경영유의사항 등 공개안

1. 금융기관명 : ㈜토스뱅크

2. 조치일 : 2026. 8. 25.

3. 조치내용

제재대상	제재내용
기 관	○ 경영유의사항 22건 ○ 개선사항 35건
임 원	○ 해당사항 없음[1]
직 원 등	

주 1) 경영유의사항 등은 기관에 대한 조치에 해당

4. 제재대상사실

가. 경영유의사항

(1) 자본비율 관리체계 강화 및 위기시 자본관리계획 개선

은행은 내규 「자본관리규정」에 따라 매년 사업계획 수립시 자본비율을 전망하고, 자본관리계획을 수립하는 등 법규상 요구되는 자본비율 규제를 준수하기 위한 자본관리 업무를 수행하여야 한다.

그러나 은행은 규제비율에 기반한 최소한의 자본비율 관리 수준만을 정하고 있을 뿐, 연간 영업전략에 기반한 자본비율 목표를 설정하고 있지 않아, 정기적으로 자본비율 목표 대비 실적을 평가하여 이사회에 보고하고, 필요시 영업전략을 변경하는 등의 전사적인 자본비율 관리체계가 미흡하다.

또한, 규제자본비율을 하회하는 위기상황에 대비하여 위기단계별* 자본관리계획을 마련하고 있으나, 자본확충 실행계획(대주주, 기존주주, FI투자자 등) 없이 심사전략 강화를 통한 전체 익스포저 축소만을 내용으로 정하고 있으며, 대주주와 체결한 “유동성공급계약서”상 유동성 공급 사유가 BIS비율 □□%미만, 규제자본비율 미달 등으로만 되어 있는 등 실효성이 부족하다.

* 관리목표 자본비율 하회시 “주의 단계”, 최소유지자본비율 하회시 “경계 단계”로 구분

<조치할 사항>

따라서 은행은 경영계획 수립시 자본비율 목표를 설정하고 정기적으로 자본비율 목표 대비 실적을 점검하여 이사회에 보고하고 대응방안을 마련하는 등 체계적인 자본비율 관리체계를 수립하시기 바랍니다.

또한, 위기 시 자본관리계획은 익스포져 축소 계획 등을 상품군, 차주유형별로 나누는 등 구체화하고, 대주주와의 유동성공급계약을 실효성 있게 보완하여 반영하는 등 개선하시기 바랍니다.

(2) 개인사업자 업종별 CSS 고도화 및 심사 전략 강화

은행은 중·저신용자 대출의 부실 또는 건전성 악화를 예방하기 위하여 대안정보의 범위를 지속적으로 확대하는 등 신용평가시스템(Credit Scoring System, 이하 “CSS“)의 고도화를 추진해야 한다.

그러나 은행은 개인사업자 심사시스템에 대안정보 반영 등이 미흡한 상태에서 대출을 출시(2022.2월)하여 부실이 증가하였고, 최근에는 건전성 관리를 위해 보증서 대출 위주로 영업하는 것으로 보이나 개인사업자 중·저신용자 대출의 건전성이 지속적으로 악화될 우려는 상존한다.

<조치할 사항>

따라서 은행은 카드, 전자상거래 매출, 상권정보 등 대안정보를 적극 활용하여 개인사업자 업종별 CSS를 고도화하고 심사전략을 강화하시기 바랍니다.

(3) 중·저신용자 대출 공급 목표 합리화 및 관리 절차 마련

은행은 설립 취지*상 디지털혁신에 기반하여 포용금융에 기여할 수 있도록 중·저신용자 대출 규모를 단계적으로 확대할 필요가 있다.

* 「인터넷전문은행 설립 및 운영에 관한 특례법」 제정 이유: 중금리대출 활성화 등을 통한 서민·소상공인 금리 단층 해소 등

※ 2023.12월 금융위원회 「인터넷은행 중·저신용자 대출 공급계획」 발표

구 분	2023.11월말*	2024년(평잔)	2025년(평잔)	2026년(평잔)
중·저신용대출	30,634억원	43,867억원	45,852억원	47,837억원

* 2023.11월말 금액은 말잔 기준(개인사업자 신용대출 등 미포함)

그러나 은행은 담보·보증부 대출 취급을 확대하면서 2024년 중에 중·저신용자 신용대출 규모가 감소할 것으로 예상됨에도, 중·저신용대출의 대출 비중 목표만 고려하고 대출공급 규모에 대한 점검 및 대응방안 등 관리 절차 마련이 미흡한 것으로 나타났다.

<조치할 사항>

따라서 은행은 중·저신용자 신용대출 비중 뿐 아니라 대출공급 규모에 대한 목표를 설정하고, 해당 목표의 이행 여부를 점검하는 절차를 수립하시기 바랍니다.

(4) 대손충당금 리스크측정요소(PD, LGD, CCF) 추정 강화

㉮ 부도율(PD) 추정을 위한 외부데이터 수집 강화

은행은 대손충당금 산출을 위한 부도율(PD)을 추정할 시에는 부도와 중요한 관련이 있는 모든 가용 데이터를 반영할 필요가 있다.

그러나 은행은 중·저신용자 대출 비중이 높음에도 외부데이터 수집시 상호금융조합, 대부업 등 일부 업권의 데이터를 제외하고 있어 대손충당금 산출을 위한 부도율을 과소 추정할 소지가 있다.

<조치할 사항>

따라서 은행은 대손충당금 산출을 위한 부도율(PD) 추정시 상호금융조합, 보험사 및 대부업 데이터를 포함하시기 바랍니다.

㉯ 부도시손실율(LGD) 추정 강화

은행은 과거 손실자료를 바탕으로 한 은행의 경험손실률을 충분히 반영하는 등 대손충당금 산출을 위한 부도시손실율(LGD)을 합리적으로 추정하여야 한다.

그러나 부도 발생 이후 경과기간에 따라 손실 규모가 달라지고 있음에도, 1년 초과

여부로만 구분하여 부도자산 부도시손실율(LGD)을 추정하고 있어 정교화가 미흡한 것으로 나타났다.

<조치할 사항>

따라서 은행은 대손충당금 산출을 위한 부도시손실율(LGD)을 추정할 시에 부도 경과기간별로 보다 세분화하여 추정하시기 바랍니다.

㉰ 신용환산율(CCF) 추정 강화

은행은 대손충당금 산출을 위한 신용환산율(CCF)을 추정할 시에는 과거 손실자료를 바탕으로 은행의 경험 신용환산율을 충분히 반영해야 한다.

그러나 내부 데이터를 활용한 경험 신용환산율(CCF) 대비 낮은 표준신용환산율(CCF, 40%)을 일률 적용하여 신용환산율을 과소 추정할 우려가 있다.

<조치할 사항>

따라서 은행은 대손충당금 산출을 위한 신용환산율(CCF)을 추정할 시에는 내부 데이터를 활용한 경험 신용환산율을 반영하시기 바랍니다.

(5) 전세자금보증대출 취급 업무절차 강화

은행은 전세자금보증대출 취급시 선순위 근저당권 설정금액과 임차보증금의 합이 보증대상 목적물의 시세를 초과하는 경우 전세자금보증대출 취급 제한 등 전세사기 방지 및 임차인 보호를 위한 조치를 취해야 하고, 대출실행 이후 사후관리를 통하여 취급된 대출이 적정하게 취급되었는지 점검하여야 한다.

그러나 은행은 시세 확인방법을 제한적으로 정하고 동 방법으로 확인이 어려운 경우 시세확인 없이도 대출취급이 가능하도록 하는 등 폭넓은 예외규정을 두고 있어 전세사기 방지 및 임차인 보호에 미흡하다.

또한 은행은 선순위 근저당권이 설정되어 있는 목적물에 대하여 선순위 근저당권 해지조건부로 대출을 취급하였으나 대출실행 이후 해당 근저당권 말소 여부를 점검하지 아니하였고(746건), 대출실행 후 1개월 이내 차주로부터 주민등록등본을 제출받아 차주의 전입신고사실을 확인하여야

하나, 이를 누락(2건)한 사실이 있다.

<조치할 사항>

따라서 은행은 주택시세 확인 방법을 확대하여 주택시세확인 예외대상을 최소화하는 등 관련 내규 및 업무처리절차를 개선하고, 대출 사후관리 점검이 누락되지 않도록 사후관리부서의 2차 전산승인 절차를 마련하는 등 관련 전산시스템을 개발 및 구축하며, 대출 사후관리를 자점검사 항목에 추가하시기 바랍니다.

(6) 사외이사 회의 활성화 방안 마련 검토

「금융회사의 지배구조에 관한 법률」 제13조에 따르면 사외이사가 아닌 자를 이사회 의장으로 선임한 경우, 선임사외이사를 별도로 선임하여야 하고, 선임사외이사는 사외이사 전원으로 구성되는 사외이사 회의의 소집 및 주재 등의 업무를 수행하도록 하고 있다.

그러나 은행은 검사대상기간 중 대표이사를 이사회 의장으로 선임하여 선임사외이사를 별도 선임하였음에도 사외이사 전원으로 구성되는 사외이사 회의가 특별한 사유 없이 한 차례도 개최되지 아니하였다.

<조치할 사항>

따라서 은행은 선임사외이사를 선임하고 사외이사 회의를 개최하도록 한 관련 법규의 취지를 고려해 선임사외이사의 업무가 실제로 수행될 수 있도록 유의하시기 바랍니다.

(7) 공동업무처리 등 계약 및 비용지급의 적정성 검토 강화

은행이 검사대상기간 중 대주주인 AA와 체결한 다수의 물품 및 용역거래 계약 일부를 확인한 결과, 인사문화 공동업무 처리에 관한 계약, 콘텐츠 관련 사용 계약 등에서 계약서상 비용 산정 기준이 불분명한 사례, 계약서상 명시되지 않은 공동업무에 대한 비용 지급 사례, 전산시스템 구축에 대한 비용 배분이 합리적이지 못한 사례가 다수 발견되었다.

또한, AA로부터 비용의 적정성을 확인할 수 있는 명확한 증빙을 확보하지 못한 채 비용이 집행되어 AA에게 지급된 사례도 다수 발견되었다.

<조치할 사항>

따라서 은행은 향후 AA 및 계열사와 업무 위수탁 또는 공동업무처리 등에 관한 계약 체결 시 제공받을 업무의 범위를 명확히 하고, 각 업무별 비용 산정 기준을 구체적으로 계약서에 명시하는 한편, 비용의 증빙과 세부내역을 명확히 제시하여 비용을 청구하도록 요구하는 등 계약 및 비용 지급의 적정성을 확보하기 위한 절차를 강화하시기 바랍니다.

(8) 사업부문별 수익성 관리 강화

은행은 수익원 다변화를 위해 비이자사업 부문을 지속적으로 확대하고 있으나, 비이자사업 손실이 지속되는 상황이므로 사업부문별 재무성과 분석 등 체계적인 수익성 관리가 필요하다.

그러나 은행은 체크카드 및 외국환거래(Foreign Exchange, 이하 “FX“) 사업 개시 당시 낙관적으로 손익을 추정한 이후 실적이 예측과 크게 벗어났음에도 그 원인 분석 및 재추정에 근거한 재무계획 재설정 및 수익성 개선방안 수립 없이 실적에 따라 일부 비용률을 조정하는 등 단편적 대응조치만 시행하였으며, 은행 경영계획상 사업부문별 손익목표를 설정하여 관리하고 있지 않아 손익 성과 분석 및 점검절차가 미흡하다.

<조치할 사항>

따라서 은행은 추정 재무계획이 실적과 차이가 나는 경우 원인을 분석하고 수정 계획 및 대응방안을 수립하여 이사회에 보고하는 한편, 연간 경영계획 등에 사업부문별 손익목표를 설정하고 목표달성 여부 등에 대해 점검하는 체계를 마련하는 등 수익성 관리를 강화하시기 바랍니다.

(9) 대출채권 매각관련 일관된 정책목표 마련

은행은 「이사회 규정」에 따라 이사회 결의를 거쳐 이루어지는 대출채권 매각과 관련하여 회계투명성 제고 등을 위해 일관된 정책 목표 아래 매각 규모의

결정 등이 합리적이고 투명하게 이루어질 필요가 있다.

그러나 은행은 일관된 매각의 정책목표(고정이하여신비율 개선 목표치 등)가 불분명하여 매각규모의 산정 근거가 부족하고, 단기 손익 목표 달성 등 경영진의 필요에 의해 매각규모를 결정할 소지도 있다.

<조치할 사항>

따라서 은행은 자산건전성 목표치 등 일관된 정책목표를 제시하고, 이를 고려하여 예상 매각규모를 산정 후 연간 경영계획에 포함하는 등 의사결정의 투명성을 제고하시기 바랍니다.

(10) 유동성 위기상황 분석 및 대응능력 강화

㉮ 유동성 위기상황 시나리오 설정의 보수성 강화

유동성 위기상황분석은 예외적이지만 발생 가능하고 은행의 생존을 위협할 수 있는 유동성 위험요인에 대한 은행의 잠재적인 취약성을 평가·보완하기 위한 것으로, 위기상황 시나리오는 은행의 각 영업활동 및 난내외 상품, 자금조달원과 관련된 리스크 요인들이 유동성 포지션에 미칠 수 있는 잠재적인 악영향을 포함하여야 한다.

그러나, 은행은 위기상황 분석대상 기간인 30일동안 소매 요구불예금이 매일 동일한 비율로 이탈하는 것으로 가정하고 유동성 위기상황분석을 실시함에 따라, 위기상황이 일부 진정된 이후 보다는 위기상황 발생 초기에 많은 예금이 급격히 이탈할 우려가 있다는 잠재적인 위험요인을 반영하지 못하고 있다.

또한, 매분기별로 위기상황분석을 실시하면서 위기상황 하에서의 예금(중도해지율, 재예치율), 여신(연체율, 만기상환율, 조기상환율)에 대한 현금 유출입 규모 추정시, 매 분석시점 기준 직전 1년간의 평균 및 표준편차를 적용함에 따라 위기상황과 무관한 평상시의 자료를 적용하여 분석을 실시하게 되어 위기상황에서의 현금 유출입 규모를 과소 추정할 우려가 있다.

<조치할 사항>

따라서 은행은 온라인을 통한 급격한 자금유출이 발생할 수 있는 인터넷전문은행 특성을 감안하여 위기상황 초기에 자금이탈이 집중 발생할 수 있음을 가정하거나, 위기상황에서의 현금 유출입 규모 추정시 과거 실제 위기상황에 준하는 상황을 적용하는 등 시나리오 설정을 강화하시기 바랍니다.

㈏ 조달측면의 유동성 대응능력 강화

은행은 유동성 위기상황에서 필요한 자금을 과도한 손실발생 없이 적시에 조달하여 지급 의무를 상환할 수 있도록 특정 자금조달 수단에 과도한 집중이 발생하지 않게 다양한 자금 조달수단을 확보·관리하여야 한다.

그러나 위기상황시 비상자금 조달액에서 보유 유가증권 매각 및 유가증권 담보 환매조건부채권 매도를 통해 조달하는 자금의 비중이 최대 80% 수준에 이르는 등 유동성 조달수단이 자금운용 수단인 유가증권에 과도하게 집중됨에 따라, 시장금리 급등시에는 환매조건부채권 매도의 차환위험이 증가하고 자산•부채간 만기불일치 부담으로 지속적인 매각이 곤란하여 시장 경색시 비상자금조달 수단으로서의 실효성이 부족하다.

또한, 2024.9월말 기준 전체 유가증권(□□.□조원)의 □□%(□.□조원)를 만기보유증권(AC)으로 보유함에 따라, 유동성 위기상황에서 자금을 조달하기 위한 매각이 곤란할 뿐만 아니라, 나머지 매도가능증권(FVOCI) 매각의 경우에도 금리상승에 따른 평가손실이 현실화되는 문제로 실행이 곤란하며, 2024.9월말 기준 만기가 정해져 있지 않은 요구불 예금이 전체 수신에서 차지하는 비중(□□%)이 높아 위기상황에서 자금이탈이 가속화될 우려가 있다.

<조치할 사항>

따라서 은행은 향후 예대율 증대를 위한 유가증권 운용규모 감축, 금리상승시의 위기상황 등에 대비하여 특정 자금 조달·운용수단에 과도한 집중이 발생하지 않도록 중장기적 관점에서의 추가적인 유동성 확보방안 및 수신구조의 안정성 제고 방안(저축성예금 확대 등)을 강구하시기 바랍니다.

㉰ **유동성리스크 관련 내부 자본한도 산정방식 합리화**

은행은 영업활동의 특성을 감안하여 합리적인 가정 및 절차를 통해 경영상 직면하는 유동성리스크를 인식·평가하고, 이를 관리할 수 있도록 적절한 유동성리스크 관련 내부 자본한도를 설정하여야 한다.

그러나 은행은 자금시장 경색에 따른 추가 조달비용 발생을 고려한 대체 조달비용을 감안하여 유동성리스크 관련 내부 자본한도를 설정하는 과정에서 원화유동성 리스크 관련 목표 생존기간을 1개월로 설정하고 1개월간의 대체 조달비용만 감안하여 내부 자본한도를 설정함에 따라, 은행의 가정과 달리 위기상황이 1개월 이상 지속될 경우 적절히 대응하기 어려운 문제가 있다.

<조치할 사항>

따라서 은행은 향후 1개월 이상 지속되는 유동성 위기상황에서도 은행의 대응능력을 제고할 수 있도록 유동성리스크 관련 내부 자본한도 산정방식을 합리화하시기 바랍니다.

(11) 유가증권 매각 관련 내부위원회 의사결정 기능 강화

내규 「자산부채관리위원회규정」 제3조에 의하면 자산부채관리위원회는 자산·부채 구조의 최적화, 유동성위험 등 경영효율 제고와 관련된 정책 및 전략을 결정하도록 규정하고 있다.

은행은 총자산의 □□% 상당을 유가증권으로 운용하고 있으며, 유동성 위기상황시 비상자금 조달액에서 보유 유가증권 매각 및 유가증권 담보 환매조건부채권 매도를 통해 조달하는 자금의 비중이 최대 □□% 수준에 이르고 있어, 유가증권 매각 등을 통해 유동성을 조달하거나 평가손실을 제한하기 위해 전략적으로 유가증권 매각*할 필요성이 상시적으로 존재한다.

* 금리상승기에 매도가능 유가증권의 평가손실 발생을 제한하기 위해 매도가능 유가증권 매각후 만기보유목적의 유가증권 매입

그러나 은행의 당기순이익에 상당한 영향을 미칠 수 있는 유가증권 매각 결정과 관련하여 자산부채관리위원회 등에 보고·승인 기준이 마련되어 있지 않아,

2022년 하반기중 □.□조원의 매도가능증권(FVOCI) 매각으로 총 □□□억원의 손실이 발생하는 과정에서 □.□조원(손실 □□□억원) 매각은 자산부채관리위원회의 사전 승인을 받았으나, 나머지는 자산부채관리위원회에 보고·승인을 실시하지 않는 등 중요 의사결정 과정에서 절차적 일관성을 제대로 확보하지 못하는 문제가 발생하였다.

<조치할 사항>

따라서 은행은 당기순이익에 상당한 영향을 미치는 전략적인 유가증권 매각에 대한 의사결정의 일관성을 확보할 수 있도록, 자산부채관리위원회 등 내부 위원회의 보고•승인 기준을 마련하시기 바랍니다.

(12) 자산·부채 등 재무리스크 관리 사업계획 수립간 연계성 강화

은행은 유동성 위기상황에서의 심각한 손실을 적절히 관리할 수 있도록 자산·부채, 유동성, 자본비율 관리 등 전체적인 재무리스크 관리체계를 충분히 감안하여 연간 사업계획을 수립·이행할 수 있도록 하여야 한다.

하지만, 2022.8월부터 증자·투자자 유치 등 IR업무를 담당하는 A디비전이 연간 사업계획을 수립(기존에는 B디비전이 담당)하도록 조직을 개편함에 따라, 유동성 등 재무리스크를 관리하는 부서(B디비전)와 연간 사업계획을 수립하는 부서(A디비전)가 상이해졌다.

이후 연간 사업계획 수립시 자산·부채, 유동성, 자본비율 등 재무적 리스크 관리보다는 IR활동 관련 여수신 규모 확대 및 예대율 개선 등과의 연계가 강화되면서, 2022년 하반기중 기 수립한 사업계획과 달리 수신자금 유출 확대가 지속되며 유동성 부족사태가 발생하고, 사업계획상의 수정된 목표치와 실적치간의 괴리가 큰 폭으로 발생하는 상황에서도,

금리인상 등을 통한 수신자금 확보 조치 없이 유가증권 매각 및 초단기 환매조건부채권 매도 확대를 통해 자금 부족에 대응하면서 여신을 증대시킴에 따라, 예대율이 급등하고, 유동성 부족 사태가 지속되는 등 유동성 위기상황에서 리스크관리와 영업전략이 상충되는 문제가 발생하였다.

<조치할 사항>

따라서 은행은 재무·유동성 등 은행의 전체적인 리스크관리체계를 감안하여 연간 사업계획을 수립·이행하고, 두 업무 간 연계성을 강화할 수 있도록 개선하시기 바랍니다.

(13) 상시감시시스템 운영 강화

내규「상시모니터링지침」제2조 등에 따르면 은행은 상시감시모니터링 시스템을 통하여 문제발생 소지가 있는 부서 또는 사고 취약 부문을 사안에 따른 적정한 방식으로 점검하여 적기에 필요한 조치를 취함으로써 적절한 내부감시 체제를 유지할 필요가 있다.

그러나, 은행은 내규「상시모니터링지침」제정(2021.3월) 이후에도 상당기간 동안 상시모니터링시스템이 구축•운영되지 않았으며, 2024.1월 상시모니터링 시스템을 구축하였으나 시스템 운영 및 개발 인력 부족으로 검사기준일 현재까지 운영중인 시나리오가 24건에 불과하며, 시나리오 내용도 추심•사망자계좌를 이용한 부정사용 등 일부에 한정되어 각종 영업 및 업무 수행 과정에서 발생할 수 있는 위규사항을 적발하는데 한계가 있다.

아울러 이상거래에 대한 소명기한 설정 및 소명절차, 점검 결과에 대한 조치방안 등 사후관리 절차를 구체적으로 마련하고 있지 않아 의심거래 발생시에도 적시성 있게 소명 및 개선이 이루어지지 않는 등 상시감시 업무가 실효성 있게 운영되지 않고 있다.

<조치할 사항>

따라서 은행은 상시모니터링 시스템 개발 및 운영 안정화를 위한 감사인력, IT개발자 등 적정 인력을 배치하는 한편, 은행 업무 전반에 걸쳐 법규 및 위규사항 점검이 이루어질 수 있도록 시나리오를 다양화(대상영역 확대)하고 사후관리 절차를 강화하시기 바랍니다.

(14) 연계대출 관련 소비자 안내 강화 필요

은행은 상품 판매시 금융소비자가 합리적인 판단을 할 수 있도록 상품의 중요한 내용에 대하여 충분히 설명할 필요가 있다.

㉮ **상품 내용 안내 미흡**

은행은 대출 심사 후 승인 거절시 다른 제휴 금융회사의 대출을 맞춤형으로 소개하는 연계대출 서비스를 운영하면서 금리 및 한도 이외에 기타 대출 조건 등 금융소비자에 대한 상품 내용 안내가 미흡하다.

㉯ **상품판매대리·중개업자 역선택 우려**

은행과 AD는 하나의 앱을 공유하고 있으나 각각 제휴 금융회사와 대출모집위탁계약을 체결하고, 연계대출 서비스를 운영하고 있어 각각 서로 다른 금리 및 한도를 제공받을 수 있으나 이러한 정보가 적절히 제공되지 아니하여 금융소비자가 상품판매대리·중개업자를 역선택할 우려*가 있다.

* 동일인이 동시에 AD 및 은행에서 각각 연계대출서비스(대출비교중개서비스)를 받을 경우 동일한 금융회사에 대하여 서로 다른 금리 및 한도를 받는 사례 발생 ex: (AD) AE은행 ㉮상품 4.5% ○○○원 한도, (토스뱅크) AE은행 ㉮상품 4.7%, ○○○원 한도

<조치할 사항>

따라서 은행은 앱에 상품 상세페이지를 추가하여 중도상환수수료 등 금융소비자에 대한 안내를 강화하고 해당 내용에 대해서 제휴 금융회사(금융상품 직접판매업자)의 확인을 받는 한편,

은행과 AD는 서로 다른 법인으로 별개의 연계대출 서비스를 운영하고 있으므로 동일한 앱을 공유하더라도 플랫폼에 따라 서로 다른 대출 조건이 제시될 수 있다는 사실을 금융소비자에게 명확하게 설명하시기 바랍니다.

(15) 리스크관리 기본계획 수립 절차 마련

은행은 경영계획이 리스크관리 전략 등에 부합할 수 있도록 리스크관리 기본계획*을 통해 자본적정성 및 자산건전성 관리 등에 필요한 세부 리스크관리 지표**를 설정하여 경영계획에 반영하고 모니터링을 강화할 필요가 있다.

* 리스크관리 기본방침 및 전략 포함
** 예) 총자본비율, 고정이하여신 비율, NPL커버리지 비율, 상품별 연체율 등

그러나 은행은 경영계획 수립시, 리스크관리 기본계획 수립 절차 없이

영업부문 계획만을 선반영하고, 리스크관리 부서는 경영계획을 사후적으로만 검토하고 있다.

<조치할 사항>

따라서 은행은 경영계획 수립시 리스크관리 계획을 병행하여 수립하고, 리스크 부서에서 관리하는 리스크관리 지표를 확대하여 운영하시기 바랍니다.

(16) 자금운용 한도 설정 및 운영 절차 강화

은행은 자금운용 한도 설정 및 한도 초과여부에 대한 모니터링 수행시 리스크관리 및 부서간 상호견제를 위해 익스포져 발생부서가 아닌 제3의 부서에서 해당 업무를 수행할 필요가 있다.

그러나, AF팀에서 운용하는 자금운용 한도 중 기관별 투자한도*를 익스포져 발생부서인 AF팀에서 설정하고 자산부채관리위원회(ALCO)에서 의결하며, 한도 모니터링도 C디비전이 아닌 AF팀에서 수행하고 있어 상호견제 기능이 미흡할 우려가 있다.

* 유가증권 및 단기자금을 포함한 기관별 투자한도(유니버스 투자한도)

<조치할 사항>

따라서 은행은 AF팀에서 관리중인 한도 중 자금운용 리스크관리가 필요한 사항을 리스크관리부서로 이관하고 위험관리협의체에서 의결토록 하며, 설정된 한도에 대한 모니터링을 리스크관리부서에서 수행하시기 바랍니다.

(17) 금리리스크 관리 강화

은행은 내규 「금리위험관리지침」 제13조 등에 따르면 금리리스크 관리를 위해 내부자본 등 각종 한도*를 적정하게 설정하고 기간별 금리갭 등 관련 지표를 모니터링할 필요가 있다.

* 내부자본 한도는 금리리스크 표준방법 △EVE(Economic Value of Equlity) 적용

그러나, 은행의 만기별 금리민감부채 규모의 변동은 미미한 반면, 금리민감자산은

가계신용대출 위주의 짧은 만기로 구성되어 있어 △EVE 비율이 높은 수준이나 아래와 같이 체계적 관리가 미흡한 측면이 있다.

우선, 자산·부채 만기구조 등 고려없이 내부자본 한도를 가용자본의 □□.□% (규제한도의 □□%수준)로 단순 설정하고, 한도소진율을 □□%로 가정하여 보조지표 (듀레이션 갭)를 설정하며, 기간별(중·장기) 금리갭 등 상세 지표를 통한 상시적인 모니터링 및 분석 절차가 부재하다.

또한, 고객분류(소매•거래/소매•비거래/도매)에 따라 핵심예금비율을 구분하여 적용하고 있는데, 적합성검증 보고서에는 고객 분류의 적정성 여부에 대한 검토 내용 없이 결과만을 기술하고 있는 수준이다.

<조치할 사항>

따라서 은행은 △EVE 관리 강화를 위한 경영계획상의 자산·부채계획 등을 고려하여 내부자본 한도를 설정하고, 기본자본 대비 △EVE 비율 감축계획(2025년도 목표비율 : □.□%)에 부합하도록 듀레이션 갭 등 보조지표를 실효성있게 설정하는 한편, 만기별 자산·부채 갭 수준 관리 및 모니터링을 실시하고 고객분류의 적정성 검증 내용을 보완하시기 바랍니다.

(18) 위기상황 시나리오 설정시 이사회 참여 절차 마련

「은행업감독업무시행세칙」<별표19>에 따르면 이사회는 위기상황분석 목표의 설정, 시나리오 정의에 대한 토론 등 위기상황분석 과정에 참여*하여 의견을 개진하여야 한다.

* 「은행업감독업무시행세칙」<별표19> 7. 이사회 및 경영진은 위기상황분석이 적절히 활용될 수 있도록 위기상황분석 절차, 가정 및 결과 등에 대해 충분히 이해해야 하며, 위기상황분석 과정에 참여하여 의견을 개진하여야 하고, 위 과정에는 위기상황분석 목표의 설정, 시나리오 정의 및 분석결과에 대한 토론 및 잠재적인 행동과 의사결정사항을 확정하는 과정 등이 포함되어야 한다.

그러나 은행은 '통합위기상황분석 결과'와 '시나리오 설정안'을 동시에 보고하고 있어, 시나리오 조정 등 이사회 및 경영진의 의견이 반영되기 어려운 측면이 있다.

<조치할 사항>

따라서 은행은 통합위기상황분석 결과를 위험관리위원회에 보고하기 전, 동 회의체에서 시나리오를 먼저 의결토록 정비함으로써, 시나리오 설정의 객관성, 정합성 등에 대한 이사회의 논의 기회를 확대하시기 바랍니다.

(19) 내부활용 목적 부도율(PD)의 일관성 제고 방안 마련

은행은 신용리스크 측정(대손충당금, 내부자본) 및 대출금리 신용원가 산출을 위해 내부 신용등급별 부도율(PD)을 사용하고 있는데, 사용 목적에 따라 내부 신용등급 산출 기준이 다르게 적용되어 신용리스크 측정 및 금리산출 목적 PD가 서로 상이하게 산출되는 등 일관성이 결여되어 있다.

<조치할 사항>

따라서 은행은 신용등급 산출 기준을 단일화하거나, 신용등급별 예상 부도율 범위 설정 등을 통하여 은행 내부 활용 목적으로 산출하는 부도율의 일관성 확보 방안을 마련하시기 바랍니다.

(20) 제3자 리스크(단일장애지점) 대응 방안 마련 필요

㉮ 모바일 어플리케이션 장애 대비 대체 전자금융거래 채널 마련 필요

은행은 AD 앱(App)을 통해서만 뱅킹서비스를 제공하고 인증수단으로 ㉮인증서만을 사용하고 있다.

그러나 은행은 AD 앱 장애에 대비한 대체 전자금융거래 채널을 마련하지 않고 있어 AD 앱 장애 시에는 은행의 전자금융서비스가 마비될 우려가 있다.

㉯ 클라우드 서비스 장애 대비 비상 대응계획 마련 필요

은행은 AD 앱에서 토스뱅크 접속 화면에 필요한 이미지 파일 등의 자원 제공 및 DNS 기능 등을 BB 웹서비스를 통해 클라우드로 구축·이용하고 있다.

그러나 은행은 전자금융거래 대체 채널을 구축하지 않고 있으며, 클라우드

서비스를 단일 서비스 제공자에 의해서만 제공받는 등 단일 장애 지점에 대한 대응 방안 마련이 미흡하여

동 클라우드 서비스 장애 시 모바일뱅킹 초기화면을 정상적으로 제공하지 못하거나 모바일뱅킹 서비스 접속에 장애가 발생할 우려가 있다.

<조치할 사항>

따라서 은행은 AD 앱 및 클라우드 서비스 장애 시 전자금융서비스 중단에 대비하여 전자금융거래 대체 채널을 확보하고 클라우드서비스 제공사를 이원화하는 등 단일 장애 지점 리스크에 대한 대응 방안을 마련하시기 바랍니다.

(21) 프로그램 개발·적용 등 정보기술부문 내부통제 강화 필요

㉮ 프로그램 개발·적용 시 통제절차 강화

은행은 내규 「개발관리지침」 제13조 및 제14조 등에 개발부서에서 개발 완료한 프로그램을 운영시스템에 적용하기 위하여 제3자 검토, 책임자 승인 및 인수테스트를 수행하도록 정하고 있다.

그러나 은행은 프로그램을 운영시스템에 적용하면서 제3자 검토와 책임자 승인을 동일인이 수행하거나 전문성에 대한 고려 없이 검토자를 지정할 수 있는 등 프로그램 변경 통제 절차를 미흡하게 운영하였으며,

프로그램 운영·배포 전 테스트 결과를 변경관리 시스템에 등록하도록 통제하지 않아 일부 프로그램이 테스트 수행 여부가 검증되지 않은 상태로 운영시스템에 적용되었고,

㉰연령, ㉱금리 등 중요 파라미터 변경 시 자동화된 배포 도구를 사용하지 않아 테스트에서 검증 완료된 값과 다른 값이 운영시스템에 적용될 수 있는 등 변경 통제가 미흡하다.

또한, 현업부서의 개발 요구사항이 프로그램에 제대로 반영되었는지 확인하지 않거나 인수테스트 절차가 부실하게 운영되는 등 테스트 관련 절차의 수립·운용이 미흡하다.

<조치할 사항>

따라서 은행은 프로그램 변경통제 절차를 강화하고 개발 요구사항의 검증 및 테스트 결과를 표준화하는 등 개선 계획을 수립·운용하시기 바랍니다.

㉯ IT시스템 작업 관련 내부통제 강화

은행은 시스템 담당자별 역할 및 작업관리 절차 등 전자금융업무의 안정성 확보 및 시스템 운영 관리에 필요한 사항을 통제하기 위하여 내규로서 「전산규정」 및 「시스템운영지침」 등을 마련하여 운영하고 있다.

그러나 은행은 내규에 해당하지 않는 「시스템 작업통제 가이드」로 책임자 승인기준을 관리하고 시스템 작업통제를 하고 있어 중요작업 수행시 책임자 승인 없이 작업을 수행할 우려가 있으며, 유관부서 간 시스템 변경 작업의 영향도 등을 사전에 검증하는 체계가 마련되어 있지 않아 대고객 업무시스템에 장애가 발생한 사례가 있는 등 중요 시스템 작업에 대한 사전 검증이 미흡하다.

또한, 은행은 인터넷전문은행으로 인가받아 대면 영업점이 없는 환경에서 단일한 비대면 전자금융거래 서비스(모바일뱅킹)만 제공하고 있어 시스템 작업이 고객 서비스에 미치는 영향도가 높은 수준이나,

대고객 트래픽 전환 대상 작업 기준을 마련하지 않아 검사대상 기간 중 전자금융거래가 일시 중단 또는 지연되는 장애가 여러 차례 발생하는 등 장애 예방 조치가 미흡하다.

<조치할 사항>

따라서 은행은 내규 「전산규정」, 「시스템운영지침」 및 「업무매뉴얼」 등에 근거하여 시스템 작업 및 변경 등을 수행할 수 있도록 내규로서 책임자 승인기준을 마련하여 운영하고,

전자금융거래에 영향을 미칠 수 있는 중요 시스템 작업은 유관부서가 작업의 영향도 등을 사전에 검증할 수 있도록 실무협의체 등을 구성하여 운영하는 절차를 마련하는 한편,

시스템 작업 시 모바일뱅킹 등 대고객 전자금융거래가 중단 또는 지연되는 일이 발생하지 않도록 데이터센터 트래픽 전환 대상 작업에 대한 세부 기준을 마련하여 운영하는 등 시스템 작업 관련 내부통제 절차를 강화하시기 바랍니다.

㉰ 단말기 관리자 및 보안프로그램 관리 강화

은행은 내규「단말보안지침」제14조에 따라 단말기의 관리자 권한 사용을 제한하여 비인가 프로그램의 무단 설치를 통제하고 필수 보안프로그램을 설치하여 단말 보안대책을 마련·운용하고 있다.

그러나 은행은 중요 단말기 및 인터넷 단말기에 대해서는 관리자 권한 사용을 제한하지 않아 비인가 프로그램의 무단 설치 가능성이 있으며,

동 단말기에서는 관리자 암호를 우회하여 보안 필수 프로그램을 삭제하는 등 단말 보안대책을 무력화시킬 우려가 있다.

<조치할 사항>

따라서 은행은 단말기 권한 통제를 강화하여 비인가 프로그램의 무단 설치 등 단말기 내 프로그램 수정·설치를 통제하고 필수 보안프로그램의 삭제가 발생하지 않도록 개선계획을 수립·운용하시기 바랍니다.

(22) 정보기술부문 중·장기 계획 수립 필요

은행 내규「전산규정」제5조 등에 의하면 은행의 중·장기 경영계획에 맞춰 정보기술부문의 기본전략을 수립·운영하여야 하고 IT투자심의회에서는 중·장기 IT투자 및 정보기술부문 계획서에 관한 사항을 심의하도록 정하고 있다.

그러나 은행의 IT사업계획이 정보기술부문 계획서에 포함되어 있지 않고 동 계획서에 IT조직 운영, IT인력 충원 및 양성 방안이 마련되어 있지 않는 등 IT부문 중·장기 계획의 마련 및 검토가 부실하게 이루어지고 있다.

<조치할 사항>

따라서 은행은 IT사업계획, IT부문 조직 및 인력 등에 관한 사항을 포함한 IT부문 중·장기 계획을 수립하여 이사회 등에 보고·검토할 수 있도록 절차를 개선하시기

바랍니다.

나. 개선사항

(1) 임원 보수체계 및 임직원 성과평가체계 개선

(가) 임직원의 성과측정 및 보수체계 합리화

은행은 내규 「경영계획규정」에 따라 반기별 경영성과 평가를 위한 목표(OKR, Objectives and Key Results)를 설정하고 그 결과에 따라 임직원의 성과보수(인센티브)를 결정하고 있다.

하지만, 2021년 하반기부터 2024년 상반기 기간동안 여•수신 성장률, 고객수 증가 등 성장•이익 위주로 목표 지표를 설정하였으며, AH부서, AI부서, AJ부서, AK부서 등 모든 임직원이 동 목표만 달성하면 인센티브를 지급하는 구조로 성과보수 체계를 운영하고 있어 은행이 성장 및 이익추구를 위하여 과도한 위험을 부담토록 유인할 가능성이 있다.

또한 은행은 일부 임원을 제외한 모든 임원에 대해서 직원과 동일하게 성과를 측정하고 있어, 임원이 관리자로서 부담하고 있는 직무의 특성 및 책임 정도가 충분히 반영되지 않는 문제점이 있다.

<조치할 사항>

따라서 은행은 성장, 수익성뿐만 아니라 자산건전성, 자본적정성, 리스크, 전략적 목표 등 각 부문별 성과가 균형있게 반영되도록 전사 목표를 설정할 필요가 있으며, 임원, 주요 부서별 성과는 각 업무의 성격 및 역할 등을 고려하여 측정되도록 임원•부서별 성과 평가기준을 마련하고, 동 평가 결과에 연동하여 성과보수(인센티브)도 달리 책정될 수 있도록 임직원에 대한 성과보수체계를 전반적으로 개선하시기 바랍니다.

(나) 별도 평가 임원에 대한 성과평가 방식 개선

은행은 내규 「준법감시인 및 위험관리책임자와 금융소비자보호총괄책임자의 보수지급 및 평가기준에 관한 규정」에 따라 준법감시책임자, 위험관리책임자,

금융소비자보호책임자의 평가기준을 별도로 마련하고 있으나, 별도 평가 대상 임원에 대하여 대표이사가 단독으로 정성평가하고 있어 관련 임원의 직무 독립성이 저하될 가능성이 있다.

* 계량지표 등 객관적인 근거 없이 대표이사가 주관적으로 평가

<조치할 사항>

따라서 은행은 각 임원들의 직무특성을 반영할 수 있는 객관적인 정량지표를 설정하거나 대표이사의 평가 비중을 축소하는 등 직무 수행의 독립성이 제고되도록 별도 평가 대상 임원에 대한 평가 방식을 개선하시기 바랍니다.

(다) 성과보수체계에 대한 보수위원회 역할 강화

은행 보수위원회는 임직원의 보수 결정에 대한 투명성과 객관성을 확보하기 위하여 성과측정 및 성과와 보수의 연계방법 등 성과보수체계 전반에 대해 심의할 필요가 있으나, 검사 기준일 현재까지 은행 보수위원회의 의결사항이 임직원에게 지급되어야 하는 보수의 수준, 지급방식에 관한 사항 등으로 한정되는 등 보수위원회의 역할과 기능이 부족하다.

<조치할 사항>

따라서 은행은 임직원에 대한 성과측정 방법, 성과와 보수의 연계방법 등 성과보수체계와 관련한 주요 의사결정이 보수위원회에서 충분히 심의•의결되도록 관련 기준과 절차를 보완하시기 바랍니다.

(라) 내부통제 위반 임직원에 대한 실효성 있는 처리방안 마련

은행은 임직원의 내부통제 위반시 성과평가 반영 등 실질적인 처리방안을 마련하고 있지 않아 내부통제기준을 위반한 경우에도 대부분 개선 권고에 그칠 뿐 임직원이 내부통제기준을 준수토록 하기 위한 성과평가 측면의 유인•통제가 미약하다.

<조치할 사항>

따라서 은행은 내부통제 기준을 위반한 직원에 대한 성과평가상 불이익

조치 혹은 인사상 제재 등 실효성 있는 처리방안을 마련하시기 바랍니다.

(2) 사외이사 후보군 관리개선을 통한 이사회 역량 강화

내규「임원후보추천위원회규정」제3조 등에 의하면 은행은 사외이사 후보자로 은행, 주주 및 기타 이해관계자들의 이익에 부합하는 자를 공정하고 투명한 절차에 따라 추천하여야 하고, 사외이사 후보군 탐색시 주주, 이해관계자 및 외부 자문기관 등 은행 외부로부터의 추천을 적극 활용하도록 노력하여야 한다.

그러나 검사착수일 현재 은행은 사외이사 후보군 □□명 중 □□명(약 □□%)을 1개 외부 자문기관의 추천으로 구성하고 있고, 소비자보호, ESG 분야에 대한 후보군도 각 1명씩에 불과하여 다양한 분야의 전문가로 구성된 사외이사 후보를 확보하지 않고 있다.

<조치할 사항>

따라서 은행은 복수의 자문기관을 활용하거나 주주, 이해관계자 추천 인원 등을 확대하여, 다양한 전문성을 가진 사외이사 후보군이 안정적으로 확보될 수 있도록 사외이사 후보군 관리 방안을 개선하시기 바랍니다.

(3) 대주주 및 특수관계인 정보 관리절차 개선

은행은 대주주(대주주의 특수관계인 포함)에 대한 신용공여가 발생하지 않도록 대주주의 특수관계인 변동 사항*을 적시에 파악할 필요가 있다.

* 대주주 및 계열사 임원 변동, 계열사 신규 편입 등

그러나 은행은 대주주의 특수관계인 변동사항 파악을 대주주 및 계열사 담당자의 협조에만 의존하고 있으며, 특수관계인이 시스템 등록을 지연할 경우 이를 촉구하는 절차가 마련되어 있지 않아 특수관계 형성일과 은행의 관리시스템 등록일 사이 시차가 발생하여 관련 법규를 준수하지 못할 우려가 있다.

<조치할 사항>

따라서 은행은 계열사 법인등기부 등본 변동사항 모니터링, 계열사 대상 공문 발송을 통한 협조 유도 등 대주주의 특수관계인 정보를 적시에 인지·등록할 수

있도록 관리 절차를 강화하시기 바랍니다.

(4) 계약 사후관리 프로세스 개선

은행은 IT 관련 계약은 AL팀에서 총괄하여 체결하고, 기타 계약 중 일부 계약(제휴, 매출 관련 계약 등)을 AM팀에서 총괄하여 체결하고 있다.

그러나 은행은 현업 부서와 계약을 체결하는 부서의 역할을 분명하게 정하고 있지 않아, 계약의 적정성 및 연장 필요성에 대한 검토가 미흡할 우려가 있으며, 계약의 갱신 및 조기종료 여부를 파악할 수 있는 시스템이 부재하여 유관부서가 계약 변동사항을 적시에 파악하기 어려운 측면이 있다.

<조치할 사항>

따라서 은행은 계약 체결을 담당하는 부서와 계약에 따라 업무를 수행하는 부서 간 역할을 내규 등에 명확하게 규정하고, 계약 대상, 계약 내용 등 계약 현황을 유관부서의 임직원이 확인할 수 있도록 관리시스템을 개선하는 등 계약 사후관리 프로세스를 개선하시기 바랍니다.

(5) 업무위수탁 계약관리 및 현황보고 업무 개선

은행은「금융기관의 업무위탁 등에 관한 규정」제4조 제2항에 따라 사후보고 대상 업무위수탁 현황을 업무보고서에 포함하여 반기별로 보고하고 있다.

하지만 은행은 검사대상기간 중 4개의 업무 위탁계약을 각 1회, 1개의 업무 위탁계약을 총 2회 보고를 누락하고, 47건의 계약에 대하여 업무보고서상 계약기간과 실제 계약기간을 다르게 보고하는 등 계약 관리 및 보고 체계가 미흡한 측면이 있다.

<조치할 사항>

따라서 은행은 업무보고서 작성시 계약 체결 담당부서의 확인 절차를 강화하여 업무위수탁 계약 관련 변동사항을 누락없이 확인하여 보고하는 한편, 업무보고서 작성 매뉴얼을 마련하여 일관된 기준에 따라 보고하는 등 보고 업무를 개선하시기 바랍니다.

(6) 공시 업무 체계 개선

은행은 「은행법」 제43조의3, 「은행업 감독규정」 제41조 등에 따라 다양한 공시 정보를 정기·수시 공시하고 있다.

그러나 은행의 공시기한 준수를 위해 마련된 시스템 알림 기능이 월초, 공시부서 요청일과 같은 일정 시기에만 작동되고, 기한 임박에 따른 추가 알림이 없는 등 공시 업무 기한 관리체계의 마련이 미흡하여 담당자 부주의 및 변경 등에 따라 공시* 의무를 준수하지 못할 우려가 있다.

* 은행업 감독규정 제41조(경영공시) 제1항에 따른 공시(결산일로부터 3개월 이내) 및 제3항에 따른 공시(공시사유 발생 즉시)

<조치할 사항>

따라서 은행은 공시기한 전 시기별 알림 체계 도입 등을 통해 유관부서가 공시 일정을 사전에 인지하고, 공시 정보를 상호 검증할 수 있도록 공시 업무 체계를 개선하시기 바랍니다.

(7) 자점감사업무 개선

은행은 사고 예방 및 사고의 조기발견을 위해 각종 업무를 수행하는 과정에서 법규 및 내규 등에서 정하는 사항의 준수 여부를 자체적으로 감사(이하, '자점감사')하는 체계를 마련하고 있다. 그러나 자점감사와 관련하여 아래 ㈎~㈐와 같은 문제점이 확인되었다.

(가) 준법감시담당자 지정•임면 기준 및 절차 마련

각 부서의 자점감사를 담당하는 준법감시담당자에 대한 자격요건(예: 실근무경력, 경험 등)이 구체화 되어 있지 않지 않아 해당 부서의 업무 경험이 1개월 미만인 자가 준법감시담당자로 지정된 사례가 다수 있으며, 준법감시담당자의 퇴사 또는 담당업무 변경 등으로 담당자를 재지정(변경) 해야 하는 경우가 발생할 수 있는데도 AO팀은 준법감시담당자 최초 지정시에만 담당업무를 AN팀에 구두로 확인할 뿐, 준법감시담당자를 지정한 이후에는 해당 담당자의 업무변경, 부서전출, 퇴사 등 인사정보를

점검 및 확인하지 않고 있다.

<조치할 사항>

따라서 은행은 실근무경력, 담당업무, 결격사유(예:인사 징계조치) 등 준법감시담당자에 대한 요건을 구체화하고, 인사시스템 연동 및 점검을 통해 적격여부를 적시에 확인하여 필요시에는 담당자를 즉시 변경할 수 있도록 준법감시담당자 지정 및 임면 절차를 개선하시기 바랍니다.

(나) 자점감사 항목 설정 및 정기적 관리 체계 마련

자점감사 항목이 설정되지 않은 부서가 상당 비율(46.8%)을 차지하고, 금융사고예방대책 관련 자점검사항목도 미비되어 있는데다, 자금•결제, 자산 운용 등 업무 성격상 일별 점검이 필요한 항목도 월별 자점감사 항목으로 운영하고 있는 등 자점감사가 시의성 있게 이루어지지 않고 있다.

또한, 각 부서의 준법감시담당자가 실시한 자점감사에 대한 부서장의 확인(승인) 등의 절차가 없어 담당자가 상당기간 자점감사를 수행하지 않은 사실이 AO팀의 사후 점검 과정에서 뒤늦게 발견된 사례도 있는 등 자점감사 업무 운영상 미흡한 점이 발견되었다.

<조치할 사항>

따라서 은행은 소관부서별 업무특성에 따라 법규 준수 필요사항, 금융사고예방대책 관련 사항이 포함되도록 자점감사 항목을 신설•정비하고, 업무 수행 빈도, 중요도 등을 감안하여 점검주기(일•월•분기)를 설정하여 적시성 있게 자점감사를 수행토록 하는 한편,

자점감사 항목별 점검 방법을 보다 구체화하고, 준법감시담당자의 자점검사 결과는 자점감사시스템을 통하여 부서장 확인(승인) 후 AO팀의 2차 점검이 적시에 이루어지도록 관련 절차와 시스템을 정비하시기 바랍니다.

(다) 사후관리 절차 구체화 및 관련 시스템 정비

각 부서내 준법감시담당자의 자체 점검 결과에 대해서는 AO팀이 2차 점검을

수행하고 있으나, 미흡사항에 대한 조치 요구 방법, 이행기일 설정, 이행결과 보고 절차를 구체적으로 마련하고 있지 않다.

이에 따라 2차 점검과정에서 나타난 미흡사항에 대한 개선계획 및 이행기일을 AO팀과 소관부서 담당자간 협의를 통해 결정하고, 이행실적도 소관부서장의 승인 등을 통한 정식보고 없이 AO팀이 이행기일 도래시에 사후적으로 재점검하며 추가 조치방안을 요구하거나 내부통제 위반사항에 대한 불이익 조치 없이 이력을 관리하는데 그치고 있는 등 실질적으로 사후 관리가 수행되지 않고 있다.

<조치할 사항>

은행은 자점감사시 확인된 내부통제 관련 위반사항에 대한 이행기일 설정 및 조치요구, 개선 결과에 대한 보고절차 등 사후관리 절차를 구체적으로 마련•규정화할 필요가 있으며, 사후관리 업무가 철저히 이행될 수 있도록 자점감사 시스템 운영을 위한 전담 인력 배치 등 준법감시 인력을 확보하시기 바랍니다.

(8) 내부감사업무 계획 및 사후관리 업무 개선

은행은 사외이사로 구성된 감사위원회를 보좌하는 AP팀을 별도로 두어 상시적인 내부감사업무를 수행토록 하고 있으나 내부감사업무와 관련하여 아래 ㈎~㈐와 같은 문제점이 확인되었다.

(가) 내부 정기감사 운영기준 마련

매년 감사위원회 승인을 거쳐 감사계획을 수립하고 있으나, 부서•업무별 감사주기 등 내부 정기감사에 대한 세부 운영기준을 마련하지 않은 채 충분하지 않은 감사 인력에 맞추어 감사계획을 수립하고 있어 주로 법령•대외규정에서 의무 사항으로 정하고 있는 내부통제시스템평가, 내부회계관리제도, 리스크 등 특정부분에 감사가 편중되고 있으며, 사고 발생 등 위험요인이 큰 일부 영업 부서 중심으로 내부감사가 수행되어 준법, 경영, 재무, IT 등 업무 전반에 대한 내부감사가 충실히 수행되지 않을 우려가 있다.

<조치할 사항>

따라서 은행 전반에 대한 내부감사가 충실히 수행될 수 있도록 은행조직 특성에 맞게 부서•업무별 집중 감사 항목 및 주기 설정 등 중장기 내부감사 운영기준을 마련하는 한편, 동 기준에 따른 내부감사 수행을 위해 전문 감사 인력을 충분히 확보하시기 바랍니다.

(나) IT부분 내부감사 업무 절차 개선

IT부분 감사업무 강화를 위해 AQ팀을 최고기술책임자 산하에 별도 설치(2024.7월)하였으나, 감사위원회를 보조하는 AP팀과의 역할과 업무분장, 부서간 업무협의 절차 등이 명확하게 마련되어 있지 않아, AQ팀의 감사업무가 감사위원회의 승인을 득하는 감사계획과 연계되지 않으며, AQ팀의 감사결과도 감사위원회 등에 보고되지 않고 IT부서를 총괄•담당하는 최고기술책임자(CTO)에게 보고하는데 그쳐 IT부분 감사업무의 실효성이 확보되지 않을 우려가 있다.

<조치할 사항>

따라서 은행은 AQ팀과 감사계획 수립 및 결과 보고시 감사위원회를 보좌하는 조직인 AP팀 간의 역할을 명확히 하고 부서간 업무협의•보고절차 등을 구체화함으로써 IT부문 자체감사 업무가 실효적으로 수행되고 주요 감사 결과가 경영진 및 감사위원회 등에 충실히 보고될 수 있도록 IT부문 내부감사 관련 기준 및 절차를 개선하시기 바랍니다.

(다) 사후관리 절차 구체화 및 관련 시스템 정비

내부감사 결과에 대한 이행기일 설정 및 개선 계획의 이행 미흡시 추가조치 요구 등 사후관리 절차가 구체적으로 마련되어 있지 않아 사안별로 감사대상 부서와 AP팀이 협의•판단하여 이행기일을 1~9개월까지 달리 설정하고 있으며, 이행기일 연장도 이행 미흡에 대한 재정리 요구나 담당임원의 승인 및 보고 등 절차 없이 부서간 협의로 가능하게 운영하는 등 사후관리 업무가 철저히 수행되지 않고 있으며, 사후조치 내역 및 이력 등이 전산시스템을 통해 체계적으로 관리되지 않고 AP팀이 엑셀로 수기 관리하고 있는 등 사후관리 업무와 관련된 제반 시스템도 미비되어 있다.

<조치할 사항>

따라서 은행은 사후관리 업무가 효과적으로 이루어질 수 있도록 내부감사 결과에 대한 이행기일 설정, 이행계획의 수립 및 결과 보고 절차 등을 구체적으로 마련하는 한편, 관련 사항이 체계적으로 관리될 수 있도록 시스템을 마련하시기 바랍니다.

(9) 프로그램 변경 시 품질보증테스트 방법 개선

은행은 2023.3월부터 전산 프로그램 변경과 관련한 품질보증 테스트 업무를 담당하는 별도의 조직(AR팀)을 신설하였다.

그러나 은행은 품질보증 테스트 수행 대상을 명확히 정의하지 않고 개발자가 테스트 필요 여부를 판단하여 테스트를 의뢰한 경우에만 품질보증 테스트를 수행하도록 하여 2024년중 전체 프로그램 변경건(배포건기준, □□,□□□건)의 □.□%(□□□건)만이 테스트 수행되는데 그치는 등 실효성 있게 수행되지 않고 있다.

<조치할 사항>

따라서 은행은 신상품 여부, 사용자 및 시스템에 미치는 영향 등을 감안하여 경미한 사항에 대해서만 사전적으로 예외 승인절차를 거쳐 품질보증업무를 생략할 수 있도록 테스트 실시 기준 및 절차를 마련(규정화)하여 그에 따라 품질보증테스트 업무를 철저히 수행하는 한편, 품질보증테스트 생략 대상에 대한 별도의 사후 점검기준을 마련하시기 바랍니다.

(10) 금리 산정 적정성 검증 내부통제 개선

(가) 금리 산정 적정성 검증 관련 내부통제 강화

은행은 여신상품 판매시 금리가 적정하게 산정 및 적용되었는지 점검할 필요가 있다.

그러나 은행은 신상품 출시 및 금리 조건 변경 등 금리산출과 관련된 중요 사항 발생시 품질보증 테스트 또는 시나리오 테스트를 수행하지 않는 등 사전적 검증 절차가 미흡한 점이 확인되었다.

또한, 여신 상품 담당 부서에서 월 단위 자점감사를 제한적 범위로만 수행하였고, 산출 금리의 자체 모니터링 과정에서 이상 요인이 발견된 경우에도 점검담당자를 지정하지 않았으며, 점검 내용을 기록•보고하는 절차가 없어 금리 오류를 적시에 발견하지 못하는 등 금리산정의 적정성 점검 절차가 미흡한 점이 확인되었다.

<조치할 사항>

따라서 은행은 금리산정 관련 프로그램 또는 시스템 개발 인력을 추가로 확보하며, 테스트를 의무화하는 등 적정 금리산정을 위해 시스템을 개선하시기 바랍니다. 또한 상품담당 부서의 자체 점검 주기를 월 단위에서 일 단위로 축소하고 점검 항목을 확대하며, 점검 담당자 지정 및 결과 보고 절차를 마련하는 등 금리산정의 적정성 점검 절차를 강화하시기 바랍니다.

(나) 금리 산정 오류 발생 시 보고체계 개선

은행은 금리산정 오류로 고객 또는 은행 손실이 발생할 경우 손실의 내용과 처리 방법을 영업담당 임원(Head of product)에게만 보고하도록 정하고 있어 고객 안내 및 손실 보상 등 금융소비자 보호 절차 및 재발 방지 대책 마련을 소홀히 할 우려가 있다.

<조치할 사항>

따라서 은행은 금리 산정 오류 발생 등으로 고객 또는 은행의 손실가능성이 높은 사항은 손실 확정 전 리스크관리 부서* 등에 적시에 보고토록 하고 중요 사항은 주요 경영진(예: 위험관리심의회)에게 보고하여 재발 방지 대책을 수립•논의할 수 있도록 보고 체계를 개선하시기 바랍니다.

* 운영위험관리를 위한 총괄 부서

(11) 명령휴가제도 운영 강화

은행은 명령휴가자에 대한 직무점검시 일부 점검항목이 누락되었거나 증빙 첨부가 누락 되는 등 미흡사항이 있었음에도 명령휴가 실시 부서장이 별도 검증 없이 승인하는 등 명령휴가자에 대한 직무점검이 적절히 이행되지 않았다.

또한, 명령휴가 대상자 및 명령휴가 기한 관리 등이 수기로 이뤄지는 등 전산 시스템으로 관리되지 않고, 명령휴가 실시 예정 통보가 누락(2건)되거나 결과

보고가 지연(3건)되는 경우도 발생하였다.

<조치할 사항>

따라서 은행은 명령휴가 실시 부서장의 1차 검증을 의무화하고, 직무점검 항목, 세부 절차* 등을 내규로 마련하는 한편, 명령휴가 대상자 관리, 기한 관리(기한 도래시 해당 부서장에 알람 발송 등), 직무점검 항목 등을 시스템으로 관리하여, 명령휴가제도의 실효성을 제고하시기 바랍니다.

* 명령휴가 실시 예정 통보 및 결과 보고에 대한 기한 설정, 명령휴가 실시 부서장의 검증 의무 등을 내규에 반영

(12) 직무분리제도 운영 개선

내규「금융사고예방지침」제8조에 따르면 은행은 분리 대상 세부 직무와 해당 직무의 담당 직원을 등록관리하는 시스템을 운영하고 변동사항이 발생하는 경우 지체없이 시스템에 반영하여야 한다.

그러나 전산 개발•운영간 직무 분리의 경우 월별로 AS팀에서 AT팀에 의뢰하여 인사시스템에 세부 직무 및 해당 직무담당 직원을 입력함에 따라 월중 인사발령 등 직무 변경사항 발생시에도 익월에 일괄 반영되어 적시성이 떨어질 소지가 있다.

또한, 같은 내규 제9조에 따라 은행은 분리대상 세부직무의 적정성을 매년 평가하고 필요한 경우에는 조정하여야 하나, 2024년 직무분리 대상자를 확정하는 과정에서 직무분리 대상 선정의 적정성 검토를 이행하지 않았다.

<조치할 사항>

따라서 은행은 직무분리 변동사항 발생 시 시스템에 즉시 반영하도록 개선하여 적시성을 강화하고, 분리대상 직무에 대한 적정성 검토를 매년 이행하여 직무분리제도의 실효성을 강화하시기 바랍니다.

(13) 법규준수 체크리스트 마련을 통한 임직원 내부통제 강화

은행은 임직원이 업무수행시 관련 법규와 절차를 적절하게 준수하고 있는지를 점검하여 내부통제 관련 업무를 평가 및 운영하여야 한다.

그러나 은행은 각 부서별로 임직원이 준수해야 하는 법규를 명확히 인지하기 어려움에도 법규준수 체크리스트를 마련하지 않았고 임직원의 내부통제 준수 여부에 대한 효과적인 점검 및 관련 교육도 이루어지지 않았다.

또한, 법규준수 체크리스트를 바탕으로 자점감사 항목 반영여부 및 점검방식 등을 판단하여야 하나, 해당 절차가 없고 법령상 준수의무가 있는 자점감사 항목을 점검대상에서 제외하는 사례가 발생하였다.

<조치할 사항>

따라서 은행은 각 부서별로 준수해야 할 법규를 명확히 인지하고, 자점감사 항목의 적정성 평가와 임직원 내부통제 관련 교육 등에 활용할 수 있도록 법규준수 체크리스트를 마련하여 내부통제를 강화하시기 바랍니다.

(14) 비대면 실명확인절차 개선

내규「신분증 모니터링 업무매뉴얼」제5조, 제6조 등에 따라 비대면 실명확인 절차가 완료된 후라도 사후 검증*을 통한 실명확인에 실패할 경우 고객이 실명확인증표를 다시 제출하고 검증을 완료할 때까지 상품의 신규, 해지 및 계좌이체 등 거래를 원칙적으로 제한하고 있다.

* 실명확인증표의 실물 촬영 여부, 사진영역/텍스트 정보에 가림이 있는지 여부 등을 확인하며, 고객정보가 불일치하거나 실물촬영이 아니거나 사진영역 노후화 등으로 식별이 불가능한 경우 반려

그러나 제3자가 피해자 명의를 도용하여 실명확인절차를 완료한 후 은행이 사후검증을 시행하기 전 거래가 허용되는 기간 중 명의도용 피해자 명의로 대출을 받은 사례*가 발생하였다.

* 민원인 甲은 제3자가 甲의 명의를 도용하여 계좌개설 후 사후검증 완료 전인 2022.8.7. 甲명의로 대출이 실행되었으나, 2022.8.8. 사후검증시 실명확인실패로 거래제한 조치 되었음

<조치할 사항>

따라서 은행은 실명확인 절차 완료 후 사후검증 시행 전 신분증 위·변조 탐지

프로그램을 강화하여 추가검증이 필요한 건을 우선 탐지하고, 해당 건에 대한 사후 검증 시행 전 대출 실행을 금지하시기 바랍니다.

(15) ㉮인증서 본인확인절차 관련 개선

(가) 대출신청 및 예금계좌 해지시 본인확인 조치

은행은 이용자가 대출을 신청하거나 예금을 해지하는 경우 AU가 발급하는 ㉮인증서를 유일한 본인확인 수단으로 활용하고 있다.

그러나 ㉯앱 및 ㉮인증서가 설치된 휴대기기의 도난 또는 분실시 이용자가 전화번호를 해지하더라도 휴대기기를 습득한 제3자가 비밀번호를 재설정하고, 휴대기기에 저장된 신분증 사본을 활용하는 수법 등을 통해 정상 거래를 할 수 있으므로 명의도용 대출이 발생할 우려가 있다.

<조치할 사항>

따라서 은행은 이용자가 은행 앱에 로그인할 경우 ㉯앱 비밀번호의 변경 여부, 은행에 등록된 기기 및 번호와 다른 기기 및 번호로 로그인 시도 여부, 휴대전화에 유심칩이 인식되지 않는 경우 등 고객 본인 여부가 우려되는 사안에 대하여 휴대전화 본인확인 등 추가 인증 절차를 도입하시기 바랍니다.

(나) 비대면 실명확인 시 ㉮인증서의 이용

은행연합회 및 금융투자협회가 마련한 「비대면 실명확인 관련 구체적 적용방안」에 따르면 은행은 비대면 실명확인 방식 5가지* 중 2가지 이상을 중첩하여 적용해야 하고 이와 함께 금융회사 자체적으로 추가 확인 방식**을 적용함으로써 가급적 다중의 검증과정을 거친 후 계좌를 개설할 것을 권고하고 있으며,

* ①실명확인증표 사본 제출, ②영상통화 등 ③본인에게 접근매체 등 전달과정에서 확인 ④기존계좌 활용 ⑤생체 정보 등 기타 이에 준하는 방법 중

** ①~⑤ 방식의 기본확인방법을 보완·보조하기 위한 것으로, "⑥타 기관 확인결과 활용", "⑦다수의 고객정보 검증" 방식 등을 추가 적용

은행은 권고사항인 추가 확인방식의 적용시 주로 ㉮인증서를 '타기관 확인

결과 활용’ 방식으로 이용하고 있다.

그러나, AU는 ㈜인증서 발급시 신분증 확인 등 본인확인 업무 일체를 은행에 위탁하고 있고, 검사대상기간 중 인증관련 업무 및 고객 서비스 대응, 신분증 진위확인 스크래핑 관련 업무를 하는 개발자 인력이 AU와 은행의 업무를 겸직한 사례가 있었으며, AU와 은행은 하나의 앱을 공유하고 있어 ㈜인증서를 독립된 제3의 기관에 의한 다중의 검증 절차로 보기엔 미흡한 측면이 있다.

<조치할 사항>

따라서 은행은 고객 정보 및 이용 패턴 등을 고려하여 고객별로 위험도를 파악하고 위험도별로 본인확인 절차를 강화하시기 바랍니다.

(16) 계약관리 절차 개선

(가) 이사회 결의 누락

「상법」 제398조, 내규「이사회규정」 제9조 등에 따르면 은행은 주요 주주 등과 계약 체결 시 이사회 결의를 받아야 하는데도 이사회 사전 결의를 받지 않은 사례*가 있다.

* 주요 주주와의 계약이 이사회 결의 대상임을 인지하지 못하거나, 기 체결된 계약의 변경 계약 체결시 이사회 사전결의를 거치지 않은 경우 등

<조치할 사항>

은행은 계약 검토 과정에서 주요 주주에 대한 안내 문구가 표시되도록 시스템을 개선하여 이사회 결의 누락을 방지하고 이사회 결의시 승인의 범위를 명확히 하시기 바랍니다.

(나) 계약의 적정성 검토 절차 미흡

내규「일반계약사무지침」 제6조 및「IT계약사무지침」 제6조 등에 따르면 업체 선정 방법에는 공개경쟁입찰, 제한경쟁입찰, 지명경쟁입찰, 수의계약이 있으며, 계약 담당자는 사업의 특성을 고려하여 적정한 방법을 결정하여야 하나, 검사대상기간 중 은행이 체결한 계약 □,□□□건 중 수의계약이 □,□□□건에 해당하는 등 수의계약 비중(□□%)이 높고,

대주주의 특수관계인과의 계약에 따른 광고 진행에 앞서 광고비 책정 기준을 마련하지 못해 광고비를 사전에 확정하지 못하고 광고를 진행한 사례가 있었다.

<조치할 사항>

따라서 은행은 수의계약 체결시 비교 견적을 받도록 하고, 비교 견적이 불가능할 경우 IT투자심의소위원회 등 독립적인 조직의 승인을 받아서 가격의 적정성을 검토하도록 하며, 대주주 및 특수관계인과의 거래시 기존 동종업계의 평균단가를 활용하거나 회계법인과의 용역계약 체결을 통해 적정가격을 산출하는 등 계약의 적정성 검토를 강화하시기 바랍니다.

(다) 소급계약 등 계약체결 관리 절차 미흡

내규「계약사무규정」제6조 등에 따르면 계약담당자는 AW팀 또는 AX팀 등 유관부서의 사전 검토를 받아야 하지만 일부 계약은 AW팀 검토를 누락하였고, 계약의 체결은 계약 시작 일자 이전에 이루어져야 하지만 검사대상기간 중 체결한 129건의 계약은 계약 시작일자 이후에 체결되어 소급하여 효력이 발생하였다.

<조치할 사항>

따라서 은행은 AW팀 검토가 누락되지 않도록 시스템을 개선하고, 소급계약을 체결하지 않도록 임직원을 대상으로 교육을 진행하는 한편, 불가피한 경우 그 사유와 재발방지대책을 명시하도록 개선하시기 바랍니다.

(17) 통신사기피해환급법에 따른 본인확인조치 누락

은행은 이용자의 계좌가 피해의심거래계좌로 추정되어「통신사기피해환급법」제2조의5에 따라 임시조치*를 하는 경우 피해 예방을 위하여 본인확인을 거쳐야 한다.

* 해당 이용자 계좌의 전부 또는 일부에 대하여 이체, 송금 또는 출금을 지연시키거나 일시 정지하는 조치

그러나 은행은 2021.7.30~2024.9.30 기간 중 임시조치한 피해의심거래계좌

및 타 기관이 임시조치를 요청한 일부 피해의심거래계좌에 대하여 은행 내규 「이상금융거래 탐지시스템(FDS) 업무 매뉴얼」에 따라 그 임시조치를 해제하면서 본인확인 절차 수행에 일부 미흡한 사례*가 있었다.

* 본인확인조치 없이 임의적으로 피해의심거래계좌가 아니라고(오탐지) 판단하고 임시조치를 해제

<조치할 사항>

따라서 은행은 임시조치 해제 절차 중 본인확인이 적절히 이루어질 수 있도록 개선하시기 바랍니다.

(18) 개인정보 수집•제공(제3자) 최소화 및 점검절차 마련

은행은 내규 「개인신용정보보호규정」 제9조 등에 따라 개인(신용)정보는 정보주체에게 동의를 받은 이용목적에 따라 필요한 최소한의 범위 안에서 제한적으로 수집 및 제3자에게 제공되도록 하여야 한다.

그러나 은행이 수집 또는 제3자에게 제공하고 있는 개인정보에 대한 처리 목적, 범위 등에 대한 정기적인 점검 절차가 없어, 실제 활용하고 있지 않은 정보임에도 필수(동의) 항목으로 운영하여 개인정보를 지속 수집하거나, 제3자에게 제공되는 등 미흡한 사례가 발견되었다.

<조치할 사항>

따라서 은행은 개인정보 수집 및 제공범위를 목적에 부합하도록 최소화하는 한편, 향후 유사한 사례가 발생하지 않도록 계약의 변경 또는 갱신시에는 개인정보의 처리 목적 및 항목의 범위 등에 대한 정합성 검토가 재수행되도록 하고, 정기적(예:분•반기)으로 전 사업부서의 개인정보 수집•활용•이용 실태 점검을 수행하여 필요시 개인정보 수집 및 제공 중단 등의 조치를 적시에 취할 수 있도록 관련 절차를 개선하시길 바랍니다.

(19) 신용정보전산시스템 보안대책 관리 강화

은행은 내규 「개인신용정보보호규정」 제12조, 「신용정보법」 제19조 등에 따라 개인신용정보처리시스템의 제3자 접근 등에 관한 기술적•물리적 보안대책을 마련하고 관리해야 한다.

그러나 은행은 신용정보관리•보호인의 심사없이 시스템 권한 관리자 또는 소속 부서장이 개인신용정보 조회권한 요청을 승인하거나 하위 직급자(매니저)가 승인한 사례가 발생하였다.

또한 은행은 고객정보조회 기록 관리를 소홀히 함으로써 조회목적을 잘못기재하였거나, 조회목적이 확인되지 않는 등 보안대책 시행이 미흡하여 직원의 도덕적 해이와 그에 따른 고객정보 유출 등이 발생할 우려가 있다.

<조치할 사항>

따라서 은행은 신용정보처리시스템 관리 부서(AY팀, AZ팀 등)의 검토 등 적합한 심사를 거쳐 조회권한이 승인되도록 권한 부여 절차를 개선하고, 고객정보조회시 목적과 증빙을 필수로 입력하는 등 신용조회기록 관리를 강화하시기 바랍니다.

(20) 개인신용정보 처리 관련 적정성 점검 강화

은행은 내규「개인신용정보보호규정」제16조에 따라 개인신용정보 처리와 관련한 다수 시나리오를 생성하여 시나리오별 이상징후를 모니터링하고, 분기별로 개인신용정보 조회 및 처리에 대한 적정성을 점검하고 있다.

그러나 점검 과정에서 일부 시나리오의 실효성이 낮아 오탐지 건이 다수 존재하고, 이상징후가 발견된 경우, 이에 대한 소명 내용이 명확하지 않거나 증빙 확인이 되지 않았음에도 대부분 '이슈 없음'으로 종료되어 점검의 실효성이 저하될 우려가 있다.

< 조치할 사항 >

따라서 은행은 이상징후 시나리오를 고도화하여 오탐률을 최소화하고, 이상징후 발견시 소명 내용을 철저히 기록하며, 증빙을 필수적으로 첨부하는 등 점검 절차를 강화하시기 바랍니다.

(21) 채무불이행 정보 등록 관련 업무절차 개선

은행은「채권의 공정한 추심에 관한 법률」제8조에 따라 채무부존재 소송을

제기하여 진행중인 고객의 채무불이행자 등록 방지 등을 위해 법원으로부터 고객의 채무부존재 소송 관련 서류를 송달받아 소송이 진행중인 사실을 인지한 이후 전산에 이를 등록하여 관리하고 있다.

그러나 법원 우편물이 담당자에게 인계되는 과정상 절차 지연 및 전달 오류 등의 사유로 은행 소송 인지일(우편물 도달일)과 소송 전산 등록일간 차이가 발생하고 있어 채무부존재 소송 정보 등록이 지연되거나, 은행의 소송 인지 이후에도 채무불이행자로 등록될 우려가 있다.

<조치할 사항>

따라서 은행은 채무부존재 소송 등 개인신용정보의 수기 등록•변경이 필요한 사항에 대해 적시에 전산 등록될 수 있도록 관련 부서간 인계 절차를 간소화하고, 일별 점검하는 등 업무 절차를 개선하시기 바랍니다.

(22) 자료반출시스템 관리 강화

은행은 망간자료전송시스템(FTC)을 통해 내부 자료의 외부망 전송시 DLP(정보유출방지시스템) 솔루션을 통해 개인정보가 포함된 자료가 탐지되는 경우 자료반출시스템을 통해 BA팀의 승인을 득하고 반출하도록 안내하고 있다.

그러나 은행은 주민등록번호 등 개인정보가 포함된 자료임에도 토스메일 시스템을 통하면 BA팀의 승인이 아닌 소속 부서장의 승인만 받고 반출이 가능하여 개인정보 자료의 부당 유출 우려가 있다.

<조치할 사항>

따라서 은행은 개인정보가 포함된 자료의 경우 반드시 자료반출시스템을 통해 BA팀의 승인을 받고 반출하도록 지침을 마련하고, 개인정보 반출 내역을 주기적으로 사후 모니터링하는 절차를 마련하시기 바랍니다

(23) 정보보안 자체감사 조직 정비 및 감사 실효성 미흡

은행은 IT부문 감사조직을 감사팀(ㅇ명) 및 IT자체감사팀(ㅇ명, 2024.7.신설)으로

구성하여 정기·상시·특별 감사를 수행하고 있다.

그러나 은행은 감사팀 및 IT자체감사인력에 정보보안 전담 감사인력을 배정하고 있지 않는 등 정보보안 업무에 대하여 자체감사가 제한적으로 이루어질 우려가 있으며,

외주업체에 전산운영업무를 위탁하고 있음에도 검사대상기간 중 위탁처리 업무의 적정성에 대한 감사를 실시하지 않는 등 IT감사계획 및 범위의 적시성 및 실효성이 저하될 우려가 있다.

<조치할 사항>

따라서 은행은 정보보안 부문에 대한 자체 감사조직 및 인력을 확보하고 위탁처리 업무에 대한 감사계획을 수립하는 등 감사조직 및 계획을 개선하시기 바랍니다.

(24) 핵심업무 선정 기준 불명확 및 비상계획 실효성 불합리

은행은 내규「업무연속성계획 관리 지침」제5조 등에 따라 비상계획보고서를 작성하여 재해복구전략의 유효성 등을 연 1회 이상 대표이사에게 보고하고 업무연속성 유지를 위한 핵심업무를 선정하여 업무영향분석을 실시하여야 한다.

그러나 동 비상계획 보고서는 재해복구전략의 유효성에 대한 점검 없이 업무연속성계획 현황 위주로만 작성되어 있으며,

업무연속성계획 관련 문서마다 핵심업무의 종류와 개수가 서로 다르게 기재되어있는 등 핵심업무 선정 기준이 불명확하여 업무연속성계획에 핵심업무가 누락될 우려가 있다.

<조치할 사항>

따라서 은행은 재해복구전략의 유효성을 점검하고, 업무연속성계획에 핵심업무가 누락 되지 않도록 핵심업무 선정 기준을 명확히 하는 등 관련 절차를 개선 하시기 바랍니다.

(25) 대외기관과의 비상대응 훈련 불철저

은행은 내규 「업무연속성계획 관리 지침」 제8조에 따라 업무중단 사태에 대비하고 업무연속성계획의 실행가능성을 확인하기 위하여 연 1회 이상 모의훈련을 실시하여야 한다.

그러나 은행은 AD 계열사 및 대외기관과의 합동 비상대응 모의훈련은 실시하면서도,

AD 앱 장애 대비 모의훈련을 합동하여 실시하지 않았으며 핵심업무와 연계된 서비스를 제공하는 대외기관과 정기적인 모의훈련 계획도 마련하지 않았다.

<조치할 사항>

따라서 은행은 계열사 및 대외기관과 재해복구 전환훈련 계획을 마련·실시하는 등 비상대응 훈련의 실효성을 확보하시기 바랍니다.

(26) 이상금융거래탐지시스템 협의체 운영 절차 부재

은행은 내규 「이상금융거래탐지시스템 운영 지침」 제2조 등에 따라 전자금융거래 전반을 종합적으로 분석하여 이상금융거래를 탐지·차단·모니터링하는 이상금융거래탐지시스템(이하 'FDS')을 구축하여 운영하고 있다.

그러나 은행은 FDS 업무 유관부서와 FDS 탐지룰의 적정성을 정기적으로 점검하여 신규 위험에 대응하는 체계를 마련하고 있지 않는 등 이상금융거래에 대한 사전 예방 활동이 미흡하다.

<조치할 사항>

따라서 은행은 유관부서들이 함께 FDS 협의회를 정기적으로 개최하여 FDS 탐지 요건의 적정성을 검토하고, 회의 결과를 관련 부서에 전파할 수 있도록 FDS 협의체 운영 절차를 마련하여 운영하시기 바랍니다.

(27) 전산원장 변경 통제 불철저

은행은 내규「전산원장변경지침」 제4조 등에 장애 또는 오류 등으로 인한 전산원장 변경 시 변경 전·후 내용을 기록하고, 책임자 승인 및 제3자 확인을 받도록 정하고 있다.

그러나 은행은 업무시간 외 전산원장 긴급 변경에 대한 사후 승인 절차가 없고, 일부 배치프로그램을 통한 전산원장 변경은 변경 전·후 내용을 기록하지 않는 등 전산원장 변경 통제가 미흡하다.

<조치할 사항>

따라서 은행은 전산원장 긴급 변경 시 책임자 확인 및 제3자 검증을 수행하고, 배치프로그램에 의한 전산원장 변경도 변경 전·후 내용을 기록할 수 있도록 전산원장 변경 통제를 강화하시기 바랍니다.

(28) 정보처리시스템 및 데이터베이스 접근통제 미흡

은행은 내규「정보시스템 보안 지침」 제14조 및「계정관리 지침」 제10조에 따라 정보처리시스템 및 데이터베이스관리시스템에 대한 사용자 접속 및 중요 명령어 실행* 등을 서버 및 DB 접근제어시스템으로 통제하고 있으며, 서버·DB 접근제어시스템, 서버보안솔루션 등을 이용하여 정보처리시스템 및 데이터베이스관리시스템의 비인가 접근을 통제하고 있다.

* 데이터베이스에 저장된 정보의 수정(update), 삭제(delete), 입력(insert) 등

그러나 은행은 서버에 대해서 ㈜ 스크립트 사용을 통제하지 않아, ㈜ 스크립트로 DB 접근제어시스템을 우회하여 데이터베이스관리시스템에 접속할 수 있어 데이터베이스에 저장된 정보를 무단 조작할 위험이 있다.

<조치할 사항>

따라서 은행은 DB 접근제어시스템에 대한 우회 접속을 차단할 수 있도록 중요 명령어 통제 및 ㈜ 스크립트 관리 절차 등 정보처리시스템의 접근통제를 개선하시기 바랍니다.

(29) 대외 송신 파일 수작업 운영 불합리

은행은 내규「개발관리지침」제16조에 대외송신 파일 생성 배치작업 오류 발생 시 관련 파일을 수작업으로 재생성 및 전송할 수 있도록 승인 절차를 마련하였다.

그러나 대외기관에 송신하기 위한 파일을 수작업으로 재생성하는 과정에서 작업내용 기록 부실 및 데이터 정합성 검증 불합리 등과 같은 미흡사항이 확인되었고,

통합단말 내 수작업 파일 전송 이력에 전송 사유 등 주요 정보를 포함하지 않아* 대외기관으로의 파일 전송 이력에 대한 사후관리가 어려울 우려가 있다.

* 대외기관 파일전송 승인이력에 대상 기관, 전문유형, 발송사유를 기록하지 않음

<조치할 사항>

따라서 은행은 대외기관으로의 수작업 생성 파일을 송신 시 작업내용 기록 및 데이터 정합성 검증 절차를 개선하고

파일 전송 사유, 대상 기관 등의 상세내역을 통합단말 화면에 기록·마련하는 등 대외기관 파일 전송 이력 관리 절차 및 방법을 개선하시기 바랍니다.

(30) 전산센터 물리적 통제 운영 불철저

은행은 내규「물리적보안지침」제4장 등에 따라 전산실 보호를 위해 전산센터 출입 시 신분확인 및 생체인증 등의 출입통제 절차를 운영하고, 서버랙(RACK)을 설치하여 서버 등 전산장비를 운영·보호하고 있다.

그러나 은행은 전산센터에 금속탐지기 등 이동식 저장매체의 반입·반출 여부를 확인 및 검사할 수 있는 통제장치를 운영하지 않고 있으며,

전산실 내에 설치된 서버 랙(RACK)의 ○%가 잠금장치가 없이(오픈형 랙) 운영되고 있어 작업자의 과실 또는 고의에 의한 저장장치 탈착 및 저장매체 유출 등의 전산사고로 이어질 우려가 있다.

<조치할 사항>

따라서 은행은 전산센터에서의 이동식 저장매체 반입·반출 통제를 강화하고 전산장비에 위해를 가하지 못하도록 장비 훼손·유출 등의 사고위험이 큰 오픈형 랙에 잠금장치를 설치하는 등 작업통제를 강화하시기 바랍니다.

(31) 일괄(배치)작업 관리 미흡

은행의 오퍼레이터는 내규「개발관리지침」제16조 등에 따라 배치(Batch)프로그램 작업 중 오류가 발생하는 경우 작업을 중단하고 해당 업무 담당자 확인을 받고 오류 일시, 오류 내용, 확인자 등을 기록·관리하고 있다.

그러나 은행은 일부 일괄작업에서 동일한 원인에 의한 오류가 반복적으로 발생하고 있음에도 오류 발생 원인분석 및 사후관리를 하지 않고 있어 일괄작업 반복 오류로 전산사고가 발생할 우려가 있다.

<조치할 사항>

따라서 은행은 동일한 오류가 반복적으로 발생하는 일괄작업 프로그램에 대하여 오류 유형 및 원인 등을 분석·조치하고 조치 결과를 관리자에게 보고하는 등 일괄작업 반복 오류에 대한 관리 절차를 개선하시기 바랍니다.

(32) 공유 폴더 보안관리 소홀

은행은 내규「단말보안지침」제10조 및 제11조에 따라 공유폴더의 접근권한을 사용자별로 부여하고 단말기 내 개인정보 보관 여부의 탐지 및 개인정보 파일의 암호화 정책을 수립·운용하고 있다.

그러나 은행은 IT개발 등을 수행하는 외부직원이 사용하는 공유폴더는 사용자 접속 권한의 제한 없이 모든 공유폴더에 대한 접근을 허용하고 있으며,

동 공유폴더에 저장된 파일들은 개인정보 보관 여부의 탐지와 암호화 정책을 적용하지 않고 있어 중요정보가 암호화되지 않은 상태로 보관되거나 유출될 위험이 있다.

<조치할 사항>

따라서 은행은 외부직원이 사용하는 공유폴더의 접속 권한을 사용자별로 부여하는 등 접근통제를 강화하고 동 공유폴더에 대해서도 개인정보 보관 여부의 탐지 및 암호화 정책을 수립하여 운영하는 등 공유폴더 보안관리를 강화하시기 바랍니다.

(33) 단말기 보안 통제 불철저

(가) 단말기 내 필수 보안프로그램 점검 개선

은행은 내규「단말보안지침」제14조에 따라 단말기에 네트워크 접근제어 시스템을 적용하여 단말기 내 필수 프로그램의 설치 여부를 점검하고 동 필수 프로그램을 설치하지 않은 단말의 네트워크 접근 등을 통제하고 있다.

그러나 은행의 내부망 단말기에 대해서는 동 네트워크접근제어 시스템을 적용하지 않아 필수 프로그램의 삭제 여부를 점검하지 못하는 등 은행 내 보안 정책 미준수 단말기가 존재할 우려가 있다.

(나) 개인정보 자료 탐지 및 암호화 정책 개선

은행은 내규「단말보안지침」제7조에 따라 내부 자료 유출 방지를 위한 자료유출방지 시스템을 운영하여 내부망 등 단말기 내 파일의 개인정보 파일 탐지 및 암호화 정책을 적용하고 있다.

그러나 동 자료유출방지 시스템은 단말기 내 이미지 파일 등에 대해서는 개인정보 탐지 및 암호화 정책을 적용하지 않고 있어 중요자료를 허가 없이 보관하거나 자료 유출 사고 등으로 이어질 우려가 있다.

(다) 안티바이러스 프로그램 운영 개선

은행은 내규「단말보안지침」제13조 등에 따라 단말기 등에 악성코드 감염·치료 프로그램을 설치하여 악성코드 감염 여부 검사를 수행하고 악성코드에 감염된 단말기에 대해서는 네트워크 격리 및 포맷 처리 등의 조치를 하고 있다.

그러나 은행은 악성코드 감염검사를 완료하지 않은 단말기가 존재하여도 적절한 개선 조치 없이 그대로 방치 및 운영하거나,

악성코드에 감염된 단말기에 대한 조치 결과를 책임자에게 보고하지 않는 등 조치가 미흡하여 악성코드 감염으로 인한 전산사고가 발생할 우려가 있다.

<조치할 사항>

따라서 은행은 단말기에 네트워크 접근제어 시스템을 적용하는 등 필수 프로그램의 설치 여부 점검 및 통제 절차를 강화하고

자료유출방지 시스템의 적용 대상을 이미지 파일 등에 확대 적용하는 등 개인정보 파일 탐지 및 암호화 정책을 개선하며

악성코드 검사 결과 관리 강화 및 감염 시 책임자 보고 체계를 마련하는 등 악성코드 예방 및 감염 방지 대책을 강화하시기 바랍니다.

(34) 암호화 키 관리절차 미흡

은행은 내규「암호화지침」제11조 등에 따라 암호화 키 관리 시스템(KMS)으로 회사 내 암호화 키를 관리하면서 암호화 키 외부 반출 시 보안USB 등을 사용하여 전달하고 있으며,

SSL(Secure Socket Layer) 인증서 키는 접근이 제한된 공유폴더에 보관하고 있어 필요시 동 공유폴더에 대한 접근을 신청하여 인증서 키에 대한 접근권한을 부여·관리하고 있다.

그러나 은행은 암호화 키의 외부 반출, 암호화 키 분실 시 재발급 절차 등의 상세절차를 마련하지 않아 암호화 키 분실 등의 사고로 이어질 우려가 있고

SSL 인증서 키가 보관된 공유폴더에 접근권한을 신청하는 경우 관련 담당자의 검토 등 확인 절차를 마련하지 않아 부적절한 권한으로 접근이 이루어지는 경우 동 인증서 키가 변경되거나 삭제될 우려가 있다.

<조치할 사항>

따라서 은행은 암호화 키 반출 및 재발급 등 구체적인 운영 절차를 보완하여 내규를 개정하고 인증서 키 사용 절차 및 사용 이력의 적절성 검증 절차를

마련하는 등 암호화 키 통제절차를 강화하시기 바랍니다.

(35) 업무보고서 보고의무 강화

은행은「은행업 감독업무 시행세칙」제99조 등에 따라 업무보고서 보고, 본점 검사 관련 보고 등의 감독기관 보고의무를 이행하고 있다.

그러나 은행은 '기업대출금 업종별 연체채권 현황' 보고서 등의 업무보고서를 지연 제출하는 등 업무보고서 취합 체계 및 검토 절차에 미흡한 점이 있다.

<조치할 사항>

은행은 앞으로 감독기관 보고의무 사항이 제출기한 내에 정확하게 이행될 수 있도록 관련 업무절차를 보완하고 내부통제를 강화하시기 바랍니다.