견된 취약점은 ♤♤♤개

기술적으로 조치 가능한 취약점임에도 '다수 서버 적용 어려움' 등 불가피성을 인정하기 어려운 사유로 위험수용으로 처리하고 있으며,

위험수용 대상을 정보보호위원회 심의·의결 안건에 포함하여 최고경영자에게 일괄 보고·승인하고 있어, 취약점을 제거하지 않아 발생 가능한 문제점을 최고경영자가 명확하게 인지하지 못할 우려가 있으므로

취약점 제거 및 조치가 지연 없이 이행될 수 있도록 취약점 조치 이행 현황에 대한 주기적인 점검 실시, 반복적으로 발견되는 취약점에 대한 조치 방안을 수립하는 등 통제·관리 방안을 마련하고

불가피한 취약점에 대한 위험수용 처리 관리 기준을 마련하며, 최고경영자가 관련 문제점 등을 충분히 인지한 이후, 위험수용 승인 여부를 결정할 수 있도록 절차를 마련하는 등 취약점 조치 이행관리를 강화하여 운영하시기 바람

(15) 중금리대출 취급 활성화 및 개인신용정보 보호대책 마련

○ 은행의 연계대출(대출의 중개·주선) 겸영업무 취급*과 관련하여 자체 중금리대출이 위축되지 않도록 유의하고, 고객의 개인(신용)정보 보호대책을 마련하도록 하였으나

* 금융감독원 겸영업무 신고('♠♠.♠.♠♠.) 관련 '겸영업무 신고결과 통보(♠♠♠♠♠-♠♠♠, '♠♠.♠.♠.)

'19.4월 ~ '21.3월 기간 중 총 연계대출 취급액은 ♠♠,♠♠♠억원으로 동 기간 순

수 중금리(중신용)대출 취급액(♠,♠♠♠억원) 대비 약 ♠.♠배 수준으로 과도하고, 제휴사 공동 개인(신용)정보 수집·이용·제공 동의서 상 대출 미체결 시 보유·이용 기간을 정보제공일로부터 법 상 기간(3개월)이 아닌 6개월 이내 파기하도록 하고 있으므로

중·저신용자 전용 신용대출 신상품을 출시*하는 등 관련 대출의 공급을 확대하고 제휴사 공동 개인(신용)정보 수집·이용·제공 동의서 양식을 개정할 필요가 있음

* 주주사 및 통신데이터 등을 활용한 신용평가모형을 개발·적용

(16) 대손충당금 관련 리스크요소(부도율) 산정 방식 불합리

○ 대손충당금 산정을 위한 집합평가 부도율(PD) 추정시 부도율 산정을 위한 기준시점에는 존재하지 않았으나 관측기간 중 신규로 발생하는 부도(이하 신규부도)를 부도율 산식*에 반영하지 않아 대손충당금이 과소 산정될 우려가 있으므로

* 바젤 부도율 = (기준시점 정상 차주 중 부도차주 + 관측기간 중 신규부도) / (기준시점 정상차주 + 관측기간 중 신규부도)

대손충당금 산정을 위한 부도율(PD) 추정 시에도 신규부도를 반영하도록 관련 절차를 개선하시기 바람

(17) 여신감리 업무의 독립성 및 실효성 제고

○ □□□□부서는 여신관련부서의 여신취급실태 및 자산건전성 분류 등의 재검토 결과를 이사회 등에 보고하는 기능을 적절히 수행할 수 있도록 독립적으로 운영하여야 하나

위험관리위원회에 부의하는 자료 검토결과, □□□□팀의 '권고의견'이 1건에 불과하고, 위험관리최고책임자(CRO)를 비롯한 □□□□팀(□□□□□팀) 및 감리대상업무 수행팀*이 한 공간에서 구분 없이 근무함에 따라 □□□□팀의 감리업무 수행이 적절하게 운영되지 않고 있으며,

* 감리대상업무 수행팀 : ■■■■■팀, △△△△△△△△팀, ▲▲▲▲▲▲▲▲팀

향후 신사업 확장* 과정에서 감리 담당 인력 부족으로 여신감리 정책이 소홀히 운영될 우려가 있으므로 신사업 확장에 맞춰 관련 인력 및 조직을 보강하는 등 독립적이고 실효성 있는 여신감리 정책을 추진할 필요가 있음

* 금년 중 중금리 관련 신상품 출시, 주택담보대출 및 중소기업대출 등

(18) 대출금리 산출체계 합리성 제고

○ 은행은 대출 기준금리 및 리스크프리미엄 등 주요 가산금리를 합리적으로 산정·운용하기 위하여 산출기준에 관한 사항 등 임직원이 직무를 수행할 때 따라야 할 기본적인 절차와 기준을 내규에 반영*하여야 하는데도

* 「대출금리 체계의 합리성 제고를 위한 모범규준」 제16조

내규 상 리스크프리미엄, 자본비용, 목표이익률에 대한 구체적인 산출기준을 정하지 않고* 재무전략협의회에서 안건으로 검토하여 승인처리하고 있으며, 내규 상 산출기준이 명확하게 명시되어 있지 않은 업무원가에 대해서도 일부 연도별 산출기준을 상이하게 운영**한 사실이 있으므로

* 산출의 기본 원칙(예: '조달리스크프리미엄이라 함은 당행의 리스크로 인해 시장에서 유통되는 은행채AAA에 비해 당행이 조달을 위해 추가로 지급해야하는 금리를 말한다.')만을 내규에 규정
** 간접업무원가율 산정방식이 명시되어 있지 않으며, 직접업무원가율 산정 관련 연도별 스크래핑비용, 비상금대출 미사용한도 보증료율 산정방식도 상이

대출금리 구성항목별 합리적인 산출기준을 구체적으로 내규화하고 산출내역을 충실하게 문서화하는 등 대출 가산금리 산정방식 및 운영체계를 강화할 필요가 있음

나. 개선 사항

(1) 대주주에 대한 신용공여 통제 절차 개선

은행은 내규「여신규정」제6조 등에 따른 대주주(대주주의 특수관계인 포함)에 대한 신용공여 통제 시 대부분의 절차를 수기로 진행하고 있어 신용공여 금지 위반 사례가 지속·반복 발생될 우려가 있으므로

대주주와의 정보 공유방법을 개선하고, 전산시스템에 입력한 대주주 정보에 대한 검증절차를 마련하는 등 관련 업무절차를 개선하여 대주주에 대한 신용공여 금지 위반 사례가 사전에 방지될 수 있도록 개선하시기 바람

(2) 금융거래정보 제공사실 통보 업무 개선

「금융실명거래 및 비밀보장에 관한 법률」상 거래정보등 제공사실 통보 업무와 관련하여 아래와 같이 불합리한 점이 있으므로 관련 전산시스템 및 절차를 개선하시기 바람

① 거래정보등 제공사실 통보 업무의 내부시스템 개선 필요

은행은 법원 등 대외기관 정보제공 업무 중 결과등록을 수기로 시스템에 입력하는 방식으로 등록함에 따라 직원의 업무상 부주의로 결과등록을 지연하여 거래정보등 제공사실 통보업무가 지연되는 등 다수의 법 위반사항이 발생한 바 있으므로, 정보제공결과 미등록 건에 대해 일별 알림 및 점검프로세스를 구축하는 방법 등으로 전산시스템을 통해 거래정보 제공사실 통보업무가 관리·통제되도록 개선하시기 바람

② 정보제공 및 제공결과 명의인 통보업무에 대한 전결규정 미비

♡♡♡♡♡팀은 거래정보등 제공사실 통보업무에 대해 전결규정이 없고, 책임자 점검 절차가 미흡함에 따라 통보가 지연된 건에 대해 검증이 부실하여 법 위반사항이 발생한 바 있으므로, 직무전결기준을 정비하여 권한과 책임을 명확히 하고, 개정된 전결기준에 따른 책임자 점검 프로세스를 추가하여 거래정보등 제공사실 통보업무 관련 내부통제를 개선하시기 바람

③ 통보서 우편발송 결과에 대한 처리내역 관리·감독 강화

은행은 대외기관 정보제공 업무를 수탁업체(♥♥♥♥㈜)에 위탁하고 있으나, 발송결과에 대한 검토 프로세스를 갖추지 않아 명의인 통보업무에 대한 사후관리가 미흡하므로 수탁업체의 통보대행업무에 대한 모니터링을 강화하는 등 관련 내부통제를 개선하시기 바람

(3) 개인신용정보 관리절차 개선

고객의 개인신용정보 관리 업무와 관련하여 아래와 같이 불합리한 점이 있으므로 관련 전산시스템 및 절차를 개선하시기 바람

① 개인신용정보 동의서 양식 개선

은행은 개인(신용)정보 동의서상 제공 목적을 상품·서비스 개선 및 제안을 위한 데이터 분석, 고객 금융 데이터 분석 목적으로 운영하고 있어 과도한 고객 정보 활용의 가능성이 있으므로

상거래관계의 설정 및 유지 등의 사항 외의 목적으로 개인신용정보를 수집·이용하는 경우 고객이 개인신용정보 제공 여부를 선택할 수 있도록 개선하시기 바람

② 개인신용정보 동의내역 및 조회기록 관리 개선

은행의 개인신용정보 제3자 정보 제공을 위한 고객 동의내역 관리*의 일관된 기준이 부재하여 동의내역 관리가 미흡하고 일부 개인신용정보 조회가 가능한 시스템의 조회로그에 조회 항목이 불명확**하여 조회로그의 적정성 점검이 미흡하므로

* 제3자 정보제공이 필수 전제 조건인 서비스 중 일부는 시스템 구조상 고객이 동의하는 경우에만 서비스 이용이 가능하도록 통제하고 있어 어플리케이션의 화면 접속 로그로만 동의 내역 확인 가능

** 빅데이터플랫폼 및 캠페인시스템내 고객대상 선정 화면의 조회로그는 사용자 ID, SQL 등을 적재하며 특정 고객을 조회하는 경우에만 사유를 검토

고객 동의여부, 동의일 등을 전산 상 저장하도록 개발하고 조회로그에 조회 항목 등을 명확히 하여 조회로그에 대한 적정성 모니터링을 강화할 수 있도록 개선하시기 바람

③ 빅데이터플랫폼 권한 관리 개선

은행의 빅데이터플랫폼 테이블에 대한 조회 권한 부여·회수 작업이 수작업으로 진행되고 있어 작업이 누락될 가능성이 있으므로

빅데이터플랫폼 개별 테이블에 대한 권한 부여의 적정성 점검을 강화하여 권한 승인 절차를 개선하시기 바람

(4) 수익증권 위험가중자산 산출 관련 통제 절차 강화

집합투자증권의 익스포져에 대해 기초자산접근법을 적용하여 위험가중자산을 산출하는 경우 은행은 집합투자증권의 기초자산에 대한 상세한 정보를 적시에 입수하여 실제 은행이 기초자산을 보유하는 것처럼 위험가중치를 적용하여야 함에도

자산운용사로부터 이메일 등 비공식적으로 집합투자증권의 기초자산 명세를 입수하는데, 입수한 기초자산 명세에 대한 내부 검증 프로세스가 미비*함에 따라 일부 거래 상대방에 오류가 있는 기초자산 명세가 입수되었음에도 이를 검증하지 못하여 '20년말 위험가중자산 계산 시 오류**가 발생하였으므로

* 데이터 정합성 검증 절차 등이 있으나 명세 입수 부서(◉◉◉◉팀, ◉◉◉팀)간의 업무 R&R이 명확하지 않음

** 기초자산 명세상 환매조건부채권 거래의 거래상대방이 ◉◉◉◉◉◉◉(RW 100%)임에도 ◉◉◉◉◉◉◉(20%)으로 오입력됨에 따라 위험가중자산이 ◉.◉백만원 과소 계산

자산운용사로부터 기초자산 명세 입수시 공문 등 정식적인 절차에 따라 입수하고 입수된 자산명세에 대해서 검증 절차 및 데이터 검증 체크리스트를 보완하는 등 집합투자증권 위험가중자산 산출 관련 통제절차를 개선하시기 바람

(5) 비상금대출 연장 시 가산금리 인상 제한 기준 적용

신용대출, 마이너스대출의 경우 대출연장 시 가산금리 인상을 제한*하고 있으나, 비상금대출(SGI보증 대출)의 경우 가산금리 인상 제한을 적용하지 않음**에 따라

* 대출연장 시 가산금리 인상분이 2%p를 초과하는 경우 초과분에 대해 감면

** 은행은 차주의 신용도 하락에 따라 보증료율(가산금리의 일부) 상승 시 가산금리도 많이 상승할 수 있어 보증부대출인 비상금대출에 대해서는 가산금리 인상 제한을 적용하고 있지 않았음

여타 대출대비 과도한 금리 인상이 있을 수 있으므로 비상금대출에 대해서도 가산금리 인상 제한을 적용할 필요가 있음

(6) 대출채권 매각에 관한 내부통제기준 마련

「채권추심 및 대출채권 매각 가이드라인」에 따르면 대출채권 매각 업무*를 수행함에 있어 일관된 기준**을 마련해야 하는데, 현재 관련 기준이 없으므로 내규 상 「대출채권 매각 기준」을 마련할 필요가 있음

* 개인회생, 신용회복 확정 즉시 대출채권 추정손실 분류 후, 1회차 납부 시 상각 후 매각

** 채권 매각과 다른 채권 처리 방법(예 : 채권추심회사에 추심 위임, 자체 추심, 대손상각, 경매 등)간의 비용 편익 및 정책 목적 등을 고려하여 일관된 기준 필요

(7) 준법감시업무 관련 법규위반사항 보고절차 개선

내규 「준법감시업무메뉴얼」에 따르면 정기점검 결과 법규위반사항에 대해서는 준법감시 · 법무팀장(2차조직장)에게 보고하여야 하는데도

2020년 3분기 이후부터 준법감시 정기점검 결과보고를 3차 조직장에게만 보고하는 등 준법감시 정기점검 관련 보고 절차가 미흡하고, ●●팀 통지 기준 및 절차에 관한 사항이 미비하여* 준법감시업무 사후관리절차가 미흡하므로

* 법규위반 사항에 대한 ●●팀 통지규정 미비

법규위반 사항 발생 시 준법감시 · 법무팀장(2차조직장)에게 보고하고, ●●팀 통지 기준 및 절차를 마련하는 등 관련 내규를 개선하시기 바람

(8) 협상에 의한 계약 업무처리절차 미흡

내규 「계약규정」은 도급, 구매 등 계약을 하는 경우 계약의 방법을 일반경쟁입찰, 희망수량경쟁입찰, 제한경쟁입찰, 지명경쟁입찰, 수의계약 및 협상에 의한 계약 등의 방법으로 수행토록 하고 있으나,

'협상에 의한 계약'에 대해서는 제안서 평가 및 협상 방법 등의 업무처리절차가 구체적으로 정의되어 있지 않아,

검사대상 기간 중 '협상에 의한 계약'의 방법으로 계약을 체결한 ◉◉건 중 ◉◉건*의 계약이 수의계약과 유사한 절차로 계약이 체결**되는 등 계약방법이 불명확하므로,

* '경영지원망 메일발송 전용 ◉◉◉ ◉◉ 구매' 등

** 1~4개의 업체로부터 견적서를 제출받아 제품의 적정 여부만 평가하고, 최저가 제안업체와 계약 체결 등

'협상에 의한 계약'의 방법에 대한 업무처리절차를 구체적으로 정의하여, 동 절차에 따라 계약업무가 수행될 수 있도록 내규를 개정하는 등 관련 업무절차를 개선하시기 바람

(9) 전산자료 백업 및 소산업무 불합리

① 전산자료 백업 내역에 대한 적정성 검토 절차 마련

내규 「IT인프라관리지침」에 따라, 데이터의 중요도, 자료의 보관주기 및 복구 목표시간 등을 고려하여 전산자료 백업대상을 선정하여 주기적으로 백업하고 있으나,

시스템별 백업 대상 및 백업실시 내역의 적정성 검토를 주기적으로 대사하는 절차가 마련되어 있지 않아 운영시스템의 데이터 백업이 누락될 우려가 있으므로,

전산자료 백업 대상, 백업 전산자료의 누락여부, 정상 백업 자료의 무결성 등을 주기적으로 검토하여 백업자료의 적정성을 점검하는 절차를 마련·운영하시기 바람

② 소산 전산자료에 대한 검증방법 개선

백업 · 소산된 전산자료에 대한 데이터 검증, 실제 장애 및 재해 상황에 대비한 데이터 복구 능력 배양 등을 위해 소산 매체 및 전산자료에 대한 검증 훈련을 연 2회 이상 실시하고 있으나,

데이터 검증 훈련시, 계정계 DB데이터를 복구한 이후 소산 전산자료의 검증 과정에서 일부 암호화된 전산자료*를 복호화 검증하고 있어, 훈련기간 중 비인가자에 의한 불필요한 전산자료의 조회 및 유출이 발생될 우려가 있고,

* 특정 거래일자의 1초간 발생한 수신 거래내역 중 고객번호 및 계좌번호

계정계(AP, DB) 시스템 전산자료만 백업 ·소산하고 있어 장애·재해발생시 소산 대상 외에는 복구하기 어려우므로

소산전산자료에 대한 검증 훈련시 암호화된 전산자료의 형태로 소산 전산자료의 정합성을 점검하고, 채널계 및 정보보호시스템, 운영체제 및 설정내용 등의 주요 전산자료가 소산대상에 포함하여 관리할 수 있도록 관련 절차 및 시스템 등을 개선하시기 바람

(10) IT업무 연속성 계획의 실효성 강화

① 업무 연속성 계획의 적정성 검토절차 마련

재해 등으로 인한 전산센터(서울시 마포구 상암동 소재) 마비에 대비하여 업무지속성을 확보할 수 있도록 총 728개 단위업무를 5단계*로 분류하고, 이 중 155개 업무를 핵심업무로 선정하여 재해복구시스템을 구축·운영하고 있으나,

* 단위업무를 5등급으로 세부 분류하고, 이 중 1등급 핵심·중요 업무에 대해 재해복구시스템 구축

전사적 업무영향분석*을 통해 선정한 핵심업무와 ◎◎팀이 선정한 IT핵심업무를 비교·분석하여 핵심업무 지정의 적정성, 재해복구시스템 구축 필요성 등을 점검하는 절차가 마련되어 있지 않으므로,

* 은행 영업연속성의 위험요인을 파악하기 위한 영업영향분석(BIA)을 ○○팀에서 담당

전사적 업무영향분석과 ◎◎팀의 IT업무 영향도 분석을 상호 연동하여 실시할 수 있는 절차를 마련하여 은행의 핵심업무가 재해복구시스템 구축대상에 누락되지 않도록 관련 업무절차를 개선하시기 바람

② 재해복구센터 내 대외기관 통신망 구축

재해복구센터(경기도 성남시 분당구 야탑동 소재)에 핵심업무 중심으로 재해복구시스템을 구축·운용하고 있으나,

일부 주요 업무(신용대출, 햇살론, 휴면예금찾기 등) 관련 대외기관*(총 4개 기관, 5개 회선)과의 통신망이 재해복구센터에 구성되지 않아 주전산센터 재해 발생 시 관련 업무가 중단될 우려가 있으므로,

* □□□□□(통신사만 이원화), □□□ □□□□□□, □□□□□□, □□□□□□□□(□□□, □□□□□□) 등

재해복구센터 내 미구축 대외기관 등과의 통신망을 보완하는 등 업무연속성 계획의 실효성을 강화하시기 바람

(11) 경영지원망 및 클라우드 저장소 내 전산자료 통제 강화

내부통신망을 금융업무망*과 경영지원망(인터넷망)**으로 분리구성하고 있으나,

* 전자금융업무 및 고객정보를 처리하는 업무망
** 사내 시스템(그룹웨어, 게시판 등) 운영 및 업무자료 공유·보존 등의 목적으로 클라우드 저장소 서비스(G-Suite Google Drive)를 활용하고 있으며, 경영지원망 단말기 및 클라우드 저장소 내 고객정보가 포함된 전산자료가 취급·저장되지 않도록 개인정보탐지솔루션(DLP)을 적용하여 운영

경영지원망 단말기와 클라우드 저장소에서는 주민등록번호 등 고유식별정보를 대상으로만 개인정보탐지솔루션을 운영하여 신용정보 등 중요정보가 유출 될 우려가 있으므로,

금융업무망 정보처리시스템을 통해 생성된 전산자료를 금융업무망 내에서만 처리할 수 있도록 제한하고, 경영지원망으로 이관되는 전산자료에 대한 검증절차를

강화하는 한편,

경영지원망 단말기와 클라우드 저장소에 저장이 가능한 전산자료의 세부 운용기준을 마련하여, 정기적으로 주요 전산자료 저장의 적정성을 점검하고, 개인정보탐지 솔루션 정책을 강화하는 등 관련 전산시스템 및 절차 등을 개선하시기 바람

(12) 시스템 영향도 분석 및 테스트 강화 필요

내규 「IT개발지침」 등에 따라 프로그램 신규 개발 및 유지보수시 테스트 자동화 도구 등을 활용하여 단위테스트, 통합테스트, 인수테스트 등을 실시하고, 모바일앱 테스트 전문 조직(QA*)을 구성·운영하고 있으나,

* 품질보증(Quality Assurance)

프로그램 변경·배포, 정보처리시스템 패치·구성변경 등의 작업과정에서 기존 프로그램 처리방법, 전문규격 등을 변경하는데도 동 변경작업에 대한 사전 영향도 분석·검토가 미흡하여, 테스트 단계에서 오류를 발견하지 못하고 운영시스템에 반영되어 거래내역 알림 메시지 오류, 대출실행내역 및 약정서 대량 중복 발송 등이 발생된 사례*가 있으므로,

* 알림톡 메시지 오류('21.3.), 계정계 로직 변경 오류('20.9.), 조회 및 이체 외 상품개설 중단 오류('20.7.), '대출실행내역 및 약정서 안내' 대량 e-mail 발생 오류('18.7.) 등

신규 서비스 출시, 프로그램 변경, 정보처리시스템 구성변경시 장애·오류를 방지하기 위하여 운영시스템 및 서비스의 사전 영향도 분석을 강화하고, 영향도 분석 결과에 따른 리스크를 프로그램 테스트시 반영하도록 관련 전산시스템 및 절차 등을 개선하시기 바람

(13) 프로그램 유지보수에 필요한 문서화 방법 불합리

내규 「IT개발지침」에 정보처리시스템의 개발 업무 관련 프로젝트 관리 및 테스트 절차 등을 마련하여 운영하고 있으나,

관련 내규 등에 프로그램 등록·변경·폐기 및 상세 테스트 수행 결과, 정보처리시스템 운영에 필요한 의사결정사항 등 프로그램의 유지보수시 필수적인 사항에 대해 문서화 대상을 정의하지 않아 업무 수행 내역의 적정성 및 프로그램 변경통제 내역의 정확성 확인이 어려워질 수 있으므로

프로그램 유지보수 등 정보처리시스템 운영의 주요 세부사항을 문서화 대상으로 규정하여 준수하는 등 관련 내규 및 절차 등을 개선하시기 바람

(14) 오픈소스 프로그램 관리방안 불합리

검사착수일 현재, 모바일뱅킹 앱에 활용되는 오픈소스에 대해서는 라이선스 정책 고지의무*에 따라 앱프로그램 관련 오픈소스 활용내역을 식별하여 고지하고 있으나,

* ☺☺☺☺☺☺ License ☺.☺, ☺☺☺ License, ☺☺☺ License 등

프로젝트 관리, 프로그램 개발, 빅데이터 분석 등 내부 업무처리에 오픈소스 프로그램*을 다수 도입·운영하고 있음에도, 회사 내 오픈소스 활용현황의 식별·관리 등 관리절차가 마련되지 않아 오픈소스 프로그램 활용으로 인한 리스크**가 발생할 우려가 있으므로

* ☺☺☺☺☺☺☺(빌드·배포관리), ☺☺☺☺(이슈관리), ☺☺☺☺☺☺(형상관리), ☺☺☺☺☺☺☺☺(정적코드분석) 등
** 공개된 소스코드로 인한 중요 취약점 노출, 패치 무결성 검증 리스크 등 보안위협 및 오픈소스 라이선스 사용 저작물의 소스코드 공개 · 분쟁, 라이선스 양립성 등의 리스크

오픈소스 프로그램에 관한 도입·활용·유지보수 등 생명주기 전반에 걸친 관리체계를 마련하는 등 오픈소스 프로그램 통제·관리를 개선하시기 바람

(15) 암호 프로그램 및 암호화키 관리대책 불합리

내규 「암호화관리지침」을 수립하여 암호프로그램 및 암호키 관리 방안을 마련하여 등록된 암호프로그램 및 소스 코드에 대해 비인가자의 접근 및 이용을 통제하고, 암호프로그램의 원시 소스 코드는 별도의 저장매체(CD 및 보안USB)에 저장하고 내화금고 등 안전한 장소에 보관토록 정하고 있으나,

검사착수일 현재, ◇◇팀 등 소관부서 담당자의 신청으로 암호프로그램을 등록하도록 하여 취약한 암호화 알고리즘을 사용하거나 암호화 알고리즘 사용 연한 도래 등 암호프로그램 적정성 검증이 누락될 우려가 있으며

암호프로그램 및 암호키를 보관하는 내화금고에 대한 통제절차가 미흡*하고, 내화금고에는 암호프로그램의 원시 소스코드 등을 별도 보관하고 있지 않는 등 암호프로그램의 관리 절차가 미흡하므로,

* 내화금고를 ◇◇◇◇팀 사무실 內 공용공간에 배치하고 있으나, 별도의 CCTV 및 출입통제장치 등이 마련되어 있지 않고, 내화금고의 비밀번호를 암호프로그램 담당자가 아닌 ◇◇◇◇◇팀 공동

으로 관리토록 운용

은행에서 사용하는 암호프로그램에 대해 전수 조사를 진행하여 암호프로그램의 목록을 주기적으로 현행화하여 관리하고 암호프로그램 및 암호화키 관련 통제 절차 등을 개선하시기 바람

(16) ITSM 내 장애보고서 관리절차 불합리

정보처리시스템 장애 발생 시 장애일시, 장애내용 및 조치사항 등을 기록하여, ITSM시스템에 장애상황기록부를 등록하여 관리하고 있으나,

장애발생 원인이 프로그램 변경 또는 시스템 작업인 경우 등 원인행위 및 조치결과가 장애상황기록부에 상세히 기록·관리하지 않아, 장애원인 및 처리과정의 적정성 등을 확인하기 어려우므로

ITSM시스템 내 장애보고서와 장애발생 원인 및 조치결과를 연계하여 체계적으로 관리할 수 있도록 관련 전산시스템 및 절차 등을 개선하시기 바람

(17) 전산원장 통제절차 강화 필요

내규「IT데이터관리지침」에 의하면, 프로그램 오류 등으로 인한 전산원장 변경 절차 등을 마련하고, 데이터의 변경 전후내용 자동기록 및 보존을 위한 전산원장 통제용 전산시스템*을 구축·운영하고 있으나,

* '전산원장 변경 이력관리 시스템', 'DB접근통제 시스템', 'SQL 소명 시스템' 등

전산원장 변경 전용 단말기(1대)를 ◇◇◇팀 사무실 內 공용장소에 배치*하고 있어, 비인가자에 의한 전산원장 정정용 단말기 접근, 전산원장 무단조작 등이 발생할 우려가 있고,

* 별도의 CCTV 및 출입통제장치 등 미마련

전산원장 변경작업시 IT자체감사 담당자가 ◇◇◇팀의 전산원장 변경과정 및 결과를 확인하고 있으나, 세부 확인기록이 없어 업무수행의 적정성 확인이 어려우므로,

전산원장 변경 전용 단말기를 출입통제 장치가 마련된 별도의 업무 공간으로 옮기고 전산원장 변경내용의 정당여부에 대한 제3자 확인을 거치는 등 전산원장 변경통제 절차를 개선하시기 바람

(18) 고객데이터 암호화 정책 관리 불철저

주민등록번호 등 주요정보를 데이터베이스(DB)에 저장하면서 암호화하여야 하는 대상을 메타데이터시스템*으로 정의하고, DB암호화 솔루션을 통해 암호화 저장·관리하고 있으나,

* 테이블 컬럼 상세 설명, 레이아웃 정의를 위해 메타데이터시스템을 운영

메타데이터시스템 암호화 대상 선정기준이 명확하지 않아 테이블별로 암호화 적용 대상이 상이하고, 일부 업무는 개발자 판단으로 암호화 여부를 결정하고 있어 암호화 대상이 누락될 우려가 있으므로,

데이터베이스 암호화 대상 선정기준을 명확히 마련하여 고객정보 등 주요 정보 저장시 일관된 암호화 기준이 적용될 수 있도록 메타데이터시스템에 반영하고, 암호화 대상이 누락되지 않도록 관련 전산시스템 및 절차 등을 개선하시기 바람

(19) 챗봇서비스 관련 고객 데이터 관리 불합리

고객상담 챗봇서비스*를 제공하면서, 챗봇서비스 관련 고객과의 대화 내역을 수집하고, 수집한 정보를 빅데이터 분석 등에 활용하여 고객 편의를 제공하고 있으나,

* 카카오 엔터프라이즈에서 제공하는 “카카오i 커넥트톡” 서비스를 활용하여 카카오톡으로 상품설명 및 제출 서류 안내 등을 수행

플랫폼 제공 사업자(카카오 엔터프라이즈)와의 계약서에 고객 정보(대화기록, 카톡ID 등) 보관 주기, 관리 방법, 삭제결과 확인 등 관리 절차가 명시되어 있지 않고, 수집된 고객과의 대화(상담) 기록이 플랫폼 제공 사업자(카카오 엔터프라이즈*) 및 카카오뱅크에 암호화되지 않고 저장되어 개인정보 유출 우려가 있으므로,

* 빅데이터 분석을 위해 30일간 보관하고 삭제

플랫폼 제공 사업자(카카오 엔터프라이즈)와 고객 정보 관련 전산자료에 대한 구체적인 관리 절차 등을 마련하여 계약서 등에 보완·적용하고, 카카오 엔터프라이즈 및 카카오뱅크가 보관중인 고객과의 대화기록에 대해서도 암호화를 적용하는 등 고객 데이터 보호 절차를 개선하시기 바람

(20) 이상금융거래탐지시스템(FDS) 운영 실효성 제고

비정상 이상금융 거래 등에 대한 탐지·차단을 위해 FDS*를 구축하고, 이상거래 탐지를 위한 시나리오(총 ◈◈개)를 마련·운영하고 있으나,

* Fraud Detection System

검사대상 기간 중 전체 이상거래 탐지 시나리오 중 16개는 탐지 사례가 없는데도 탐지 시나리오 존치여부에 대해 검토를 하지 않고

ATM 및 카드 관련 이상거래의 경우 자체 FDS에 별도 탐지 시나리오 등을 마련하지 않고, 카카오뱅크의 체크카드 승인업무를 위탁·운영하고 있는 KB카드 FDS의 탐지 시나리오에 의존*하여 운영하고 있으며,

* KB카드의 탐지 시나리오 총 ◈◈◈개 중 카카오뱅크가 ◈건(◈.◈%)의 시나리오를 추가

사고 개연성이 높은 고위험* 이상거래의 경우 영업시간 외에는 고객에게 정상거래 여부 확인 및 본인확인 등의 절차를 수행하지 않아 이상거래 탐지 후 후속대응**이 누락될 우려가 있으므로,

* 블랙리스트 기기를 활용한 로그인 및 이체, ATM을 통해 단기간 소액을 다수 출금하는 경우 등
** 중위험 거래에 대해서는 ARS 등을 통한 확인 절차로 24시간 대응 중

이상거래 탐지 시나리오의 적정성을 유관부서와 정기적으로 점검하여 신규 위험에 대응할 수 있는 탐지 시나리오의 지속적인 개발, 기존 이상거래 탐지 시나리오의 임계치 및 탐지조건의 조정, ATM 및 카드 관련 이상거래에 대한 고도화 방안 마련 등을 통해 탐지 실효성을 제고하고 야간 및 주말에 탐지된 고위험 이상금융거래에 대한 대응 절차 등을 개선하시기 바람

(21) 정보처리시스템 성능관리 대상 선정 미흡

정보처리시스템의 장애예방 및 성능의 최적화를 위하여 주요 정보처리시스템을 선정하여 스토리지, CPU, 메모리에 대한 성능을 집중 모니터링하고 있으나,

정보처리시스템 성능분석 대상 선정시 별도의 선정 기준을 마련하지 않아 코어뱅킹, 채널, 인증 서버 등 일부 정보처리시스템만을 대상*으로 수행하고, 일부 주요 정보처리시스템(오픈뱅킹, UMS, 통합운영DB 서버 등)을 성능분석 대상으로 포함하지 않아, 추이분석 및 증설 필요여부 검토 등 사전 예방조치를 적기에 하지 못할 우려가 있으므로,

* 총 ▣,▣▣▣대 중 코어뱅킹, 채널, 인증 서버 ▣▣▣대만 성능분석 대상으로 선정

업무 및 자산의 중요도 등을 고려하여 성능분석 대상 선정기준을 마련하고, 성능분석 대상을 확대하는 등 정보처리시스템 성능관리 절차를 개선하시기 바람

(22) 정보처리시스템에 대한 접근통제 불합리

서버 등 정보처리시스템 접속시 서버 접근통제 시스템을 활용하여 계정 및 비밀번호 이외에 OTP 등을 활용한 추가 인증절차를 적용하고 있으나,

서버 가상화시스템(Vmware, Nutanix)의 관리자 계정*은 추가인증 절차가 없어 관리자 계정으로 로그인하면 개별 가상화시스템에 직접 접속이 가능하여 접근통제가 다소 취약하고

* 서버 가상화시스템은 가상화된 다수의 서버를 최상위 관리자 계정으로 통합 관리·접속이 가능하도록 구성되어 있어, 최상위 관리자 계정이 해킹 등 위험에 노출될 경우 다수의 서버가 동일 위험에 노출

가상화시스템에 관리자 계정으로 접속 후 일시적으로 시스템 로그인을 종료*한 경우 별도 로그인 과정없이 재접속이 가능하여 접속통제 절차 등이 무력화 될 우려가 있으므로,

* 접속창에서 아무런 작업을 하지 않아 접속이 끊긴 경우 등

서버 가상화시스템의 관리자 계정을 통한 정보처리시스템 접속 시에도 추가인증 절차를 적용하고, 서버 재인증 절차를 강화하는 등 관련 전산시스템 및 절차 등을 개선하시기 바람

(23) 무선통신망 운영·관리 불합리

금융업무망과 인터넷망(경영망)에 무선통신망을 구축하고 비인가 무선통신망 사용을 통제하기 위하여 무선접속장비(AP) 및 무선침입방지시스템(WIPS)를 구축·운영하고 있으나,

검사착수일 현재, 총 7대의 단말기(공용단말기 포함)에 대하여 무선통신망을 이용한 금융업무망 접속을 예외·허용('모니터링' 사유)하면서 공식화된 무선통신망 사용신청·승인 절차*를 거치지 않아 사용에 대한 정당성을 확인하기 어렵고,

* 내규「정보처리시스템보안지침」및「무선통신망 사용신청 기준/절차」에는 무선통신망 이용 업무를 최소한으로 하고 무선사용에 대한 용도를 명확히 하도록 규정

인가 단말기에서 비인가 AP간의 접속 등은 WIPS에서 '차단' 하면서도 비인가 단말기와 비인가 AP와의 통신은 '탐지' 기능만 적용하여 비인가 AP 접속에 대한 실시간 차단·대응이 곤란하므로,

금융업무망에서 무선통신망 사용신청 시에는 업무 용도를 명확히 하여 내부 사용 신청·승인 절차를 거쳐 정당성을 확인하고, 전산센터 등 중요시설에 대해서는 비인가 통신에 대한 실시간 차단 정책을 적용하는 등 관련 전산시스템 및 절차 등을 개선하시기 바람

(24) 전산자료 보안관리 대책 불합리

전산자료의 유출을 방지하기 위하여 사용자 단말기에 문서암호화 프로그램(DRM)을 구축하여 주요 문서파일*에 대한 암호화를 적용하고 있으나,

* doc, docs, xls, xlsx, ppt, pptx, hwp, pdf

Mac 단말기*의 경우 프로그램 호환성 사유로 문서암호화 프로그램(DRM) 설치를 예외**적용하여 동 단말기에서 생성한 문서는 저장 시 암호화되지 않아 전산자료 유출 우려가 있고

* 업무용 단말기의 종류(Windows 또는 Mac OS기반)를 임직원이 직접선택 할 수 있어 전체 임직원에게 지급된 단말기 5,514대 중 Mac 단말기는 480대(8.7%)

** 보안문서를 열람하기 위해 별도의 문서열람 전용 프로그램을 설치하여 사용 중

통합단말시스템 조회결과에 대한 다운로드 및 데이터 관리에 빈번하게 사용하는 문서파일(csv/txt, accdb 등)을 암호화 적용 대상으로 등록하지 않아 대량 데이터 파일에 대한 암호화 누락 우려가 있으며,

또한, 금융업무망에서 '복사 및 붙여넣기(추출)' 기능을 허용하여 암호화에서 비암호화 문서에 암호화 없이 편집·저장이 가능하여 문서 암호화 정책을 우회할 위험이 있으므로

금융업무망에서는 문서암호화 프로그램을 모든 단말기에 적용하기 전까지는 업무상 불가피성이 인정되는 경우에만 Mac 단말기 사용을 허용하고, 개인정보탐지 정책 및 점검을 강화하는 등 추가 보안통제 대책을 적용하여 업무용 단말기 내 중요 전산자료에 대한 암호화 관리를 강화하며

통합단말시스템 및 데이터 관리에 사용되는 주요 문서파일에 대한 암호화 적용 대상 확대, 암호화 미적용 문서에서 암호화된 문서 내용 편집·저장 금지 등 문서암호화 프로그램의 보안대책을 개선하시기 바람

(25) 통합단말시스템 보안관리 불합리

통합단말시스템*의 화면 접근권한을 공통 및 부서업무 별로 부여하고, 분기 1회 권한부여 내역 및 사용 현황에 대한 적정성을 검토하고 있으며, 「개인정보취급자 업무 매뉴얼」의 개인정보 표시제한 보호조치 기준에 따라 주민등록번호 등 주요 고객정보를 마스킹 하는 정책을 운영하고 있으나,

* 카카오뱅크의 수신·여신·카드·외환 등 전자금융업무를 관리하는 업무 시스템

화면 접근권한 신청·변경 시 권한 요청자와 요청자의 팀장 결재만으로 권한을 부여할 수 있어 업무상 불필요한 권한을 부여한 사례*가 있고,

* 현업 부서로부터 제휴신용카드사 문의사항(PIN인증 이력조회) 확인 목적으로 '전자금융기본정보조회' 화면에 대한 권한 추가 요청받아 전 임직원에게 공통으로 접근권한을 부여(2021.2.1.)하였으나, 접속 이력 확인 결과 부정사용 로그는 없었음

통합단말시스템 화면 담당 부서마다 마스킹 적용 기준·방법이 상이하여 일부 화면에 대해서는 마스킹을 적용하지 않는 등 미적용 화면에 대한 점검·관리가 미흡하여 정확한 현황 파악이 어렵고

개인정보취급자가 다건의 고객정보를 일괄 조회하는 경우 업무 이외에 불필요한 정보가 과다 노출될 우려가 있으므로,

화면 접근권한(공통, 부서별) 적정성을 재검토하여 업무상 필요최소 인원으로 접근권한을 제한하고, 화면 접근권한 신청·변경 시 소관부서의 확인 단계를 추가하여 권한부여의 정당성을 확보하는 한편,

통합단말시스템에 일관된 기준의 마스킹 정책을 적용하고, 다건의 주요 고객정보가 일괄 조회되는 화면의 경우 개인정보취급자에 대해서도 마스킹 해제 절차를 마련·운용하는 등 관련 전산시스템 및 절차 등을 개선하시기 바람

(26) 서버·DB 접근통제솔루션 보안대책 불합리

① 서버 접근통제 불합리

서버 사용자 접근권한 통제, 추가인증 등을 위해 서버 접근통제솔루션을 구축하고, 동 솔루션을 경유(ID, 비밀번호, OTP 추가인증)하여 접근권한이 부여된 서버에 접근하도록 통제 절차를 마련하고 있으나,

서버에서 다른 서버로 내부사용자의 직접 접속(SSH)을 허용하고 있고, 서버 접근

통제 및 모니터링 정책 우회, 고위험 명령어*에 대한 실행 권한을 통제하지 않아 정당한 사유 없이 고위험 명령어를 임의 실행하는 경우 파일시스템 일괄 삭제, 무권한 시스템 종료 등 사고 발생의 위험 등이 있으며

* 파일 삭제(rm -rf), 시스템 종료(shutdown) 등

시스템 관리자 외 DB관리자에게도 서버 최고관리자 권한(root) 상시 부여하거나 일부 개발자에게 최고관리자 권한 사용을 허용하는 등 권한관리가 미흡하며

서버 접근통제솔루션을 활용하여 접속한 이후 잠금 해제 시 추가인증을 재요구하지 않는 등 내부사용자에 대한 서버 접근통제 보안설정이 취약하므로,

내부사용자의 서버 우회 접근, 고위험 명령어 사용을 통제하고, 시스템 관리자 이외에 최고관리자 권한은 장애 등 예외적인 상황에서만 제한적으로 부여하고, 서버 접근통제솔루션 재접속 시 추가인증 하는 등 서버 접근통제 절차와 전산시스템을 개선하시기 바람

② DB 접근통제 불합리

DB 접근통제 솔루션(DB-Safer, Tadpole, PPOU 등)을 활용하여 DB계정 접근권한을 통제하거나 접근이력 모니터링 등을 수행하고 있으나,

서버에서 데이터베이스시스템(DBMS) 접속 명령어(sqlplus) 사용을 통제하지 않아 DB접근통제 및 마스킹 등 DB보안통제 정책을 우회한 접속이 가능하고, DB 직접 조회 시 주요정보에 대한 마스킹 정책을 정보계 DB에 한해서만 적용하고 있어 업무상 불필요한 정보가 노출될 우려가 있으므로,

DB서버에 직접 접속하는 비인가 경로를 차단하고, 주요 고객정보 등을 처리하는 계정계 DB 등에 대해서도 마스킹 정책을 적용 하는 등 DB 접근통제 관련 전산시스템 및 절차 등을 개선하시기 바람