경영유의사항 등 공개안

1. 금융회사명 : 중소기업은행

2. 조치일 : 2022. 3. 2.

3. 조치내용

대상	내용
기관	○ 경영유의사항 14건 ○ 개선사항 30건

※ 경영유의사항 및 개선사항은 금융회사의 주의 또는 자율적 개선을 요구하는 행정지도적 성격의 조치임

4. 조치대상사실

가. 경영유의사항

1) 여신감리 결과 사후관리 강화

□ 신용감리 대상 여신에 대하여 감리를 실시하여 감리등급을 부여하고 채권보전강화, 추가여신 취급 억제, 대출금 상환유도 등 조치사항이 있는 경우 이행기한을 부여한 뒤, 연 x회 이상 조치사항 이행여부를 점검하고 있으나,

조치사항 이행기한을 일괄적으로 다음 분기말일로 부여하고 있어 기한 내 이행완료가 어려운 경우가 대부분이며, 심사역이 조치사항 이행여부를 점검할 때에도 이행 및 미이행 여부를 구체적으로 확인하지 않고 형식적으로 의견을 입력하는 등 감리결과 조치

사항에 대한 사후관리가 미흡하여 조치사항이 장기간 이행 완료되지 않고 있는 사례가 다수 존재하므로

감리결과 감리등급 별로 조치사항에 대한 이행기한을 차주의 영업상황, 상환능력, 신용위험 등을 고려하여 개별 부여하는 한편, 이행여부 점검시 이행 및 미이행 여부를 명확히 확인하여 기록·유지하고, 감리결과 조치사항에 대한 이행현황을 주기적으로 경영진에게 보고하는 등 감리결과에 대한 사후관리를 강화할 필요가 있음

2) 조기경보등급 상향조정 승인절차 강화

□ 기업차주의 신용위험을 조기경보시스템을 통해 점검하고, 부실징후의 정도에 따라 5단계로 분류하여 '예비주의' 이하 기업차주에 대해서는 신용등급 하향, 대손충당금 추가적립 등 중점 관리하고,

* 정상, 관찰, 예비주의, 주의, 경보 5단계로 구분하여 이상징후 기업차주를 관리

조기경보기업의 조기경보 분류단계(예비주의, 주의, 경보) 중 '주의', '경보' 기업의 분류단계 상향(주의·경보→예비주의)은 조기경보시스템을 통해 △△△△부의 승인을 받도록 하고 있으나, '예비주의' 기업의 분류단계 상향(예비주의→관찰·정상)은 영업점의 부·점장 전결로 결정토록 하고 있어 '예비주의' 기업의 분류단계 상향 조정이 부·점의 자의적 판단으로 이루어질 우려가 있고,

부실징후가 보다 높은 '주의', '경보' 기업에 대한 분류단계 상향도 △△△△부의 승인만으로 처리되고 있어 관대하게 상향될 소지가 있으므로

조기경보 단계상 '예비주의' 기업의 분류단계를 상향할 때에도 본부 △△△△부의 승인을 받고, '주의', '경보' 단계를 상향할 때

에는 △△△△부 승인뿐만 아니라 ▽▽▽▽부 등 독립된 부서의 승인을 받도록 하는 등 조기경보등급 상향 승인절차를 강화할 필요가 있음

3) 여신 승인조건 부여 및 이행여부 관리 강화

□ 본부 △△△△부에서 승인한 여신 중 신규 건축을 위한 시설자금 대출의 경우 담보후취에 대한 승인조건을 개별 심사역 판단 하에 사안에 따라 달리 부여하고 있으며,

준공완료 후 담보 미취득 등 승인조건을 x년 이상 이행하지 못하고 있는 사례가 있는데도, 승인조건 미이행시 이행을 위한 적극적인 조치 없이 영업점에서 그 사유를 보고받아 영업점 운영리스크 평가시 변별력 없이 반영할 수 있을 뿐 기한의 이익 상실 등 적극적인 조치를 취하지 않는 것에 대해 본부 △△△△부에서 승인조건 이행을 촉구하는데 어려움이 있으므로

앞으로 신규 건축을 위한 시설자금대출 승인시 시설물 완공 후 담보취득 승인조건이 자동부여 되도록 조치하고, 승인조건 장기 미이행 건에 대하여는 운영리스크 평가에 변별력 있게 반영되도록 하는 등 여신 승인조건 이행여부 관리체계를 강화할 필요가 있음

4) 이사회 내 위원회 운영 강화

□ 은행「정관」제31조(의사록)에 따르면 이사회 의사 운영과 관련하여 안건, 경과요령 및 그 결과, 반대하는 자와 그 반대이유를 의사록에 기재하고 출석한 이사가 이에 기명날인 또는 서명하도록 규정하면서, 이사회 내 위원회에 대해서도 이를 준용하여 운영하도록 하고 있으나

이사회 내 위원회(AA위원회, BB위원회 및 CC위원회)가 서면 결의하는 경우도 있어*, 중요사안에 대해 충분한 토의·심의가 없이 형식적으로 이루어질 우려가 있고,

* 은행의 「지배구조 내부규범」에 의하면 보고·토의를 요하지 아니하거나 긴급한 경우에만 서면결의가 가능하나, 20xx~20xx년 기간 중 AA위원회가 전부 서면결의로 운영된 사례가 있음

「금융회사의지배구조에관한법률」에 따라 이사회가 사외이사가 아닌 자를 이사회 의장으로 선임하는 경우에는 선임사외이사를 두어야 하는 다른 금융회사와 달리 중소기업은행은 「중소기업은행법」에 따라 은행장이 이사회 의장이 되는 관계로 사외이사의 효율적 업무수행 및 책임성 제고가 저해될 우려가 있으므로

중요사안에 대한 충분한 심의가 이루어지도록 이사회 내 위원회를 가급적 대면회의방식으로 운영하고 이사회 및 이사회 내 위원회에서 사외이사의 효율적 업무수행 및 책임성 강화를 위해 은행의 주요사안 의사결정에 필요한 정보를 사외이사에게 신속하고 충분하게 제공할 필요가 있음

5) 금융투자상품 불완전판매 방지를 위한 내부통제 강화

□ 「금융회사의지배구조에관한법률」 제24조 등에 따른 새로운 금융상품 개발 및 판매 과정에서 금융소비자 보호 및 시장질서 유지 등을 위하여 준수하여야 할 업무절차에 관한 사항을 포함하여 내부통제기준을 마련하여야 하고,

「자본시장과금융투자에관한법률」(이하 "「자본시장법」") 제46조, 제46조의2, 제47조 및 제71조 등에 의하면 금융투자업자는 일반

투자자에게 금융투자상품 판매시 적합성원칙, 적정성원칙, 설명의무, 투자권유자문인력이 아닌 자에 의한 투자권유 금지 및 녹취대상 상품에 대한 판매과정 녹취의무 등을 준수하여야 하나,

금융투자상품 심사·선정, 판매 및 사후관리 체계가 전반적으로 미흡한 수준이므로 금융투자상품의 불완전판매 방지를 위한 실효성 있는 내부통제 기준 및 내부통제시스템을 마련할 필요가 있음

㈎ 상품 심사 및 선정 단계

○ 사모펀드 및 신탁상품 심사·선정 기준을 은행 내부에서 계속적 구속력을 갖는 규범인 내규로 마련하지 아니하고 소관 부서에서 일반문서* 형태로 운영하고 있어 사모펀드 및 신탁 상품 심사 및 선정 절차가 형식적으로 이루어지고

* (▼▼▼▼부) PB전용상품 선정 및 사후관리 협의회 운영기준
(▲▲부) 신탁 상품선정 협의회 운영기준

사모펀드 및 신탁 상품의 상품선정위원회 구성이 소관부서의 실무자 위주로 구성되어 있고 사모펀드의 경우 투자대상자산 평가 기준도 유형별로 세분화 되어 있지 않아 상품 심사가 자의적으로 이루어질 우려가 있으며,

신상품 도입시 리스크 사전검토 대상을 일부 상품으로 한정*하여 운영하거나 법규준수 측면의 사전검토 실시 기준이 명확하지 않아 고위험 상품임에도 불구하고 상품 도입시 해당 신상품에 대한 투자위험을 사전에 인지하지 못할 소지가 있으므로

* 특정금전신탁의 경우 투자위험등급 1~3등급의 상품만을 리스크 사전검토 대상으로 정하고 있어 '⊗⊗⊗⊗신탁'의 경우 1등급 상품이 xx% 포함된 고위험 상품임에도 위험등급 4등급으로 분류되어 사전검토를 생략함에 따라 리스크를 사전에 인지하지 못함

상품 심사 및 선정 기준을 내규에 반영하고, 실무자가 아닌 그룹장을 위원장으로 하는 상품선정위원회를 구성하여 평가위원을 다양화*하며, 고위험상품의 경우 투자대상자산의 유형별**로 세부 평가기준을 마련하여 투자위험에 대한 심사를 강화할 필요가 있음

* 영업점, ◁◁◁◁◁부, ◀◀◀◀◀부, ☆☆☆☆부 및 외부전문가 등에서 선정

** 파생결합증권, 부동산, 특별자산(금속, 원자재, 인프라, P2P대출채권 등) 등

또한 은행연합회 「은행 비예금상품 내부통제 모범규준(2020.9.28. 제정)」에서 정한 기준에 따라 신상품 도입시 리스크 검토대상*을 확대하고

* 위험등급 1~3등급, 사모펀드, 고난도 금융투자상품, 해외 대체펀드 등

상품선정위원회 부의 안건에 소비자영향 분석결과 및 법규준수 사전검토 결과가 반영되도록 상품 심사 및 선정 관련 사전검토 절차를 개선할 필요가 있음

㈏ 상품 판매 단계

○ WM센터에서만 판매 가능한 투자위험이 높은 “PB전용상품_☆☆☆☆☆”을 일반영업점과 연계하여 판매하면서 금융소비자 보호를 위한 별도의 판매기준을 마련하지 않아 다수의 영업점에서 불완전판매가 발생*하였으며

* 20xx.x.x.~20xx.x.x. 기간 중 xx개 영업점에서 총 xxx건을 판매하는 과정에서 적합성 원칙을 위반

상품 가입 과정에서 투자자성향 분석*, 상품설명 녹취**, 상품가입 원본서류 전산 사후등록***등의 기본적인 검증절차에 대한 전산 통제 소홀로 인해 불완전 판매가 발생한 사례가 있음

* 투자자성향분석 원본서류가 없음에도 전산에 입력된 투자자성향을 그대로 활용

** 상품설명 녹취대상 상품인 경우 실제 녹취가 이루어지지 않았음에도 상품 가입이 가능

*** 상품가입 원본서류를 가입 절차 진행 후 일괄 스캔하여 ★★★시스템에 사후등록

또한 투자권유자문인력이 아닌 자에 의한 투자권유를 통제하는 장치가 미비하여 투자권유자격이 없는 직원이 상품 가입서류에 투자권유한 직원으로 기재하고 실제 투자권유를 할 수 있으며

복합점포 내에서 은행과 계열회사가 상품명 및 투자구조가 유사한 상품을 판매하면서 고객이 판매사 정보를 혼돈하여 민원이 발생한 사례가 있으므로

○ PB인력이 있는 WM센터에서만 판매 가능하도록 정한 “PB전용상품_☆☆☆☆☆” 판매시 일반영업점에서 투자권유 및 상품설명이 이루어지지 않도록 제한하고, 고객이 WM센터에 내방한 경우에만 판매 가능하도록 상품 판매 기준 및 통제 절차를 마련하며

영업점에 전자식 가입신청서를 도입하여 전산 오조작에 의한 불완전판매 가능성을 차단하며 상품 판매 전 투자권유 직원의 자격요건 충족여부를 자동 검증하여 미충족시 판매 절차를 통제할 수 있도록 투자권유 직원 정보를 전산시스템으로 관리하고

복합점포 내에서 고객의 판매사 관련 혼란이 발생하지 않도록 상품 판매사에 대한 설명 및 고객 확인 절차를 마련할 필요가 있음

㈐ 상품 사후관리 단계

○ 상품 사후관리 기준이 부재하여 동일 상품을 회차별로 계속적으로 판매하는 경우 이전 회차의 판매분에 대해 부실 발생 여부 모니터링 등 사후관리를 하여 다음 회차 상품 판매 결정시 반영하는 등의 적절한 사후관리가 이루어지지 못하고 있어 상품의 투자구조·투자대상자산 등에 리스크가 내재되어 있음에도 적절한 조치*를 취하지 못하고

* 상품판매 중단 및 판매 한도조절 등

파생결합증권펀드(DLF)·파생결합증권신탁(DLT) 등 시장가격에 연동된 파생결합상품에 대한 조기경보체계가 부재하며 주가연계신탁(ELT)의 경우 조기경보체계가 문서화되어 운영되지 않아 고객 알림서비스가 실효성 있게 운영되지 않을 소지가 있으므로

○ 투자대상자산·상품 유형별 사후관리 기준을 마련하고 기존에 판매된 상품의 리스크를 주기적으로 평가하여 리스크 수준에 따라 필요한 조치*를 취할 수 있도록 사후관리 기준을 내규로 마련·운영하고

* 투자자에게 통지, 상품판매 중단 및 판매 한도조절 등

파생결합증권펀드(DLF)·파생결합증권신탁(DLT)·주가연계신탁(ELT)의조기경보체계를 문서화하여 운영함으로써 사후관리가 체계적으로 실시되도록 개선할 필요가 있음

6) 금융사고 사전인지 및 감사 기능 강화

□ 내규「내부통제규정」제29조에 의하면 은행은「은행법」제34조의3 등에 따라 금융사고 예방대책을 마련하여야 하고,

내규「감사직무규정」제8조에 따라 ▷▷부는 영업점의 일상거래중 사고취약거래 및 오류발생 개연성이 큰 특정거래에 대한 그 처리의 적정 여부 등에 대하여 상시감사를 실시하고 있으나,

○ 검사종료일 현재 ▷▷부에서 운영중인 "☆☆시스템"의 상시감사지표(xxx개) 중 임직원의 금융사고를 모니터링하기 위한 특이거래지표 xx개*의 경우 금융사고 의심거래 추출기준의 유효성이 낮아 새로운 패턴의 금융사고를 체계적으로 분석하여 식별하는데 한계가 있으므로

* xx개는 사고 모니터링을 위한 "특이거래지표"로 운영하고 있으나 사고 의심거래 추출기준이 단순히 일정 기준 초과시 의심거래로 분류하는 방식으로 운영되고 있어 사고발생 원인을 체계적으로 분석하여 사고 개연성이 있는 거래를 추출하는 데는 한계

금융사고 유형별(횡령·유용 등)로 사고 개연성이 있는 의심거래를 종합적으로 분석(거래종류, 발생빈도, 발생기간 등) 가능한 상시감사지표 및 지표별 사고위험 수준(고·중·저)을 판별 가능한 위험판별 모형을 개발하는 등 ☆☆시스템을 고도화 하고,

☆☆시스템에서 판정한 위험수준에 따라 감사운영 방식을 차등화(고위험 의심거래에 대한 현장감사 강화 등)하는 방안을 마련할 필요가 있음

7) 불건전·불공정 영업행위에 대한 통제절차 강화

□ 내규「내부통제규정」제26조 및 제28조 제1항에 의하면 은행은 은행의 건전한 운영 및 신용질서를 저해하는 불건전·불공정 영업행위를 하여서는 아니 되고,

내규「여신업무 취급세칙」제7조에 의하면 우월적 지위를 이용하여 고객의 권익을 부당하게 침해하거나 건전한 금융거래질서를 저해하는 행위를 하여서는 아니 되며,

동 세칙 제243조 제2항 등에 의하면 여신거래시 연대보증 설정한도는 신용취급금액의 xxx%로 정하고 있는데도

이번 검사기간 중 불건전·불공정 여신취급 실태를 점검한 결과 다음과 같은 문제점이 확인됨에 따라 이에 대한 개선방안을 마련할 필요가 있음

㈎ 여신취급시 연대보증 부당 운용 관련

○ 2016.11.7.~2020.4.29. 기간 중 ☏☏☏☏지점 585개 영업점에서 9,593개 법인거래처의 총 12,151개 계좌에 대해 x조 x,xxx억원의 여신을 취급하면서 은행 내규에서 정한 연대보증 설정한도(신용취급금액의 xxx% 이내)를 초과하여 연대보증을 부당하게 운용한 사실이 있으며

그 결과 은행 내규상 정한 연대보증 한도를 초과하는 보증채무 정보(신용거래정보)가 한국신용정보원에 집중*되어 연대보증인의 신용평가 정보로 활용될 경우 금융거래에 불이익이 발생할 소지가 있으므로

* 한국신용정보원에 집중되는 개인채무보증정보 등록금액(연대보증)은 주채무자의 대출원금을 한도로 함(「일반신용정보관리규약」 <별표1> 신용정보관리기준 5) 개인채무보증정보, <일반신용정보관리규약 실무해설> 4. 개인채무보증정보

일부담보대출에 대해 입보된 연대보증인의 경우 기한연장시 연대보증금액을 내규에서 정한 연대보증 설정한도(신용취급금액의 xxx% 이내) 이내로 감액하는 한편, 기한연장 및 조건변경 등 여신거래시 연대보증금액을 내규에서 정한 연대보증 설정한도를 초과하여 운용하지 않도록 관련 업무절차를 개선하고 전산시스템에 대한 통제를 강화할 필요가 있음

㈏ 임직원의 가족 및 가족 관계법인 대출 정당성 심사 강화

○ 2020.8월말 기준 임직원의 가족대출은 14,015건, x,xxx억원이고, 이중 여신 취급시 이해상충 발생 가능성이 높은 임직원의 가족* 또는 가족 관계법인** 에 대한 셀프대출***은 전체 가족대출의 13.2% (1,856건, x,xxx억원(금액기준 xx.x%)) 비중을 차지하는 수준이나,

* 「임직원에 대한 대출규정」 제31조의2 제1호에 의하면 “가족”의 범위는 배우자, 본인·배우자의 직계존속·직계비속 및 본인·배우자의 형제자매를 의미

** 「임직원에 대한 대출규정」 제31조의2 제2호에 의하면 “임직원 가족 관련 기업”이란 임직원 또는 임직원의 가족이 대표자인 법인, 개인사업자, 법인격 없는 조합 및 단체를 의미

*** 「임직원에 대한 대출규정」 제31조의3에 의하면 임직원은 본인, 그 가족 또는 가족 관계 법인에 대한 여신취급 의사결정에 관여할 수 없음

이번 검사대상 기간 중 여신 취급시 임직원의 가족대출 및 가족 관련 셀프대출에 대한 사전 통제 및 검증 절차 부재로 ♨♨♨♨♨♨ 등 7개 영업점에서 14개 차주(40개 계좌)에 대해 시설자금을 취급하면서 여신관련 서류 임의작성*, 담보가치 과대평가** 및 대출한도 과다산정*** 등의 부당대출 취급 사례가 발생하였으므로

* 가족 관계법인의 여신거래약정서, 근저당권설정계약서 등의 서류를 임의 작성

** 담보물 시가조사시 선순위보증금 누락, 선순위 설정액 오류 차감 등 담보가치 과대 운용

*** 소요시설자금 산정시 매매계약금액에서 기 지급된 금액(계약금 등) 미차감

담보가치 과대평가, 대출한도 과다산정 등 이해상충 발생 가능성이 있는 임직원 셀프대출 등 의심거래에 대해 은행이 사전 인지할 수 있도록 '영업점 자점감사 상시감시지표'를 개발하고, 의심거래에 해당될 소지가 있는 경우 '임직원 가족 관련 대출취급 점검표'에 따라 점검하며 그 점검결과를 전산 등록·관리하는 등 임직원 셀프대출에 대한 사전심사를 강화할 필요가 있음

8) 국내외 본점·지점의 자금세탁방지업무 내부통제 강화

□ 내규「자금세탁방지업무 취급규정」제26조 및「자금세탁방지업무 취급지침」제56조 제1항 등에 따른 고액현금거래 보고(CTR), 의심거래 보고(STR), 고객확인(CDD) 등의 업무 수행과 관련하여, 다음과 같은 문제점이 확인되므로 이에 대한 개선방안을 마련할 필요가 있음

㈎ 고액현금거래(CTR) 보고대상 제외사유 관련

○ 고액현금거래 보고대상 제외사유를 '고객요청'과 '전산조작 오류'에 의한 현금처리 등 2개만으로 운영하고 있어 고액현금거래 보고(CTR) 대상 거래임에도 영업점 직원의 주관적 판단에 따라 고액현금거래 보고가 누락될 가능성이 있으므로

고액현금거래(CTR) 보고대상 제외사유에 대한 세부적용 기준을 마련하여 전산코드로 관리하고, 제외사유를 추가하는 경우에는

본부부서로부터 사전 승인을 거치도록 관련 업무절차 및 전산시스템을 개선하는 등 고액현금거래 보고 누락 방지 방안을 마련할 필요가 있음

㈏ 의심거래 보고(STR) 관련

○ 2016.11.5.~2020.10.31. 기간 중 의심거래 보고(STR) 추출기준(Rule)별 의심거래 보고(STR) 보고율 50% 미만이 전체 대비 84%(10,341건)를 차지하고 금융정보분석원의 '자금세탁방지(AML) 제도이행 종합평가' 중 중소기업은행의 의심거래 보고(STR) 충실도 점수*도 낮은 수준이므로

* 2019년 중소기업은행 x.xx점/x점 만점(시중은행 평균 x.xx점)

의심거래 보고(STR) 추출기준의 유효성(정보건수, STR 보고율 등) 분석을 통해 개별 추출기준의 자금세탁 위험도를 고위험·중위험·저위험으로 분류하고, 고위험 의심거래의 경우 원칙적으로 본부부서에서 사전심사를 강화할 필요가 있음

㈐ 개인 고객확인의무(CDD) 관련

○ 가족대리인이 자녀 명의로 신규계좌 개설시 차명거래* 등의 우려가 있음에도 고객확인을 생략하고 있어 개인 고객확인의무를 소홀히 할 우려가 있으므로

* (예시) 비과세 증여한도 초과로 부과되는 증여세를 회피하기 위한 차명거래 등

가족대리인의 신청에 따른 계좌 개설시 비과세증여한도를 초과하는 거래 등 차명거래가 의심되는 경우에는 반드시 고객확인의무를 이행하도록 절차를 개선하는 등의 통제 수단을 마련할 필요가 있음

㈑ 법인·단체 고객의 실제소유자 확인절차 관련

○ 법인·단체 고객의 실제소유자 확인을 위한 전산등록 화면이 실제 소유자 판단기준 해당여부를 순서에 따라 단계적으로 확인하도록 구현되어 있지 않고, 영업점 직원이 임의로 특정단계를 직접 선택할 수 있도록 구성되어 있어 실제소유자 확인을 소홀히 할 우려가 있으므로

법인·단체 고객의 실제소유자 전산등록시 실제 소유자 해당 여부 확인업무가 「특정금융정보법」에서 정한 기준에 따라 단계적으로 이루어지도록 전산시스템을 개선하는 등 통제 수단을 마련할 필요가 있음

㈒ 중계무역 등 영위기업에 대한 위험관리체계 관련

○ 법인의 고객확인은 「특정금융정보법」에 따라 대표자·실제소유자 정보를 확인하고 있으나, 은행 특성상 수출입·중계무역업 등을 영위하는 법인이 많아 해외 금융감독당국 금융제재 대상과의 거래 등의 위험에 노출될 가능성이 높으므로

금융제재 위반 가능성이 높은 고위험 업종(수출입·중계무역업 등) 영위기업의 경우 고객확인 단계에서 「특정금융정보법」에서 확인하도록 명시되어 있지 않더라도 등기임원 등 관련인 정보를 추가로 수집·분석·평가하고 위험도에 따라 사전심사를 차등화할 필요가 있음

㈐ 국외지점의 자금세탁방지 성과평가 및 내부통제 관련

○ 국외지점의 법규준수부문 경영평가와 현지 준법감시인에 대한 성과평가 기준이 대부분 정성적 요소로 구성되어 객관성이 낮고, 국외지점의 내부통제 활동에 대한 현지 준법감시인의 위험평가 및 보고 적정 여부를 종합적으로 모니터링 할 수 있는 점검체계가 없어 국외지점의 내부통제 위험에 대한 효과적인 대응이 어려우므로

국외지점의 성과평가 기준을 합리적으로 개선하고, 국외지점의 내부통제 위험평가 결과 도출된 이상거래를 본점 차원에서 종합적으로 모니터링이 가능한 점검체계를 구축할 필요가 있음

9) 개인신용정보 보호 및 관리 기능 강화

□ 「신용정보의이용및보호에관한 법률」 제15조(수집·조사 및 처리의 원칙) 등에 의하면 개인신용정보의 수집·제공·활용시 신용정보주체의 동의를 받아야 하고 동법 제18조 제1항에 의하면 신용정보의 정확성 및 최신성을 유지해야 하며

동법 제20조의2 제2항에 의하면 상거래가 종료된 날로부터 최장 5년 이내에 개인신용정보를 삭제해야하고, 동법 제32조 제7항에 의하면 개인신용정보를 타인에게 제공하려는 자 또는 제공받은 자는 개인신용정보의 제공사실 및 이유 등을 사전에 해당 신용정보주체에게 알려야 하는데도,

개인신용정보의 수집과 관련하여 2018.10.8.~2019.7.11. 기간 중 '☒☒☒☒☒펀드' 및 '⊗⊗⊗⊗신탁' 상품 투자자에 대한 '개인신용정보 수집 및 이용 동의서'를 점검한 결과, 고객이 작성한 동의서가

없음에도 전산에는 마케팅 수신에 동의한 것으로 잘못 등록된 사례가 확인되었고

개인신용정보 이용 관련하여 공동관리고객 제도*의 경우 일반 영업점 VIP 고객의 수신 만기도래 정보를 고객정보관리시스템(CRM)에서 파일로 일괄 내려받아 은행과 증권사가 동일한 공간에서 업무를 수행하는 복합점포(WM센터)에 공유하고 있어 고객의 개인신용정보가 무단 출력 등에 따른 외부유출 및 개인신용정보 수집 목적 외로 이용될 가능성이 있고

* WM센터와 일반영업점간 연계영업 강화를 위해 일반영업점의 VIP 고객을 WM센터에 소개하여 WM센터에서 PB 상품을 가입할 경우 그 실적을 각각 100% 인정해 주는 제도

개인신용정보 제공 관련하여 보건복지부 등 외부기관에 개인신용정보가 포함된 금융거래정보를 제공하는 과정에서 업무처리 시스템 설계상 오류로 인하여 담당직원이 금융거래정보 제공 사실에 대한 고객 통지를 지연하거나 누락한 사례가 발생하였고

개인신용정보 집중 관련하여 개인의 채무보증정보를 한국신용정보원에 집중하는 과정에서 신용금액이 감소한 경우 보증채무금액을 축소해야 하는데도 연대보증 설정한도에 대한 전산통제를 실시하지 않아 감액된 주채무 금액보다 큰 보증채무금액 정보가 한국신용정보원에 집중되고 있어 고객의 금융거래에 불이익이 발생할 소지가 있으며

개인신용정보 삭제 관련하여 은행연합회의 은행권 공통 기준에 따라 금융거래가 종료된 고객의 개인신용정보는 단계별*로 삭제하고 있으나, 관련 세부사항이 내규에 반영되어 있지 않아 개인신용정보 삭제 업무를 소홀히 할 소지가 있음

* 1단계(3개월) : 선택적 파기, 2단계(5년) : 원칙적 파기, 3단계(10년) : 영구적 파기

따라서, 개인신용정보 처리 단계(수집·이용·제공·집중·삭제)에서 확인된 취약점에 대한 업무절차 및 시스템을 개선하고, 개인신용정보 보호 및 점검 업무에 대한 컨트롤 타워 기능을 강화하며

은행 내 모든 전산자원(업무용 PC, 업무시스템, 인터넷 등)에 대하여 개인신용정보의 보관, 반출 및 불필요한 접근통제 등에 대한 내부통제 기준을 정비하고 정기 점검을 실시하고

개인신용정보가 많이 포함되어 있거나 개인·신용정보 이용 빈도가 높은 업무처리 시스템에 대한 모니터링 기능을 강화하며

개인신용정보의 파기 대상정보, 파기절차, 파기방법 및 보관대상 정보 등에 관한 세부사항을 관련 내규에 반영할 필요가 있음

10) 리스크관리와 여신운영 업무간 상호견제 강화

□ 내규「내부통제규정」제4조에 의하면 은행은 업무의 종류 및 성격, 이해상충의 정도 등을 감안하여 직무 간 상호 견제와 균형이 이루어질 수 있도록 업무분장 및 조직구조를 수립하여야 하고,

내규「리스크관리규정」제5조에 의하면 리스크관리 조직은 원칙적으로 영업부문과 독립적으로 운영되어야 하는데도

여신운영업무 총괄부서인 '▶▶▶▶부'에서 조기경보시스템 운영, 재무이상치 분석 업무를 수행하는 과정에서 조기경보모형 및 재무이상치 추출기준에 대한 리스크 검증 기능이 없어 부실징후 여신에 대한 사전적·사후적 리스크관리 업무를 소홀히 할 가능성이 있으며,

▶▶▶▶부에서 대출사기방지시스템을 운영하면서 대출사기 의심거래에 대한 내부통제 조직간 정보공유 체계가 없어 금융사고 발생시 신속한 대응이 어려운 측면이 있고,

기업신용평가시스템에서 평가한 모형등급에 대한 신용등급 조정(Override) 기준을 여신심사 조직인 '△△△△부'에서 관리하고 있어 신용등급조정 기준을 관대하게 운영할 소지가 있으므로

조기경보시스템 관리 및 여신감리 등 리스크관리 업무를 영업부문과 독립적으로 운영하여 이해상충을 방지하고, 사전적 건전성 관리를 위하여 조기경보모형, 재무이상치 및 신용등급 조정(Override) 기준 등에 대한 리스크관리 조직의 적합성 검증을 강화할 필요가 있으며, 내부통제 조직에서 대출사기방지시스템을 내부통제 감시체계와 연계하여 분석하는 등 모니터링 기능을 강화할 필요가 있음

11) IT자체감사 강화방안 마련

□ 은행 IT업무는 CIO가 통할하는 ♤♤그룹과 CISO가 통할하는 정보보호최고책임자(조직)로 구분 편제되어 있고, ♤♤그룹은 그룹장 직할의 ♠♠♠♠♠♠팀이, ♡♡♡♡부는 ♡♡♡♡부 소속 ♥♥♥♥♥♥팀이 자체감사업무를 각각 수행하고 있으나,

♤♤그룹은 ♠♠♠♠♠♠팀이 자체감사업무 외에도 테스트지원 시스템 운영, 국가기반시설 위기관리, IT상담센터 관리 등 감사대상 업무를 함께 수행하고 있고, IT업무나 감사업무 수행 경험이 없는 직원을 일일감사자로 배치하였으며, 전산원장 변경 건에 대해서는 ♠♠♠♠♠♠팀이 정당성 여부를 확인하지 않고 있고,

감사대상 업무를 수행하는 ♧♧♧♧부장이 자체감사자 업무 성과에 대한 평가를 하고 있으며,

정보보호최고책임자(조직)는 자체감사업무 담당자가 부서 총괄 기획업무를 함께 수행하고 있고, 월별감사 및 기별감사는 정보보호 업무 실무를 담당하는 책임자가 업무를 수행하고 있으며, 자체감사 업무에 대한 보고통제 및 자체감사자에 대한 업무성과 평가에 감사대상 업무를 수행하는 소속 팀장 및 ♡♡♡♡부장을 포함토록 하고 있는 등 IT자체감사 업무체계가 미흡하므로,

IT자체감사 조직 및 담당자가 감사대상 업무를 함께 수행하지 않도록 조치하고, 전문성 있는 적임자를 자체감사자로 배치하며, 전산원장 변경에 대해 ♠♠♠♠♠♠팀의 확인 절차를 추가하고, 자체감사업무에 대해서는 CIO 및 CISO가 직접 통제하며, 자체감사자에 대한 업무성과평가시 감사대상 업무 수행조직의 부서장 등은 평가자에서 제외하는 등 자체감사업무의 전문성 및 독립성을 강화하시기 바람

12) 정보처리시스템 운영·관리 및 IT통제 전문성 강화

□ 은행「업무분장규정」등에 따라, 계정계 시스템 등 주요 정보처리시스템의 운영 및 보안통제 업무를 IT전담 조직인 ♤♤그룹 및 ♡♡♡♡부에서 수행하고 있고, 동 조직으로 하여금 정보처리 업무의 외부주문에 대해 자체적으로 통제가 가능하도록 통제기준을 마련하여 운영하고 있으며, 이에 대한 규정 준수 및 적정성 등에 대해 정기적으로 감사활동을 실시하여 통제하고 있으나,

○○○○○○○시스템 등 22개 단위업무시스템을 IT전담조직이 아닌 동 단위업무의 소관부서에서 운영하면서 아래와 같이 불합리한

점이 있으므로 조직업무 분장 및 관리인력을 조정하는 등 정보처리시스템 운영·관리 업무를 재검토하고 관련 IT통제를 강화하시기 바람

㈎ ♧♧♧♧부는 은행 내 시스템 운영 및 프로그램 관리, IT업무위탁 관리를 총괄*하여야 하는데도 일부 소관부서에서 직접 운영·관리하는 단위업무시스템 및 외주직원 등에 대한 체계적인 관리가 미흡하므로 관리통제를 강화할 필요가 있음

* 「업무분장규정」 제62조(♧♧♧♧부)

㈏ 일부 단위업무시스템의 경우, 은행 「업무분장규정」에 단위업무시스템 운영에 대한 명시적인 근거가 없음에도 별도의 타당성 검토없이 IT전담조직이 아닌 소관부서에서 단위업무시스템을 운영·관리하고 있어 단위업무시스템에 대한 기술적·관리적 통제가 소홀할 우려가 있으므로, 단위업무시스템 별도 운영에 대한 타당성을 검토하여 기술적·관리적 통제의 적정성 및 책임소재 등을 명확히 할 필요가 있음

㈐ IT전문성이 부족한 소관부서에서 동 단위업무시스템을 위탁 운영*하는 외주직원(▨▨▨시스템)의 관리 및 승인 등의 통제업무를 수행하고 있어, 전문적인 IT업무에 대해 적절히 통제되지 않을 우려가 있으므로 IT전담조직에서 시스템 운영 및 프로그램 관리를 수행하는 등 IT통제를 강화할 필요가 있음

㈑ IT전담조직이 아닌 단위업무를 담당하는 소관부서에서 일부 단위업무시스템을 운영·관리하면서 위와 같이 불합리하게 운영·관리되고 있으므로, 관련 업무 등에 대해 정기적으로 감사업무를 수행하는 등 IT통제를 강화할 필요가 있음

13) 체계적인 업무지속성 확보 대책 마련

□ 업무지속성을 확보하기 위해 업무별 중요도를 분석하여 핵심업무를 선정하는 경우 관계 부서간 협의 등을 통해 전사적 관점에서 판단해야 하는데도,

별도의 핵심업무 선정절차 없이 재해복구 대상업무 확대를 위해 업무영향분석(BIA)을 수행하고 동 분석결과 선정된 재해복구 대상이 익년도에 예산이 배정되어 재해복구시스템으로 구축된 경우에 한해서만 핵심업무로 분류하고 있는 등 핵심업무 선정절차가 다소 미흡하므로

현업부서 간 합의절차를 거친 업무영향분석(BIA)을 통해 대고객 업무를 포함한 핵심업무를 재정비하고, 매년 상기와 같은 절차를 거쳐 핵심업무를 조정하는 등 사전에 핵심업무가 정의·갱신될 수 있도록 하며, 동 핵심업무 조정 결과를 기반으로 업무지속성 확보방안을 마련·개선할 수 있도록 핵심업무 선정절차 및 업무지속성 수립방안을 마련하시기 바람

14) 대외 업무연속성 확보를 위한 통신망 구성 강화

□ 영업점 통신망은 장애·재해 등 비상상황시 업무 연속성을 유지하기 위해 통신회선 및 통신사업자를 이중화하고 주전산센터(◑◑◑◑센터) 및 재해복구센터(▨▨▨▨▨▨센터) 등으로 연결을 분산*하여 통신망을 구성하고 있으나,

* 통신회선 중 하나는 주전산센터로, 나머지 하나는 재해복구센터로 연결하고 두 개 회선 모두를 운용(active-active)하는 방식으로 사용하여 통신회선 장애시에도 유연한 대응 가능

핵심업무 관련 대외기관 xxx개 중 xx개(xx.x%) 기관과의 통신회선을 이중화하지 않고 단일회선으로 구성하여 통신장애시 신속한 복구에 어려움이 예상되고, 통신회선을 이중화한 대외기관 xx개 중 xx개(xx.x%)에 대해서만 재해복구센터로 회선을 분산 구성하고 나머지는 모두 주전산센터로만 연결되도록 구성하여 비상시 장애 전환(Fail-over) 효과가 떨어지므로

앞으로 핵심업무와 연관된 대외기관 통신회선에 대해 업무 영향을 분석하여 통신회선을 이중화하고, 주전산센터로 집중되어 있는 이중화된 통신회선을 재해복구센터로 분산 구성을 확대하는 등 대외 업무연속성 확보를 위한 통신망 구성을 강화할 필요가 있음

나. 개선사항

1) 사모펀드 수탁업무 관련 업무처리 절차 개선

□ 내규「수탁재산 보관·관리업무세칙」제9조 등에 의하면 사모펀드 수탁기관인 은행은 자산의 취득·처분 및 보관·관리 등에 대한 운용지시를 이행한 후 그 지시 내용이 법령, 집합투자규약 및 투자설명서 등을 위반하는지 확인하여야 하나,

사모펀드 수탁업무와 관련하여 집합투자업자의 운용지시 및 운용행위의 적정성 여부를 점검하기 위한 세부적인 기준 및 절차가 미흡하고, 집합투자업자의 운용지시를 전문(電文)이 아닌 이메일 등을 통해 전송받고 있으며, 운용지시의 이행(자금이체 및 수취 등) 및 관리 업무를 수기 방식으로 처리하고 있어 담당직원의 전산 오조작 등에 의한 사고 가능성이 있는 등 운용지시 관련 업무처리 절차에 미흡한 점이 있으므로

집합투자업자의 운용지시 등의 적정성 점검을 위한 세부적인 기준 및 절차를 마련하여 운영하고, 집합투자업자의 운용지시 내용은 예탁자산의 경우 한국예탁결제원을 통해 전문(電文)으로 수신하며 비예탁자산의 경우 보안이 강화된 전송수단을 통해 전송받아 확인하고, 운용지시 사항의 이행(자금이체 및 수취 등) 및 사후관리 과정에서 담당직원의 전산조작 오류 등이 발생하지 않도록 수탁 관련 업무처리 절차 및 시스템을 체계적으로 개선하시기 바람

2) 여신 취급시 대출금리 산정 및 검증기능 개선

□ 은행연합회의 「대출금리 체계의 합리성 제고를 위한 모범규준」 제3조에 의하면 대출금리는 합리적 기준에 따라 체계적으로 산정하여야 하고,

동 모범규준 제6조 및 제11조 등에 의하면 신용프리미엄은 경기변동 상황 등을 반영한 예상부도율(PD)과 부도시 손실률(LGD), 업종별 위험 등을 감안하여 주기적(연 1회 이상)으로 산출하고, 동 모범규준 제15조에 의하면 보증부대출의 보증부분에 대해서는 신용프리미엄과 자본비용은 부과하지 않아야 하며

내규 「내부목적 신용위험요소 관리기준」 제9조 및 제11조 등에 의하면 내부목적 신용위험요소(PD, LGD 등)는 매년 재산출하여야 하고, 신용위험요소의 변경 또는 유지에 관한 사항은 ALM위원회의 승인을 받아야 하며

내규 「신용관리비용 운용기준」 제4조에 의하면 신용위험비용 및 자본비용은 담보회수율이 100%일 경우 부과할 수 없으나

다음과 같이 여신 취급시 대출금리 산정 및 검증 절차에 문제점이 있으므로 개선방안을 마련하시기 바람

㈎ 전액 담보대출에 대한 신용프리미엄 가산금리 과다 부과

○ ◘◘◘◘지점 등 18개 영업점에서는 2016.12.2.~2019.9.27. 기간 중 총 18개 거래처(개인사업자 10개, 법인 8개)의 20개 계좌에 대하여 xxx억 xx백만원의 기업자금대출을 취급하면서 기한연장 신청(품의) 시점에 담보가치가 대출금액에 미치지 아니하여 일부 신용대출 부분이 있는 담보 대출에 대해 본부승인 조건에 따라 원금 일부를 상환함에 따라 담보금액이 대출약정 금액을 초과하는 전액담보로 변경되었음에도

대출약정 시점에 대출금리를 재산출하지 않고 대출실행을 위한 여신품의 시점에 일부 신용대출 부분이 있다는 전제로 산출한 대출금리를 그대로 적용하여 신용프리미엄 가산금리가 과다 부과되는 결과를 초래한바

담보(전액 담보 및 일부 담보)대출 취급시 여신신청(품의) 금액과 대출실행 금액의 차이로 인해 담보회수율이 변경될 경우 대출실행 전 금리 재산출을 통해 차주에게 신용프리미엄이 과다하게 부과되지 않도록 관련 업무절차 및 전산시스템을 개선하시기 바람

㈏ 보증부대출에 대한 신용프리미엄 가산금리 과다 부과

○ ◆◆◆지점 등 14개 영업점에서는 2017.4.13.~2019.12.27. 기간 중 총 14개 거래처(개인사업자 11개, 법인 3개)의 14개 계좌에 대하여 xx억 x,xxx만원의 보증부대출을 취급하면서

동 대출은 보증비율이 100%인 전액신용보증서 담보대출임에도 불구하고 영업점 직원이 담보등록 과정에서 실수로 신용보증서의 보증금액을 실제 보증금액보다 적게 입력하여 일부신용이 발생함에 따라 신용프리미엄 가산금리가 과다 부과되는 결과를 초래한바

보증부대출 취급시 영업점 직원의 전산조작 오류 등으로 인한 신용프리미엄이 과다 산출되지 않도록 보증부대출의 금리산정 절차 및 검증 기능을 체계적으로 개선하시기 바람

㈐ 대출금리 산출을 위한 신용위험요소 운영방식 불합리

○ 은행은 예상부도율(PD), 부도시 손실률(LGD) 등 금리산출에 활용되는 신용위험요소를 매년 산출하여 ALM위원회의 승인을 받고 있으나, 2020년도에는 신용위험요소를 산출하였음에도 실제 적용은 하지 않는 등 신용위험요소 운영과 관련하여 경기변동 상황 등을 제대로 반영하지 못할 우려가 있으므로

예상부도율(PD), 부도시 손실률(LGD), 신용회수율, 담보할인율 등 금리산출에 활용되는 신용위험요소는 경기변동 상황을 반영하여 정기적으로 산출·적용하고 ALM위원회의 승인을 받는 등 합리적으로 운영하시기 바람

3) 보증부대출 취급시 보증조건 등 검증체계 개선

□ 내규「여신업무 취급세칙」제286조 등에 의하면 신용보증기관의 신용보증서 담보대출 취급시 신용보증기금 등 신용보증기관이 부여한 보증조건 및 보증특약의 이행 여부를 확인하여야 하는데도

아래와 같이 신용보증서 보증조건을 적정하게 이행하지 않아 은행의 채권보전에 문제가 발생하거나 금융소비자의 피해가 발생할 위험이 있으므로

신용보증서 담보대출 취급시 보증조건 및 보증특약을 위반하는 사례가 발생하지 않도록 관련 업무처리절차 및 전산시스템을 체계적으로 정비하시기 바람

㈎ 신용보증서 보증만기와 대출만기의 불일치

○ 2018.3.7.～2020.4.23. 기간 중 ◘◘◘◘지점 등 13개 영업점에서 13개 법인에 대해 13개 계좌(총 xx억 x,xxx만원)의 신용보증서 담보대출을 취급하면서 한도거래 대출에 대한 대출만기와 보증만기의 일치 여부를 전산상 통제하지 않아 신용보증서 보증만기를 대출만기보다 짧게 적용함으로써 대출 만기시점에 차주의 부도 발생시 신용보증기관의 보증조건 미충족으로 인해 은행의 채권보전에 문제가 발생할 소지가 있고

㈏ 대출금 입금전용계좌 운용특약의 미이행

○ 2018.4.6.～2019.12.31. 기간 중 ◘◘◘지점 등 4개 영업점에서 4개 법인에 대하여 4개 계좌(총 xx억 x,xxx만원)의 신용보증서 담보대출을 취급하면서

보증특약에 따라 입출금전용계좌를 신설하여 대출을 실행하여야 함에도 신용보증기관에서 보증내역을 전문(電文) 형태로 전송하는 과정에서 대출금 입출금 전용계좌 운용 특약을 누락하였는데도

이를 은행에서 검증하지 않아 입출금 전용계좌가 아닌 일반 계좌로 대출을 실행하여 대출금의 용도외 유용 등이 발생할 경우 은행의 채권보전에 문제가 발생할 소지가 있으며

㈐ 대출금리 특약 조건의 미이행

○ 2016.10.19.~2019.11.22. 기간 중 ◎◎◎지점 등 3개 영업점에서 3개 법인에 대하여 3개 계좌(총 x,xxx만원)의 신용보증서 담보 대출을 취급하면서

영업점 직원의 부주의로 대출금리 특약조건으로 정한 금리상한을 초과하는 대출금리를 적용하여 대출이자(3계좌, 총 xxx,xxx원)를 부당 수취한 사례가 있음

4) 준법감시 조직 및 내부통제 통할기능 강화

□ 내규「내부통제규정」제7조 및 제9조 등에 의하면 은행장은 내부통제 환경조성·체계의 유효성 등을 재검토하여야 하고, 은행은 전문성을 갖춘 인력으로 구성된 지원조직을 갖추어 준법감시인의 직무수행을 지원하여야 하며,

준법감시인은 내부통제기준의 준수여부 점검 등 내부통제 업무를 총괄하여야 하고, 준법감시 활동을 효과적으로 수행하기 위한 준법감시체계(조직구조, 업무분장 및 승인절차, 의사소통·모니터링·정보시스템)를 마련하여 운영하도록 하고 있으나,

준법지원부 내 준법감시 업무를 수행하는 팀을 1개(x명)로 운영하고 있어 내부통제 업무를 총괄하여 수행하기에는 부족하고,

본부부서 내부통제 점검업무를 ▷▷부가 경영감사 측면에서 수행하고, 준법감시조직은 테마점검 위주로만 내부통제 점검업무를 수행하고 있어 내부통제 통합관리 기능 부재로 준법감시 사각지대가 발생할 우려가 있으며,

준법감시 업무수행을 위한 책임자급 실무인력(x명)이 부족*하고 주요 업무에 대한 내부통제·상시감시 모니터링 기능이 각 소관부서에 분산 운영되고 있어 영업점 및 본부부서의 업무처리과정에서 임직원의 위법·부당행위를 사전식별·분석·판별할 수 있는 통합 상시감시시스템이 부재하여 사고가능성이 높은 거래에 대한 적기 대응이 어려운 상황이므로

* 타 은행의 경우 내부통제·상시감시 담당 준법감시 조직의 책임자급 실무인력이 xx명 규모임

내부통제를 총괄 관리할 수 있는 조직을 신설하여 영업점 및 본부부서의 법규준수 여부 및 내부통제 측면의 잠재적 위험요인에 대한 통합 관리·감독 기능을 강화하고

영업점 및 본부부서의 수행업무에 대한 사전적·상시적 준법감시 업무가 원활히 수행되도록 책임자급 실무전문인력을 확대하며

각 소관부서에서 추출된 이상거래를 종합하여 고위험거래를 조기에 식별·분석·판별이 가능한 “고위험거래 판별모형” 및 “통합상시감시시스템”을 구축하고

통합상시감시시스템에서 추출된 고위험거래는 내부통제를 총괄 관리하는 조직에서 사전 점검을 거쳐 중대한 법규위반 사항에

대해서는 ▷▷부에 감사의뢰 하는 등 준법감시 업무와 검사 업무 간 연계체계를 구축하시기 바람

5) 영업점 및 본부부서간 중층적 상시감시 강화

□ 내규 「자점감사 운용기준」 제1조 내지 제3조에 의하면 은행은 영업점 및 본부부서의 사고 예방 및 자율적인 경영개선을 위해 사고발생의 취약점이 있는 분야에 대해 자점감사 항목을 마련하여 자체적으로 감사(이하 “자점감사”라 함)를 실시하고 있으나,

영업점 및 본부부서의 업무처리 과정에서 발생 가능한 고위험 거래*에 대한 사전적·상시적 자점감사 항목이 없고 준법감시인력 부족 등의 사유로 사후점검도 체계적 수행이 어려우므로

* 임직원 가족 및 가족 관계 법인에 대한 셀프대출, 부당한 담보·보증 요구, 가산금리 부당 수취 등

본부부서 및 영업점 업무처리 과정에서 발생할 수 있는 고위험 거래에 대한 자점감사 항목을 신설하고, 영업점에서 먼저 고위험 거래를 인지하여 자체 점검하고 내부통제 조직에서 추가 검증하는 중층적 상시감시체계를 구축하고

영업점 경영성과평가 중 ‘내부통제 감점항목’에 자점감사 이행 실적을 반영하여 자점감사 기능을 강화하시기 바람

6) 구속성 영업행위 관련 내부통제 절차 개선

□ 「은행법」 제52조의2, 제24조의5 및 「은행업감독규정」 제88조, 내규 「예금의 구속행위 관련 업무취급지침」 제2조 내지 제4조, 제8조,

제9조 등에 의하면 은행은 차주의 여신규모 및 신용도 등을 감안하여 구속행위에 해당되는지 여부를 정기적으로 점검하는 등 구속행위를 방지할 수 있는 내부통제절차를 마련·운영하여야 하나,

「은행법」에 따른 구속행위에 해당하지 아니하나 실질적으로 중소기업 관계인(대표이사, 임원, 직원 및 그 가족)의 의사에 반하는 구속성 행위에 해당될 소지가 있는 경우를 체계적으로 검증하고 통제할 수 있는 실효성 있는 내부통제 기준 및 절차가 미흡하므로

중소기업 차주 관계인에 대한 구속성 행위 의심거래 판별기준을 마련하고 여신 취급과정에서 중소기업 차주 관계인의 의사에 반하는 구속성 행위 의심거래 사전인지가 가능하도록 영업점 자점감사 항목을 개발하는 등 내부통제 점검 및 운영절차를 개선하시기 바람

7) 개인고객 환전거래 본인확인 프로세스 개선

□ 내규 「외국환업무 취급세칙」 제9조 및 제11조 등에 의하면 1백만원 이하에 상당하는 외국통화의 매입·매도에 해당하여 고객의 실명번호를 입력하지 않고 실명확인 생략이 가능한 경우를 제외하고는 「금융실명법」 등에서 인정하는 실명확인증표를 받아 외환거래에 대한 의사표시를 하는 본인인지 여부를 확인하여야 하나,

영업점에서 1백만원 이하에 상당하는 외국통화의 매입·매도에 해당하여 실명확인 생략이 가능한 거래임에도, 환전거래 실적으로 인정받기 위해 전산시스템상에 고객의 실명번호를 입력하면서 자칫 실명확인이 생략 가능한 것으로 오인하여 본인확인을 소홀히 할 소지가 있으므로

해당 전산시스템상에 고객의 실명번호를 입력한 후, 필수적으로 ① 디지털 본인인증을 하거나 ② 실명확인증표를 스캔하여 저장하는 등 본인확인 절차를 이행하여야만 매입·매도거래가 완료될 수 있도록 관련 업무절차를 개선하시기 바람

8) 카드론 수수료 등급산출 및 운영방식 개선

□ 내규「신용관리비용 운영기준」제4조 내지 제6조 및「내부목적 신용위험요소 관리기준」제4조 및 [별표2] 등에 의하면 대출금리 구성요소 중 신용위험비용* 및 자본비용** 산출에 적용되는 부도율은 고객의 신용등급을 기준으로 차등 적용하고 있으나,

* 표준신용위험비용 = 예상부도율 × (1-회복률) × (1-신용회수율)

** 표준자본비용 = 예상외부도율 × (1-회복률) × (1-신용회수율) × 순자본비용률

카드론의 경우 카드론 대출금리 산출에 이용되는 '카드론 수수료 등급' 산출기준을 내규가 아닌 일반문서 형태로 운영하고 있어 관련 부서가 영업 목적에 따라 자의적으로 운영할 경우 신용프리미엄이 고객에게 부당 전가될 소지가 있고,

'카드론 수수료 등급'의 경우 카드론 대출금리를 결정하는 중요한 요소임에도 불구하고 리스크관리조직(★★★★★부)이 아닌 카드영업조직(◓◓◓◓부)에서 산출하고 있어 이해상충 발생 소지가 있으므로,

'카드론 수수료 등급' 산출기준의 일관성이 유지되도록 산출기준을 내규에 명시하여 운영하고 카드론 수수료 등급별 신용위험요소 산출 과정에서 이해상충이 발생하지 않도록 관련 업무절차 및 전산시스템을 개선하시기 바람

9) 지급보증거래의 약관 및 약정서 운영 미흡

□ 「보증인보호를위한특별법」 제5조 등에 따르면 은행(채권자)은 보증계약을 체결한 후에 주채무자가 원본 등 채무를 이행하지 아니하는 경우 보증인에게 지체 없이 그 사실을 알릴 의무가 있으나

「지급보증거래 약정서」 제18조는 보증인이 통지를 원하지 않을 것을 선택할 수 있는 약정사항으로 운영하여 주채무자의 채무불이행정보 등이 보증인에게 제공되지 않을 우려가 있고

「여신거래 약정서」, 「지급보증거래약정서」 제13조에 보증인의 피보증채무 범위에서 제외하는 대상으로 신용보증기금·기술보증기금 등의 보증서만으로 한정하여 열거하고 있으나,

「은행업감독규정」 제88조의2(부당한 담보 및 보증요구 금지 등)에 따라 제3자가 은행에 예치하고 있는 예적금 등을 담보로 제공하면서 연대보증의 책임을 담보제공 범위 이내로 제한하는 경우도 피보증채무 범위에서 제외한다는 내용을 기재할 필요가 있고,

「은행업감독규정」 제88조의2에 의하면 여신취급과 관련하여 백지수표를 받는 행위를 금지하고 있으나,

사채 지급보증 관련 「기업여신상품 취급세칙」 및 상품권 지급보증 관련 「상품권 보증약정서」에는 차주로부터 백지어음을 징구하도록 하고 있으며*,

* 2010년 이후 사채·상품권 지급보증 관련 기업 여신거래가 없었기 때문에 실제로 백지어음을 징구한 사례는 없었음

은행이 지급보증하는 계약의 해지권한은 은행과 보증처가 행사할 수 있는데도 「지급보증거래 이용약관」 제8조 등에서 보증신청인(채무자)이 해지권한을 행사할 수 있는 것처럼 기재되어 있어 오해를 유발할 수 있으므로

「보증인보호를위한특별법」에 맞게 주채무자 채무불이행정보 통지 관련 보증인의 선택약정사항을 삭제하고, 제3자가 은행에 예치하고 있는 예적금 등을 담보로 제공하면서 연대보증 책임을 담보제공 범위 이내로 제한하는 경우에도 피보증채무 범위에서 제외한다는 내용을 명시하며, 사채·상품권에 대한 지급보증 관련 백지어음 징구조항을 삭제하거나 상품폐지를 검토하고, 지급보증계약의 해지권한 행사 주체·절차, 추가보증료 수취 근거 및 기간을 명확히 하는 등 지급보증 약관 및 약정서를 개선할 필요가 있음

10) 영업점 및 본부부서 성과평가기준 개선

□ 최근 불건전 영업행위(◇◇◇◇◇·◎◎ 사모펀드 불완전판매 등) 및 금융사고(직원 셀프대출, 횡령)가 발생하는 등 영업점의 소비자 보호 및 내부통제의 문제점이 부각되고 있는데도

「종합경영평가지침」의 고객가치 성과평가지표(KPI)*는 2020년 하반기에 도입하여 운영 초기상태이며, 해피콜제도 등 고객신뢰 성과평가지표(KPI)는 일부 금융투자상품(펀드, 신탁)만을 대상으로 운영하여 사전적 내부통제 기능이 미흡하고,

* 고위험상품 쏠림 및 투자성향 초과판매 관리 등

감사부문 성과평가지표(KPI)는 외부감사(금융감독원, 감사원)의 경우 문책 및 주의 등 조치의 경중에 관계없이 당해 연도에

사유가 발생한 지적건수 만을 대상으로 비중을 동일하게 적용하고, 현지조치 등을 배제하는 등 사후적인 내부통제수단으로서 효과가 제한적인 상황이므로

금융소비자의 투자성향 및 수익률에 영향을 받는 퇴직연금도 펀드, 신탁상품과 같이 '고객가치 성과평가지표(KPI) 항목'에 추가·운영하여 고객가치를 제고하고

해피콜대상으로 기존의 투자상품에 지수연계형수신상품(ELD), 퇴직연금상품도 추가하고, 해피콜 대상으로 새로 추가한 상품과 기존의 여신상품 해피콜결과를 '고객신뢰 성과평가지표(KPI) 항목'에 반영하여 불완전판매 예방효과를 높이며

현업 소관부서는 해피콜 대본 등 불완전판매 방지를 위한 기준 및 해피콜관리시스템을 마련하여 고객센터에 제공하고, 고객센터는 해피콜 담당인력의 금융역량을 강화하며, ◀◀◀◀◀부와 소관부서는 판매 및 해피콜의 적정성 여부를 점검하고 공유하여 사전적인 내부통제로서의 해피콜 실효성을 강화하고

감사부문 성과평가지표(KPI)에 문책 및 주의와 함께 경영유의, 개선사항, 현지조치 등도 포함하여 조치의 경중에 따라 평가점수를 차등화하여 외부감사효과를 제고하시기 바람

11) 대출금리 산출을 위한 신용회수율 산정방식 개선

□ 「신용관리비용 운용기준」 제4조 내지 제6조, 「신용위험요소관리기준」 제24조 및 「내부목적 신용위험요소 관리기준」 제2조 등에 의하면 대출금리 산출시 적용할 목적으로 신용위험비용*을 산정하고 있으나,

* 신용위험비용 = 표준신용위험비용** × (1-담보회수율) × (1-특정과목추가회수율)

** 표준신용위험비용 = 예상부도율 × (1-회복률) × (1-신용회수율)

표준신용위험비용 측정 요소 중 신용회수율 산정에 적용하는 할인율에 유효이자율*보다 높은 자기자본비용률**을 사용(신용회수율 하락 요인)하고 있어 신용위험비용이 과다 산정될 소지가 있으며,

* 대출신규시 적용하는 '정상이자율'로 기업대출의 경우 통상 3~5% 수준

** 규제자본 산출시 적용하는 할인율로 은행은 통상 10~12% 수준(기업은행 xx.xx%)

또한, 신용회수율 산정시 은행의 채권보전을 위한 간접비용률(x.xx%)은 차감하고, 구조조정 차주 및 부실자산 매각 등에 따른 회수금액은 반영하지 않고 있어 신용위험비용이 과다 산정될 소지가 있으므로

표준신용위험비용 측정 요소 중 신용회수율 산정시 적용하는 할인율은 유효이자율을 사용하도록 개선하고, 신용회수율 산정시 간접비용률은 차감하지 않고 구조조정 차주 및 부실자산 매각 등 회수금액을 반영하여 대출금리 산출시 신용회수율이 합리적으로 반영되도록 산출방식을 개선하시기 바람

12) 기술금융대출 취급대상 검증절차 불합리

□ 기술금융대출과 관련하여 대출 심사시 차주의 신용 이외에도 기술력 등을 검토하여 취급하고 있고,「기술금융 업무취급지침」제11조 등에 따라 기술금융 대출 취급 가능한 기술신용평가 적용대상 업종을 열거하고 있으며, 평가대상 업종 외에도 실제 기술력을 보유하고 있는 경우 기술신용평가를 신청할 수 있도록 규정하고 있으나,

기술신용평가 제한 업종 및 유의할 필요가 있는 업종에 대한 대출 취급기준이 마련되어 있지 않아, 2020년중 기술연관성이 낮은 업종(非기술 업종)에 대해서도 기술금융대출을 취급*한 바 있어 기술금융대출이 취지와 부합하지 않게 운용될 소지가 있으므로

* 한식 일반 음식업점 xx건, 커피전문점 xx건, 부동산 중개 및 대리업 xx건, 일반 화물 자동차 운송업 xx건 등

금융위원회가 발표한 '기술금융 가이드라인(2020.12.18)'을 내규에 보다 충실하게 반영하여 기술연관성이 낮은 업종(非기술 업종)에 대한 대출이 취급되지 않도록 기술평가 시스템을 개선하시기 바람

13) 담보물건 재감정 운영방법 등 개선

□ 「여신업무취급세칙」 제490조 등에 의거 담보물건 감정평가 후 일정기간 경과*한 경우 재감정을 실시하고 있으나,

* 토지· 건물 구분평가 부동산 및 시세 확인 불가한 집합건물(x년), 준부동산 (x년), 동산 (x개월), 대용가격 없는 유가증권(x개월)

재감정 기한 도래시 담보물 실태조사 실시 등 일부 조건을 충족하는 경우 재감정 기간을 기간제한 없이 유예하거나, 외부 감정평가기관의 감정평가를 생략하고 시가조사로 대체하고 있어 담보가치가 부동산의 시장 변화 등을 충분히 반영하지 못할 우려*가 있으며,

* 담보물에 대하여 xxxx년 최초 외부감정 이후 재감정 기한을 지속 연장하여 재평가만 실시한 사례 확인

외부 감정평가법인으로부터 전문(電文) 형태로 제공받은 담보평가금액이 전산시스템에 등록되는데, 영업점 직원이 금액을 임의로

수정할 수 있어 담보평가금액이 실제와 다르게 전산 등록될 소지가 있으므로,

재감정 유예 가능 기한을 제한하여 일정기간 경과 후 재감정을 실시하고, 재감정을 시가조사로 대체하는 경우에도 여신규모가 크거나 시세파악이 어려운 일반부동산에 대해서는 일정기간 경과 후 외부감정을 실시하고, 영업점 직원이 전산 등록된 담보평가금액을 임의로 수정할 수 없도록 관련 규정을 개정하는 등 감정업무절차를 개선하시기 바람

14) 동산담보대출 사후관리 절차 불합리

□ 「동산·채권담보대출담보운용기준」에 따라 동산담보대출에 대한 담보물 점검*을 자회사인 ◔◔◔신용정보에 위탁하고 영업점은 ◔◔◔신용정보로부터 '부적합'으로 통보된 담보물에 대한 사후관리**를 실시하고 있으나

* 동산 담보권을 침해할 권리설정 유무 확인, 등기사항전부증명서상 담보목적물 및 보관장소의 일치 여부, 담보물 멸실·훼손 여부, 정상가동 여부 등

** 담보물 재감정을 실시하여 실질적인 담보가치 반영, 채권보전상 필요시 여신상환 요청, 담보물 처분을 통한 대출금 회수 등

부적합 사유를 동산담보물 관리대장에 기재하고 있지 않으며 사후관리의 이행기일이 규정되어 있지 않아 동산담보물에 대한 사후관리의 적시성이 담보되기 어려우므로

동산담보대출의 담보물 점검 결과 부적합으로 통보된 담보물에 대한 부적합 사유를 구체적으로 기재·관리하고 사후관리의 이행기일을 지정하는 등 동산담보대출 사후관리 절차를 합리적으로 개선하시기 바람

15) 부동산임대업 대출 용도외유용 점검체계 불합리

□ 「여신업무취급세칙」 제462조 등에 따라 개인사업자에게 부동산 임대 시설자금대출 취급시 부동산을 사업목적에 맞게 실제 임대하고 있는지 임대차계약서 등 확인을 통해 용도외 유용 여부를 점검하고 있으나,

용도외유용 점검 대상을 주된 업종을 부동산 임대업으로 등록한 개인사업자의 시설자금대출로 한정하고 있어 임대업 이외 업종의 개인사업자에 대한 대출금이 임대목적 외(차주 본인 거주 등)로 사용되는 사례가 있으며,

또한 임대할 부동산 신축자금은 시설물이 준공되지 않을 경우 임대여부를 점검할 수 없는데도 내규 「자금용도외 유용 사후점검 기준」에 따라 점검기일을 대출 취급 후 6개월로 관리하고 있어 임대목적 용도 점검이 형식적으로 이루어질 소지가 있으므로

개인사업자에게 부동산 임대사업 용도로 취급하는 시설자금대출에 대해서는 차주의 주업종에 관계없이 임대목적 부동산의 소유권 이전 또는 소유권보존 등기가 이루어진 이후 최장 6개월 이내에 용도에 맞게 사용하는지 여부를 점검하도록 관련 규정 및 업무절차를 개선하시기 바람

16) 직원기숙사용 부동산 매입자금 대출 용도외유용 점검절차 개선

□ 기업에 대한 시설자금대출은 운전자금과 달리 시설투자 실행분에 따라 시설 공급자에게 대금을 직접 지급하므로 대출금의 용도외 유용 사후점검 대상에서 제외하고 있어

직원기숙사 용도의 고가 부동산 매입자금의 경우 심사단계에서 시설투자의 필요성 및 자금용도의 타당성 검증을 소홀히 하여 목적과 다르게 사용되더라도 용도외 유용 사후점검이 실시되지 않는 관계로 대출금 회수 등 차주에 대한 불이익이 부과되지 않을 우려가 있으므로

기업의 직원기숙사용 부동산 매입을 위한 시설자금대출 심사시에는 부동산의 소재지, 면적 등과 거주할 직원 수 등 용도의 타당성 여부를 면밀히 심사하도록 하고, 기한연장시 전입세대열람 등을 통해 당초 신청한 용도로 사용되고 있는지를 확인하도록 하는 등 용도외유용 여부 확인절차를 합리적으로 개선하시기 바람

17) 국가리스크 관리절차 불합리

□ 「은행업감독업무시행세칙」 제41조 및 [별표15]에 따라 국가리스크 관리를 위하여 차주의 귀속국가별 익스포져 한도를 설정·운영하고 있으나, 전염위험(Contagion Risk)에 선제적으로 대응하기 위하여 개별 국가수준보다 상위수준인 지역별(유럽, 아시아 등) 익스포져 한도를 설정하도록 내규 「국가별 익스포져 한도지침」에 선언적으로 규정하였을 뿐, 실제로 지역별 한도를 설정·운영하지 않고 있고, 연결대상 자회사의 익스포져를 국가리스크 관리대상에 포함하지 않는 등 관리가 미흡하므로

개별 국가보다 상위수준의 지역별 한도를 구체적으로 설정·운영하고, 연결대상 자회사의 익스포져까지 관리대상에 포함하는 등 국가리스크 관리절차를 개선하시기 바람

18) 대손충당금 산정을 위한 리스크요소 추정방법 등 불합리

㈎ Stage 분류요건 정비

□ 대손충당금 적립시 자산의 손상 인식과 관련하여 차주의 현재 신용등급이 최초 등급 대비 하락한 경우 국제회계기준(IFRS9) 기준상 Stage2*로 분류하고 있는데, 최초평가 이후 신용평가모형이 변경된 경우 최초 등급을 변경된 모형 기준으로 재산정(Back-rating)하지 않고 최초에 산정된 등급을 적용하고 있어 Stage 분류에 오류가 발생할 소지가 있으므로

* 보고일 현재 신용위험이 낮지 않고, 최초 인식일 이후 신용위험이 유의적으로 증가한 자산

신용평가모형이 변경된 경우 최초 신용등급을 변경 후 모형 기준으로 재산정하여 Stage 분류시 재산정한 등급을 활용하도록 분류요건을 개선하시기 바람

㈏ 개별평가 담보회수율 산정방식 불합리

□ 대손충당금 산정을 위한 개별평가에 활용하는 담보회수율은 최근 x개월간 법원 경매데이터를 활용한 경락률을 사용하고 있으나 장기데이터(최소 x년 이상)를 활용하는 집합평가 손실률과의 일관성이 미흡하고 단기데이터 사용에 따라 대손충당금이 경기변동에 순응할 우려가 있으므로

대손충당금의 합리적인 산정을 위해 개별평가를 위한 담보회수율 추정시 장기데이터(최소 x년 이상)를 활용하도록 관련 업무처리 방법을 개선하시기 바람

㈐ 집합평가 부도율(PD) 산정방식 불합리

□ 대손충당금 산정을 위한 집합평가 부도율(PD) 추정시 관측기간 중 신규로 발생하는 부도(이하 신규부도)를 포함하지 않고 있으며*

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

2020.6월 부도율 예측모형 산출시 전기 부도율을 신규 설명변수로 반영하였으나, 중기업 부도율 예측모형의 경우 전기 부도율의 계수가 통계적으로 유의적이지 않으며 방향성이 일관적이지 않은 측면*이 있으므로

* 은행의 부도율 예측모형에 의하면 소기업의 경우 전기 부도율이 클수록 예상 부도율이 증가하나, 중기업의 경우 전기 부도율이 클수록 예상 부도율이 감소하는 경향을 보이고 있음

집합평가 부도율(PD) 추정시 '신규 부도'를 포함하여 산정하며, 부도율 예측 모형상 전기 부도율 반영의 적합성 여부를 검토하고 코로나19 등으로 인한 경제변동성 확대 등이 감안되도록 산정방식을 합리적으로 개선하시기 바람

㈑ 집합평가 부도시 손실률(LGD) 산정방식 불합리

□ 국제회계기준(IFRS9)에 따르면 금융자산의 손상차손은 당해 금융상품의 최초 유효이자율로 할인하여 추정하여야 하는데도, 추정 모집단 부도계좌의 가중평균 유효이자율*로 할인하고 있으므로

* 부도시 손실율(LGD) 추정을 위한 부도계좌의 부도시점 유효이자율을 활용

집합평가 대손충당금 산정을 위한 부도시손실률(LGD) 추정시 당해 금융상품의 최초 유효이자율을 반영하도록 산정방식을 개선하시기 바람

19) Total exposure 한도초과 여신 취급 및 관리절차 개선

□ 「Total exposure 관리기준」 제5조에 의하면 그룹군 혹은 총익스포져(Total exposure) xxx억원 이상인 개인·법인에 대하여 동 한도를 초과하여 여신을 취급하는 경우 선임심사협의회 혹은 여신위원회의 승인을 받도록 하고 있으나,

동일자에 취급하는 금액이 xx억원 이내인 경우 횟수 제한 없이 정밀심사협의회 승인*으로 취급함에 따라 당초 한도 금액을 초과하여 과도하게 취급될 우려가 있으며,

* 검사대상 기간 중 정밀심사협의회의 건별 승인을 받아 여신을 취급한 건(xxx건) 중 최초 총익스포져(T/E) 한도 대비 총익스포져(T/E) 잔액이 xxx억원을 초과한 여신이 총 xxx건(xx.x%)

영업부점은 한도 초과시 ★★★★★부에 한도감축 계획(이행기일 포함)을 제출하나, 영업부점의 이행기일 연장 요청시 ★★★★★부가 횟수 제한 없이 연장 승인하고 있어 감축이행을 소홀히 할 우려가 있으므로

그룹군 및 총익스포져(Total exposure) xxx억원 이상 개인·법인에 대하여 동 한도 초과 여신 취급시 정밀심사협의회 승인으로 여신을 취급할 수 있는 경우를 제한적으로 운용하도록 기준을 마련하고, 한도 감축계획 이행기한 연장 승인 횟수 제한 및 미이행시 경영평가에 반영하도록 하는 등 관련 규정 및 업무절차를 개선하시기 바람

20) 운영리스크 경영평가 방법 불합리

□ 「운영리스크관리기준」 제14조에 따라 업무수행 중 발생한 위험요인을 조기에 해소하기 위하여 영업점 및 지역본부에 대한 상·하반기 경영평가시 운영리스크지표(xx개)별 발생 건수 등을 기준으로 점수화하여 감점제로 운영하고 있으며, 평가는 각 지표별로 발생건수(1건 이하 제외)를 기준으로 0.5점~2.0점을 차등하여 반영한 뒤, 지표별로 반영된 점수를 합산하여 최고 10점까지 감점하고 있으나,

발생 건수가 1건인 경우 미이행 기간에 관계없이 감점하지 않고, 3건 초과 30건 이하인 경우 1.0점을 일괄 감점하고 있어 감점 구간이 세분화되어 있지 않아 영업점별 발생건수가 크게 차이나는데도 동일하게 평가됨으로써 변별력이 없는 등 운영리스크 경영평가 방법의 합리성이 부족하므로

운영리스크 관리의 합리성과 변별력이 제고되도록 각 지표별 발생 건에 대한 미이행 기간 및 감점 구간 값의 감점 적용방법을 개선하시기 바람

21) IT업무 관련 규정 관리 불합리

□ IT업무 처리를 위해 「IT업무규정」 및 「IT업무처리지침」의 내부규정 및 정보처리시스템 보안 가이드 등 7개 가이드라인, 390개 업무·운영 매뉴얼을 마련하여 운영하고 있으나,

「IT업무규정」의 경우, 2012.12.5. 개정 이후 현재까지 장기간 개정되지 않아 「IT업무처리지침」 등의 개정사항을 반영하지 않는 등 IT업무와 관련한 변경사항이 적절하게 반영되지 못하고 있으므로

앞으로 IT업무의 변동사항 등이 적시에 내규에 반영될 수 있도록 관련 내규에 대한 관리 업무를 강화할 필요가 있음

22) 테스트데이터 변환절차 불합리

□ 프로그램 테스트를 위해 주민등록번호 등 개인정보가 포함된 데이터는 테스트데이터 변환시스템(◒◒◒시스템)을 사용하여 소속 부서장의 승인을 받아 변환하고 있으나,

테스트데이터 변환 신청시, 테스트데이터 이용 종료일자를 필수로 등록하지 않고 테스트 종료 확인 후 테스트데이터를 삭제하고 있으며, 동 업무와 관련된 절차 및 기준 등 명문화된 규정이 부재하여 테스트데이터 이용 및 관리 업무가 미흡하므로

앞으로 모든 테스트데이터 변환 신청시, 이용기간을 최소화하고 종료일자를 명시하여 테스트 종료시 즉시 삭제하며, 테스트데이터 변환 관련 절차 및 기준 등 명문화된 규정을 마련하는 등 테스트데이터 변환업무 관련 통제를 강화할 필요가 있음

23) 모바일뱅킹 앱프로그램 통제절차 미흡

□ 모바일 앱프로그램의 개발 및 배포시 형상관리시스템 등을 통해 변경내역을 등록하고 담당 책임자 승인 등을 실시하여, 단말기 제조사의 공식앱 배포처를 통해 배포토록 운용하고 있으나,

테스트환경이 인터넷망에 위치하고 있어 소스코드 난독화 등이 적용되지 않은 앱프로그램이 유출될 경우 보안이 취약할 우려가

있으며, 테스트 후 변경승인 절차가 미비하는 등 모바일 프로그램 특성을 고려한 개발·배포절차가 별도로 마련되어 있지 아니하므로

모바일 앱프로그램의 테스트 환경을 내부망으로 이동하는 등 보안을 강화하고, 모바일 프로그램 개발·배포 환경을 관련 내규에 반영할 수 있도록 시스템 및 절차 등을 개선할 필요가 있음

24) 배치작업 통제 관리 미흡

□ 배치작업 등록·실행 등 관리를 위해 배치작업관리 솔루션을 설치하여 직무에 따라 권한을 부여하고 작업시 관련 책임자의 승인*을 거치고 있으나,

* 개발자 → 현장대리인 → 팀장/부장 → 배치관리자 → 시스템 팀장(정기배치, 사후승인)

영업외시간(08:00~18:00)에 요청되는 수시 배치작업 건은 긴급성 여부와 상관없이 사후승인으로 자동 변경되어, 배치관리자의 승인 없이도 배치운영요원(OP)의 승인만으로 작업 등록이 가능하여 통제절차를 우회하는 배치작업이 수행될 우려가 있으며

검사착수일 현재 개발담당자(OOO담당자 등 3명)에게 배치작업 제어 권한 일부를 부여하고 있어 기등록된 배치작업의 임의 재실행(Rerun) 등 오조작으로 인해 시스템 오류가 발생할 가능성이 잔존하므로

앞으로 영업외시간 수시 배치작업에 대해서도 장애 등 긴급상황을 제외하고는 배치관리자의 사전승인을 받아 처리하고, 개발담당자에게는 배치작업 결과 확인 목적의 권한만을 제한적으로 부여하는 등 배치통제 절차를 개선할 필요가 있음

25) 자동화기기(ATM) 운영통제 대책 미흡

□ 자동화기기(ATM)의 안전한 운영을 위해 전용 보안솔루션을 활용하여 업무 목적상 허용된 프로세스(또는 프로그램) 실행, 매체제어 등을 통제하고 있으나,

허용된 프로세스의 세부 정보를 식별·관리하지 않아 출처와 사용 목적이 불분명한 일부 파일 실행이 허용되고 있고, 허용 프로세스 무결성 검증 방법 중 'OOO'을 비교하는 보안정책을 운영하고 있으며, 자동화기기 내 OO 사용을 허용하고 있어 파일명 변조 등을 통해 보안솔루션을 우회한 악성코드가 설치·실행될 우려가 있으므로

앞으로 자동화기기 허용 프로세스에 대한 정보를 주기적으로 식별·관리하여 불필요한 프로세스를 제거하고, 프로세스 무결성 검증 방법을 추가 보완하는 등 자동화기기 운영 통제 대책을 개선할 필요가 있음

26) 기술지원 종료 운영체제 사용에 따른 보안통제 미흡

□ 검사종료일 현재 가동 중인 시스템 총 x,xxx대(운영, DR기준) 중 xxx대에서 제조사 기술지원이 종료된 운영체제(OS)를 사용하고 있어

동 운영체제에 대한 신규 취약점 보완 및 기능개선 등을 위한 보정(patch) 작업이 곤란하여 미보완 취약점을 이용한 해킹, 악성코드 감염 등 침해사고가 발생할 우려가 있으므로

앞으로 기술지원 종료 운영체제를 상위 버전으로 업그레이드하거나 제조사와 기술지원 연장 계약을 체결하는 등 운영체제 장애발생을 미연에 방지하기 위한 구체적인 대응계획을 마련하여 조속히 이행할 필요가 있음

27) 소산센터 및 전산실 작업통제 관리 미흡

□ 주전산센터(◑◑◑◑센터) 백업 전산자료의 안전한 보관을 위해 원격지 소산센터(OO 소재)를 설치하고, 소산 저장매체(Tape 등)를 내화금고 등에 보관하고 있으나,

소산매체 반출입시 부서 책임자의 승인 후 소산을 실시하면서도, 소산센터에서는 보유중인 소산매체 내역 및 출입관리대장을 별도 기록·관리하지 않아 비상시 소산매체 식별 및 활용, 소산매체 분실시 출입자 추적 등에 어려움이 예상되고

재해복구센터(▨▨▨▨▨▨센터)에서 시스템 유지보수 등 작업을 수행하는 외부 직원에 대한 현장통제 및 모니터링에 미흡한 점이 있으므로

앞으로 소산센터에서도 소산매체 내역 및 출입관리대장을 기록·관리하고, 재해복구센터에 출입하는 외부직원의 시스템 작업에 대한 통제 및 모니터링 대책을 마련·운영하는 등 소산센터 및 전산실 작업통제 관리를 개선할 필요가 있음

28) 침해사고 대응훈련의 실효성 불합리

□ 홈페이지 및 인터넷뱅킹에 대해서는 해킹, DDoS공격 등에 대비한 침해사고 대응훈련을 연 x회 실시하고 있으나,

모의해킹 훈련은 홈페이지 등 웹서버 위주로 훈련하고 있어 모바일뱅킹 등에 대한 해킹 위협 대응이 다소 미흡할 우려가 있으므로

앞으로 침해사고 대응훈련의 실효성을 제고하기 위해 모바일뱅킹 및 메인 홈페이지 외 기타 웹페이지에 대해서도 침해사고 대응 훈련을 추가하여 실시할 필요가 있음

29) 정보처리시스템 접근권한 관리통제 미흡

□ 서버접근통제시스템 및 DB접근통제시스템을 활용하여 단말기를 통한 정보처리시스템의 주요명령어* 실행을 통제하고 접근기록 및 명령어 실행기록을 보관하고 있으나

* OO 등 xx개 명령어를 차단하였고, OO 등 xx개 명령어를 중요명령어로 등록하여 통제 (계정등록시 승인 후 사용가능)

사용자가 특정서버에 접속한 후 서버접근통제시스템을 거치지 않고 일부 주요명령어를 이용하여 다른 서버로 접속할 수 있고

IT부서 외 업무부서*에 직접 운영DB를 조작할 수 있는 권한을 과도하게 부여하고 있어 DB명령어 오조작에 따른 서비스 중단 등 운영 중인 서비스에 영향을 미칠 우려가 있으므로

* IT부서 외 ◕◕◕◕◕팀 등 xxx명에 xxx개 DBMS 조작 권한 부여

접근통제시스템의 중요명령어 통제 대상을 확대하고, 서버간 원격 접속을 통제하며, 업무부서의 운영DB를 조작할 수 있는 권한을 최소화하고 불필요한 권한을 회수하는 등 정보처리시스템 접근 통제를 강화할 필요가 있음

30) 내부 전산자료 통제 불합리

□ 업무용 단말기에서의 고객정보 등 주요 정보의 유출방지를 위해 내부정보유출방지시스템(DLP), 개인정보검색시스템 등을 설치하는 등 전산자료 보호체계를 갖추고 있으나

일부 사용자들이 업무자료 공유 목적으로 공유폴더를 사용하고 있어 공유폴더를 통한 바이러스 전파 및 PC해킹 등의 침해위협이 발생할 수 있으므로

앞으로 업무용단말기에서의 공유폴더 사용을 제한하고, 직원간 내부자료 공유는 기구축하여 운영 중인 웹디스크시스템 등을 활용하는 등 내부 전산자료 통제를 강화할 필요가 있음