경영유의사항 등 공개안

1. 금융회사명 : 한국수출입은행

2. 조치일 : 2023. 5. 24.

3. 조치내용

대상	내 용
기관	경영유의사항 16건, 개선사항 20건

4. 조치대상사실

가. 경영유의사항

(1) 내부자본적정성 관리 및 보고 절차 강화

은행은 매년 '리스크관리 기본계획(안)'을 통해 예상 가용자본에 일정 비율로 내부자본 한도를 설정하고 산출된 리스크량이 내부자본 한도를 넘지 않도록 관리방안을 마련하여 이사회 승인을 받고 있으나

예상 가용자본 산정 시 기본자본 외에 보완자본 일부(정상 또는 요주의 충당금 중 보완자본 인정금액*)를 포함하여 가용자본이 과다 산정되어 내부자본 한도가 높게 설정되고 있고

* 「은행업감독업무시행세칙」 <별표3>에 따르면 표준방법을 사용하는 경우 자산건전성 분류 결과 "정상" 또는 "요주의"로 분류된 자산에 대하여 적립된 대손충당금은 신용위험가중자산의 1.25% 범위내에서 보완자본에 산입하는 것을 허용

금융감독원에 제출하는 내부자본 적정성 보고서도 이사회 또는 리스크관리위원회에 보고 없이 리스크관리 총괄책임자(CRO)에게 구두로만 보고하고 제출하는 등 관리 체제가 미흡하므로

실질적인 자본금액이 제대로 반영할 수 있도록 가용자본 산정방식을 재검토하여 합리적으로 변경하고 내부자본적정성 관리와 관련하여 내부보고 절차를 강화할 필요가 있음

(2) 신용등급 평가 및 조정 업무 강화

여신부·점의 경우 신용평가에 대한 전문성이 본부 신용평가 부서에 비해 상대적으로 부족할 뿐 아니라 신용평가와 영업의 이해상충 가능성이 있으므로 보다 면밀한 견제장치를 마련하여야 하나

은행 신용평가 재무이상치 분석시스템에서 적출된 차주의 경우 차주의 재무제표 신뢰도에 문제가 있거나 차주의 부실화 가능성이 있는 경우에 해당할 수 있는데도 본부부서 등 제3자에 의한 별도의 확인 절차 등 보다 면밀한 견제장치 없이 여신부·점에서 신용등급을 평가하고 있으며

여신부·점에서 재무평가와 비재무평가를 토대로 산출한 신용등급 대비 최종 신용등급을 별도의 통제장치 없이 일정 부분 상향할 수 있는 구조이므로

여신부·점에서 재무이상치 분석시스템에 적출된 차주를 신용평가 하거나 최초등급 대비 최종등급을 상향하고자 하는 경우 추가적인 검토 절차를 마련하는 등 신용등급 평가 및 조정업무를 강화할 필요가 있음

(3) 익스포저 한도 관리 실효성 확보를 위한 관리체계 개편

내규「리스크관리세칙」제11조 및 제12조에 따라 은행은 자산건전성 유지를 위하여 총 익스포저 한도를 관리하고 있으나

은행 전체 익스포저 한도를 바젤I 당시의 규제비율(8%) 수준에서 수용 가능한 위험가중자산의 총액인 은행 자기자본의 12.5배로 설정하고 있어 현재 은행 전체 익스포저 대비 한도가 과도하게 높게 설정되어 있어 전체 익스포저 한도 관리가 실효성이 있지 않고

기업별 한도를 개별기업 익스포저 한도와 신용 여신한도로 구분하여 관리하는데 신용 여신한도는 산식상 개별기업 익스포저 한도보다 작게 설정되어 있고, 신용 여신한도는 모든 기업에 대해 적용하고 있어, 전체 여신 중 신용여신비율이 높은 은행의 구조상 실질적으로 신용여신 한도만이 관리 수단으로 활용되는 상황이므로

익스포저 한도 관리가 자산건전성 유지를 위한 실효성 있는 관리 수단으로서 역할을 할 수 있도록 은행 전체 익스포저 한도 및 개별기업 익스포저 한도를 포함하여 종합적인 익스포저 한도 관리체계를 마련할 필요가 있음

(4) 신용 및 편중리스크 내부자본 관리 강화

신용 및 신용편중리스크 내부자본 한도 설정 및 증액은 은행 업무에서 발생하는 리스크를 정확하게 파악하여 은행이 최대로 부담할 수 있는 리스크를 계산하는 과정이므로 은행의 사업구조 및 재무계획, 통합위기상황 분석결과, 경기전망 및 리스크 측정 요소 변경 여부 등을 고려하여 충분한 검토를 거쳐야 하는데도

신용 및 신용편중리스크 내부자본 한도 설정 및 증액에 대한 명시적인 기준이 없어 자의적 판단이 개입될 가능성이 있으므로 한도 설정 및 증액 시 검토하여야 할 항목·방법 등을 마련하는 등 내부자본을 체계적으로 관리할 필요가 있음

(5) 조기경보시스템 운영 관리 강화

은행은 조기경보기업의 확정등급을 중점관리기업으로 최초 분류 시 신용등급 재평가 의무만을 부여할 뿐 판정 결과를 신용평가에 반영하고 있지 않아 조기경보체계가 조기에 위험을 식별하여 선제적으로 대응하기 어려우므로 판정 결과를 신용평가에 반영하여 조기경보와 신용평가와의 연계를 강화할 필요가 있음

또한 일부 국외기업의 경우 조기경보 기업감리에서 제외하여 연 1회 사후관리 감리만 실시하고 있어 해당 기업에 대한 조기 위험 식별 및 선제적 대응이 어려울 수 있으므로 제외 차주에 대한 감리 주기를 조정하고 부실 발생 가능성을 조기에 식별할 수 있도록 검토항목을 확대하는 등 리스크관리 체계를 강화할 필요가 있음

(6) 부책심의 사후관리 강화

「금융기관채권대손인정업무세칙」 제5조 등에 의하면 금융회사는 대손인정을 신청하고자 하는 부실채권 관련 서류를 본부에 집중하고 조속한 시일 내에 자체 책임심의를 완료하여야 하나

내규상 부책의 시효 외에는 부실채권에 대한 부책심의 처리기한을 별도로 정하지 않아 장기간 부책심의가 지연되는 사례가 있으므로

부책심의가 적시에 이루어질 수 있도록 실시계획을 수립하고 이행현황을 관리하는 등 부책심의 업무를 강화할 필요가 있음

(7) 수출채권 매입업무 관리 강화

은행은 수출 거래의 실재성 확인 및 수출업체의 부도 위험 점검 등을 위해 수출채권 매입서류 심사 및 사후관리 방안을 마련하여 시행하고 있으나

영업부·점 담당 직원들이 수출채권 매입 시 활용할 체크리스트가 없고 수출채권 미결제 이력이 있는 업체 등에 대한 별도의 심사기준이 마련되지 않은 등 수출매입 업무 관련 사고 위험성을 절감하기 위한 표준화된 업무처리 체계 구축이 미흡하므로

수출채권 매입 시 필수서류별로 매입서류의 완전성 등을 자가 점검할 수 있는 체크리스트를 마련하고 그에 따른 점검결과 입력, 승인권자의 확인 등 전산통제 할 수 있는 체계와 수출채권 관련 미결제 이력을 점검하도록 하는 심사기준을 마련할 필요가 있음

(8) 적합성 검증 및 제3자 점검업무 강화

「은행업감독업무시행세칙」 <별표3의9>에 따르면 은행은 내부감사 또는 유사한 독립적인 조직이 내부자본적정성 관리체계를 연 1회 이상 점검하도록 하여야 하며,

동 세칙 <별표19>에 의하면 은행은 위기상황분석 결과, 분석기준 및 절차의 적정성 등에 대해 최소 연 1회 이상 내부감사를 실시하여야 하고, 동 별표 및 은행 내규 「리스크관리기준」 제36조에 의하면 위기상황분석이 적정하게 수행되고 있는지 확인하기 위하여 감사담당부서 또는 외부전문가를 통해 연 1회 이상 모형 및 시나리오에 대해 적합성 검증을 실시하여야 하는데,

정기적인 적합성 검증업무를 수행하기 위한 관련 조직 및 인력 등 검증체계가 마련되어 있지 않고, 통합위기상황분석에 대하여 외부전문가에 의한 비정기적 검증만 실시하고, 내부자본적정성 관리체계에 대해서도 A부서에서 개별 시스템 단위의 비정기적인 점검만 실시하는 등 적합성검증 및 내부감사가 적정하게 실시되지 않고 있으므로,

업무분장 상 적합성 검증 및 제3자 점검업무 담당 조직을 명확히 하고 업무수행을 위한 필요 인력 및 예산수요 등을 포함한 세부적인 실행 계획을 마련하고 동 사항과 관련하여 내규를 정비할 필요가 있음

(9) 내부통제 조직 기능 강화

㈎ 준법감시부서와 감사부서 간 유기적 연계 강화

준법감시부서와 감사부서는 내부통제의 사전·사후를 담당하는 조직으로 정보공유를 통해 긴밀히 협조하여야 하나 상시감시시스템의 관리 및 모니터링을 감사부서에서 주관하고 부서 간 시스템도 연계되어 있지 않은 상황이며 상시감시를 통해 시정·개선으로 이어진 사안이 전무하는 등 상시감시 운영이 미흡하므로

준법감시부서와 감사부서 상호 간 정보열람 등을 통해 피드백을 줄 수 있도록 하는 등 내부통제 활용에 부서 간 협조를 제고할 필요가 있음

㈏ 감사조직 독립성 제고

감사부장에 대한 성과평가를 은행장과 임원이 공동으로 하고 있어 감사업무 수행의 독립성이 저해될 수 있는 구조이므로 감사조직의 독립적 운영 제고를 위해 감사부장에 대한 성과평가 체계를 개선할 필요가 있음

㈐ 감사인력의 전문성 제고

내규상 감사부 직원은 3년 이상 근무가 원칙이나 2022.6월말 현재 감사부 직원의 평균 근속기간은 내규보다 짧은 수준이며 외환·파생·IT부문 실무경험이 있는 전문검사역이 부재하므로 감사인력의 질적 향상을 통해 검사 실효성을 제고할 필요가 있음

㈑ 합리적인 감사계획 수립

2022.6월말 기준 내부감사 실시 후 3년 초과 본부부서, 지점 및 해외사무소·현지법인이 다수로 금융사고 개연성에 노출될 우려가 있으며

감사계획 수립 시 주기를 별도로 정하지 않고 감사 순기를 고려하여 대상 부서를 정하고 있어 감사부 상황 등에 따라 일부 부·점은 감사대상에서 제외될 소지가 있으므로

종합감사 실시 3년 초과 부·점에 대해 우선적으로 감사하는 방안을 감사계획에 반영하는 등 감사 주기에 대한 원칙을 수립하여 장기간 감사를 받지 않은 부·점이 발생하지 않도록 합리적인 감사계획을 수립하여 운영할 필요가 있음

(10) 내부통제체제 운영의 실효성 제고

은행장은 내규 「내부통제규정」에 따라 내부통제체제의 구축 및 운영에 필요한 제반 사항을 지원하고 적절한 내부통제 정책을 수립해야 할 의무가 있으나

실제 은행장이 주관하거나 참석하는 내부통제 점검 회의체 없이 준법감시인을 통해

관련 내용을 보고 받는 수준에 그치고 있어 내부통제 관련 이슈 발생 시 은행장이 경영진과 함께 논의하고 적시에 대응하기 어려우므로

실효성 있는 내부통제 정책의 수립 및 내부통제체제의 운영을 위해 실질적인 내부통제 점검방안을 마련할 필요가 있음

준법감시인은 「내부통제규정」 및 「준법감시세칙」에 따라 준법감시업무를 통할하면서 준법감시활동 추진계획 및 결과, 내부통제 및 윤리경영에 관한 중요정책 등을 은행장에게 보고할 의무가 있으나

여신·유가증권 투자·외국환 거래업무 등 은행의 고유업무 전반에 걸친 내부통제체제의 실질적 운영에 관한 사항보다는 임직원의 금품수수, 내부 정보를 이용한 주식 및 부동산 거래 등 임직원 개인의 비위 등을 근절하기 위한 반부패·청렴 정책을 보고하는 데 치우친 경향이 있으므로

임직원이 은행의 고유업무 수행 시 내규 등 관련 법규를 준수하는지 점검하는 계획과 그 결과에 대해서도 은행장에게 보고하는 등 내부통제체제 운영의 실효성을 제고할 필요가 있음

(11) 자점감사제도 운영 불합리

감시실시 부·점장이 감사자를 지명하여 일상업무를 감사하고 있으나 자점감사 항목이 부서 고유업무와 직접 관련 없는 공통사항에 치중되어 있고 검사 착수일(2022.10.31.) 현재까지 자점감사 결과 지적이 전무하며 자점감사자에 대한 포상, 우대 조치 등이 없어 자점감사를 충실히 수행할 유인이 없으므로

부서 고유업무의 리스크를 감안한 자점감사 항목을 개발·운영하는 한편 우수 감사자에 대한 포상, 우대 조치 등이 자점검사의 충실한 이행의 유인으로 기능할 수 있도록 관련 업무 프로세스를 강화할 필요가 있음

(12) IT부문 내부통제 체계 강화

㈎ 감사부는 종합감사와 특정감사 등의 방법으로 디지털금융단(정보시스템부 포함) 및 정보보호실에 대한 감사를 실시하고 있으나,

감사부에 IT업무 전문성(IT업무 수행경험 등)을 보유한 감사 인력이 배치되지 않아 IT부서에 대한 실효성 있는 감사가 이루어지기 어려우며, 부서별(또는 업무별) 종합

감사 주기가 명확히 정의되어 있지 않아 2019년 IT부서에 대한 감사 실시 이후 현재까지 종합감사가 실시되지 않았으므로,

감사부에 IT업무 관련 전문성을 보유한 감사인력을 배치하여 IT부문의 감사 전문성을 확보하고, IT부문에 대한 종합감사가 장기간 누락되지 않도록 부서별(또는 업무별) 종합감사 주기를 명확히 정의할 필요가 있음

㈏ 디지털금융단은 IT자체감사인 및 IT자체감사실무자를 지정하여 디지털금융기획팀, 디지털혁신팀 등의 직할 팀과 정보시스템부에 대해 일일감사, 월별감사, 특명감사 등의 방법으로 자체감사업무를 수행하고 있으나,

정보시스템부에 대한 월별감사와 특명감사는 IT자체감사인과 IT자체감사실무자가 아닌 정보시스템부 소속 직원을 감사인으로 지정하고 내부통제업무를 수행하여 자체감사업무의 독립성 저하와 이해충돌 발생이 우려되므로,

디지털금융단에 대한 일일감사, 월별감사, 특명감사 등의 내부통제업무는 감사업무의 독립성을 확보하고 이해충돌이 발생하지 않도록 IT자체감사인과 IT자체감사실무자가 직접 실시할 필요

㈐ 준법감시인(CISO 겸직)의 통제를 받는 정보보호실은 정보보호시스템 운영 등 위험도가 높은 중요 업무를 수행하고 있음에도,

내부통제업무를 담당하는 IT보안자체감사인이 지정되어 있지 않고, 일일감사, 월별감사, 특명감사 등의 IT보안자체감사업무를 수행하고 있지 않으므로,

정보보호실은 내부통제업무 수행을 위한 IT보안자체감사인을 지정하고, IT보안자체감사업무를 수행할 필요

(13) IT업무연속성 계획 수립·운용 강화

㈎ 매년 리스크업무팀 주관으로 단위업무를 지정하고, 각 단위업무 담당부서가 수행한 전사업무영향분석(BIA) 결과를 바탕으로 핵심업무를 선정하고 복구목표시간 등을 설정하고 있으나,

업무 담당부서가 전사업무영향분석(BIA)을 수행하는 과정에서 IT부서와 협의하는 공식 절차가 부재하여 핵심업무와 연관된 복구대상시스템이 불명확할 우려가 있는 등 전사적 관점에서의 핵심업무 선정 절차가 미흡하므로

핵심업무와 관련된 복구대상시스템이 명확히 정의되도록 전사업무영향분석 시 IT부서 합의절차를 추가하는 등 핵심업무 선정 절차를 개선할 필요가 있음

㈏ 내규에서 정한 중대한 사고가 발생한 경우 금융감독원 등에 사고보고를 하도록 규정하고 있으나,

전자금융사고 기준 및 대응조직, 직무별 역할, 단계별 세부 대응·보고 절차, 사고보고 및 사후관리 절차 등의 세부내용을 포함한 전자금융사고 대응지침 및 매뉴얼을 마련하지 않아 전자금융사고 발생 시 즉각적이고 체계적인 대응에 어려움이 예상되므로

전자금융사고 대응지침을 마련하고 관련 매뉴얼을 정비하는 등 전자금융사고 대응·보고체계를 강화할 필요가 있음

㈐ 전산장비의 장애·오류 등으로 인한 서비스 중단에 대비하여 서버, 네트워크 장비 및 방화벽 등 주요 전산장비를 이중화 구성하고 있으나,

신규 시스템 구축 시 전환(fail-over) 테스트를 수행한 이후, 비정기적인 운영체제 패치작업을 하는 과정에서 시스템 전환을 수행하는 방법으로 전환검증을 하는 등 이중화 장비의 검증업무가 불합리하게 수행되고 있으므로

주요 전산장비의 전환 테스트가 주기적으로 이루어질 수 있도록 관련 내규를 정비하고, 정기적으로 전환여부를 검증하여 전산장비 업무연속성을 보장할 필요가 있음

(14) 정보보호 관리체계 강화

임원 및 본부장 업무분장에 따라 내부통제 업무를 총괄하는 준법감시인이 정보보호최고책임자(CISO)를 겸임하고 있으나,

정보보호실에서 정보보호 기획·운영, 관제 업무와 더불어 개인·신용정보보호 업무까지 포괄적으로 수행하고 있고, 관리자(실장) 1명이 정보보호 사업계획 관리, 보안정책 승인 등 정보보호 부문의 관리업무를 총괄하고 있어 정보보호 정책결정 및 관리통제 등이 적기에 시행되지 않을 우려가 있으므로

IT부문의 안전성 확보를 위한 정보보호 관련 위험관리 및 통제 수행, 정보보호 조직 및 인력 강화를 위한 노력 등 정보보호 관리체계 강화방안을 마련하시기 바람

(15) 유동성리스크 허용한도 관리 절차 강화

은행은 유동성리스크 허용한도 초과 시 보고 절차 및 대응조치 등을 문서화하고 있으나 보고 절차 및 대응조치를 구체적으로 정하고 있지 않아 유동성리스크 허용한도

관리의 실효성이 미흡하므로

유동성리스크 허용한도 초과 시 보고 시기·주체 등 구체적인 조치사항을 문서화하여 유동성리스크 허용한도 초과 발생 시 그에 따른 실질적인 조치가 이루어질 수 있도록 유동성리스크 관리전략을 강화할 필요가 있음

(16) 비상조달계획 수립 및 보고업무 강화

은행은 위기상황 발생 시 정부 및 중앙은행이 외화유동성 공급을 확대하거나 조건을 완화할 것으로 기대하여서는 아니 되는데도

검사대상기간 동안 매 분기 유동성 위기상황에서 자금 과부족을 해소하기 위한 비상조달계획을 수립하면서 중앙은행의 외화 유동성 확대를 기대하는 등 일부 불합리한 내용이 포함되어 있으므로

위기상황 발생 시 경영진이 적시에 대응책을 마련할 수 있도록 비상조달계획 보고체계를 강화하고 비상조달 방법 및 수단을 보완하는 등 유동성리스크 관리를 강화할 필요가 있음

나. 개선사항

(1) 여신 사후관리 시스템 개선

내규「여신기준」제139조 등에 의하면 수출촉진자금대출 등 여신을 취급하는 경우 여신거래의 실재성 확인 및 용도외 유용 등 사후관리를 위해 사업장을 방문하여 현물시설을 확인하고 현물시설 사진을 첨부한 공정 확인서를 작성하는 등 증빙 자료를 확보하도록 하고 있으나

현장 방문 정보 입력, 사업진행상황에 관한 증빙자료 등재 관리 등을 전산시스템으로 관리하지 않아 사후관리 업무의 적정 수행 여부를 확인하기 어려워 사후관리 업무가 형식적으로 수행될 우려가 있으므로

현장 조사내용과 사업진행상황 증빙자료 등을 관리할 수 있도록 전산시스템을 보완하고 현장 조사 여부를 주기적으로 점검하는 등 여신 사후관리 절차를 개선하시기 바람

(2) 대고객 거래 관련 외환 파생상품 거래 위험관리 기준 개선

「은행업감독규정」 제67조의2에 따르면 은행은 「은행업감독업무시행세칙」 <별표 15의2>에서 정하고 있는 '외환파생상품거래 리스크 관리기준*'을 포함한 자체적인 위험관리 기준을 설정·운영하여야 하는데도

* 외환파생상품 거래 시 위험헤지비율 한도 설정 및 운영에 관한 사항 등

내규 「외국환세칙」를 통해 기업투자자와 외환파생상품 거래 시 준수해야 할 사항을 정하여 운영·관리하면서도 동 시행세칙에서 명시한 사항 중 위험헤지비율 상한 초과 운영에 관한 사항과 비거주자와 거래 시 관리에 관한 사항을 반영하고 있지 않으므로 관련 내규를 개선할 필요가 있음

(3) 환리스크 한도 관리 개선

은행은 내규 「리스크관리기준」 <별표3> 및 이사회에서 승인하는 리스크관리기본계획에 따라 환율변동에 의한 외화자산·부채의 환리스크 관리를 위해 환포지션 및 환VaR 측정 방식으로 한도를 설정하여 관리하고 있는데

아래와 같이 한도를 합리적 근거 없이 과도하게 높은 수준으로 설정하여 최근 금융시장 변동성에도 불구하고 2022.9월말 기준 2개 한도의 소진율이 낮게 나타나는 등 한도관리의 실효성이 부족하므로 한도설정 방법을 개선할 필요가 있음

① 환포지션 한도는 ❶과거 1년간 환포지션 평균값 + ❷표준편차 x 2.33*에 ❸과거 5년간 환포지션 증감률을 추가 반영하는 등 환포지션의 변동성을 과도하게 반영하고 있고

* 99% 신뢰수준 반영 (통상 정규분포의 '평균+표준편차x2.33'으로 99%-ile 추정)

② 환VaR 한도도 ①의 방식으로 높게 산출된 환포지션 한도를 기초로 산출하여 변동성을 과도하게 반영하여 높게 설정하고 있음

(4) 위기상황분석 분석 방법 및 절차 개선

수출입은행 위기상황분석 분석방법 및 분석절차, 보고 등과 관련하여 아래와 같은 미흡한 점이 있으므로 관련 업무를 개선하시기 바람

㉠ 통합위기상황분석 분석방법 및 절차 개선

「은행업감독업무시행세칙」 <별표19> 제7조 등에 의하면 이사회와 경영진은 위기

상황분석 절차, 가정 및 결과 등에 대해 충분히 이해하고 위기상황분석 과정에 참여하여 의견을 개진하는 등 분석과정에 참여하여야 하는데도

통합위기상황분석 시나리오 설정 시 유관부서나 이사회·경영진의 참여 없이 리스크관리부가 해외경제연구소의 의견만 반영하여 분석시나리오를 최종 결정하는 등 위기상황분석 수행 절차가 미흡하며

위기시 충격이 자본에 미치는 영향을 산출하는 과정에서 비트레이딩 계정의 평가손실을 반영하지 않고 있고, '21.12월 통합위기상황분석시 PD 산출과정에서 데이터 입력 오류가 발생하는 등 분석 결과에 대한 신뢰성이 미흡하므로 통합위기상황분석 분석방법 및 수행 절차 등을 개선할 필요가 있음

㉡ 금리위기상황분석 분석 방법 개선

경영진과 이사회에 보고 중인 금리위기상황분석 결과는 매분기 금리리스크 관리지표(△EVE, △NII) 산출값에 불과하여 개별 금리위기상황분석 수행의 실효성이 다소 미흡하므로

금리리스크 지표 산출에 사용되는 세칙*상 시나리오와 다른 별도의 시나리오 등으로 보완하여 실효성있는 금리리스크 위기상황분석을 수행하도록 개선할 필요

* 「은행업감독업무시행세칙」 <별표 9-1> 금리리스크 산출기준 및 「은행업감독업무시행세칙」 <별표19> 제5장 제7절

㉢ 민감도분석 분석방법 및 보고 개선

매 분기 개별 리스크 요인 변화에 따른 BIS비율 영향도 분석(민감도분석)을 수행하여 리스크관리위원회에 보고하면서 일부 관련도가 낮은 요인의 변화에 대한 산출결과를 합산하여 취지와 달리 분석 및 보고하고 있으므로

개별 요인의 변화가 BIS비율에 미치는 영향도를 파악할 수 있도록 분석 및 보고 방식을 개선할 필요

(5) 내부고발자 제도에 대한 운영 절차 개선

① 은행은 내규 「내부자신고세칙」에 따라 내부고발자 제도를 운영하면서 은행장 등 최고경영자와 관련된 사안이 접수될 경우 내부고발 처리 과정에서 동인을 제척하여야 하는데도

모든 내부고발에 대하여 은행장에게 보고 및 승인을 받도록 운영되고 있어 관련

업무가 공정하게 처리되지 못할 위험이 있으므로 은행연합회의 「은행내부자신고제도 준칙」 등을 참고하여 최고경영자에 대한 제척 조항을 마련하는 등 운영 절차를 개선하시기 바람

② 은행은 접수된 내부고발과 관련하여 고발 내용, 고발자의 신원 등 일체의 사항을 타인에게 제공하거나 누설(이를 암시하는 행위를 포함)하지 아니해야 하는데도

익명으로 접수된 내부고발의 경우 그 처리결과를 은행 내 전산망에 공지하도록 「익명신고처리기준」에 규정하고 있어 「내부자신고세칙」과 부합하지 않고 내부고발자의 고발 내용 및 신원 등이 타인에게 노출되거나 암시될 위험이 있으므로 관련 내규를 정비하는 등 관련 절차를 개선하시기 바람

(6) 부·점별 법규준수 점검 절차 개선

내규 「준법감시세칙」에 따르면 부점별 준법담당자는 부점 직원에 대한 법규준수 모니터링, 법규준수와 관련된 소속 부·점 직원교육, 직원의 법규 위반사항 보고 등의 업무를 수행하며 준법감시업무 수행 현황 및 결과를 준법감시인에게 보고하여야 하며

준법감시인 산하 B부서는 부·점별 법규준수 활동을 월별로 보고 받아 부·점별 법규준수 업무 운영실태를 점검하고 있으나

월별 법규준수 활동 보고 내용에는 직원교육, 준법체크리스트 수정 보완, 소관 업무 관련 법규 제·개폐, 상담기타 항목만 있으며 실질적으로 준법체크리스트 항목에 대한 점검내용 등 법규준수 점검 결과 내용이 없으므로 실효성 있는 법규준수 점검을 위해 보고 항목에 법규준수 점검 결과를 포함하는 등 관련 절차를 개선하시기 바람

(7) 자금세탁방지 업무 보고체계 및 독립감사 절차 개선

자금세탁방지 업무 관련 내규에서 정하고 있는 내용이 아래와 같이 상위 법규와 다르거나 일부 미흡한 점이 있으므로 관련 내규 등을 합리적으로 개선하시기 바람

① 은행은 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」에 따라 의심스러운 거래에 대한 보고 업무 담당자로 준법감시인을 임명하고 금융정보분석원장에게 통보하였으나

내규 「자금세탁방지업무취급세칙」에서는 보고책임자 임면 사항의 감독기관 앞 보고 등 일부 업무를 자금세탁방지 업무 담당 본부장이 수행하도록 정하고 있어 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」에 따른 보고업무 담당자와 내규상의 보고

책임자와의 관계 및 책임이 불분명하므로 관련 법규에서 규정한 취지 등을 반영하여 보고업무 담당자와 보고책임자와의 관계 및 책임을 명확히 정리할 필요가 있음

② 또한 내규에서는 보고책임자 직속의 담당 조직을 두고 동 조직이 수행할 업무를 정하고 있으나

2022.9월말 현재 은행은 업무를 이행할 대상 부서를 지정하지 않고 있으므로, 실제 자금세탁방지 관련 업무를 수행하고 있는 자금세탁방지팀의 책임을 내규등에 명확히 하는 한편 전담 직원의 자격 및 인사에 대한 근거 규정도 보완할 필요가 있음

③ 한편 내규상 자금세탁방지 업무에 대한 독립적 감사 대상을 전담 조직으로만 명시하고 있어 부·점의 자금세탁방지 업무에 대한 감사가 적절히 이루어지지 않을 우려가 있으므로 전담 조직 이외의 부·점에 대한 감사 주기, 방법 등에 대한 세부 기준을 마련하여 운영할 필요가 있음

(8) 신용정보 관리 절차 개선

수출입은행의 신용정보 관리업무와 관련하여 아래와 같은 미흡한 점이 있으므로 관련 업무를 개선하시기 바람

㈎ 신용정보의 등록·변경 등 관련 절차 강화

내규 「신용정보·개인정보보호세칙」에 따르면 은행은 신용정보의 정확성이 유지될 수 있도록 신용정보의 등록·변경 및 관리를 하여야 한다고 규정하고 있고 C부서에서 정기적으로 신용정보의 정확성에 대해서 점검하고 있으나

일부 예외사유에 한하여 담당자가 수기 등록을 하고 있는데도 관련 정보를 등록하는 절차에 해당 부서내 관리자의 전산 승인 등의 절차가 미흡하여 사실과 다른 정보가 집적될 우려가 있으므로

수기등록 정보에 대해서는 신용정보를 취급하는 부서(본부부서, 지점 등)에 대한 신용정보의 등록·변경, 파기 등 업무처리의 정확성을 제고하기 위해 수기등록 정보에 대한 관리체계를 정비할 필요가 있으며

또한 동 업무와 관련하여 신용정보 취급 부서의 업무별 위임전결 규정을 명확히 하여 내부통제 책임 범위 및 법 위반 발생 시 책임소재를 명확히 할 필요가 있음

㈏ 신용정보 접근 권한관리 관련 내규 개선

내규「신용정보·개인정보보호기준」에 따라 은행은 개인신용정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 담당자에게 차등 부여하고 접근권한을 관리하고 있으나

2016.4.7. 선언적으로 '개인신용정보 접근권한 관리 개선방안(안)'을 마련하였으나 개인신용정보 접근권한 부여 및 회수 절차, 사후 점검 등에 대한 구체적인 가이드라인이 포함되어 있지 않으므로 개인신용정보 접근권한과 관련한 내규를 개선할 필요

㈐ 신용정보 관련 업무매뉴얼 개선

연체 정보 등록 등의 업무와 관련하여 실무 매뉴얼에 관련 업무 내용과 절차 등을 규정하고 있으나 매뉴얼이 최신 기준을 반영하고 있지 않아 해당 업무처리에 오류를 범할 우려가 있으므로

신용정보 업무와 관련한 실무 매뉴얼을 재점검하여 현재 기준을 반영하여 개정하고 일반신용정보관리규약 개정 등 관련 기준의 변경이 있는 경우 해당 변경내용을 확인하여 은행과 관련된 개정 사항이 있을 경우 실무 매뉴얼 등 관련 규정에 신속하게 반영할 필요가 있음

(9) 테스트데이터 변환 관련 내규 불합리

내규에 따라 프로그램 테스트 시 운영계 실데이터 사용이 필요한 경우 테스트 데이터 자동변환 솔루션 및 TDMS(Test Data Management System)를 통해 주민등록번호 등 주요 이용자 정보를 변환하여 운영하고 있으나,

테스트데이터의 생성부터 삭제까지의 절차 및 각 절차별 승인권자, 삭제 검증여부 등에 대해 내규에 상세히 명시하지 않고 있어 사후관리가 체계적으로 이루어지지 않을 우려가 있으므로 테스트데이터의 생성부터 파기까지 주기별 절차를 내규상 명확히 작성하여 관리가 체계적으로 이루어지도록 개선할 필요가 있음

(10) 정보처리시스템 성능 모니터링 불합리

내규에 따라 정보처리시스템의 장애를 예방하고 가용성을 보장하기 위해 성능모니터링 솔루션을 도입하여 상시 모니터링하고, 매월 주요 서버·네트워크 등에 대한 사용현황 및 추이분석 등의 정기적인 예방점검 활동을 수행·보고하고 있으나,

매월 수행하는 주요 서버·네트워크 등에 대한 사용현황 및 추이분석은 당월 1개월간의 정보만을 분석하여 시스템 자원 증설 등의 조치가 필요한 시점을 적시에 판단하기 어려울 우려가 있고 정보처리시스템 등에서 발생한 이상징후(알람) 및 조치내역에 대해서는 별도로 분석·보고하고 있지 않아 이상징후가 발생하였음에도 장기간 미조치될 우려가 있으므로

정보처리시스템에 대한 성능·용량 분석 시 주요 지표의 장기간 추이변화를 분석하여 적절한 대응방안을 마련·보고하고, 이상징후(알람)에 대한 조치내역 등도 정기보고에 포함하는 등 정보시스템 성능 모니터링 업무를 강화하시기 바람

(11) 이상금융거래탐지 시스템(FDS) 운영 불합리

전자금융서비스(기업금융 플랫폼 서비스)를 도입하면서 이상금융거래탐지 시스템을 도입(2022.5월)하고, 이상금융거래 기준(룰셋) 및 로그 보관기관 등 이상금융거래탐지에 대한 기준을 마련해놓고 있으나,

관련 매뉴얼에 이상금융거래탐지 시스템(FDS)의 운영근거만을 기재하여 운영하고 있어, 이상금융거래탐지 시스템(FDS) 관련 정책이 체계적으로 관리되지 못할 우려가 있으므로 이상금융거래탐지 시스템에 대한 이상금융거래 기준 및 기타 운영방침 등에 대한 상세 내용을 내규상 명시하여 관리할 필요가 있음

(12) 전산원장 잔액대사 통제 불합리

내규에 따라 여신원장의 계정금액과 계정별 잔액원장 금액의 일치여부에 대해 내부업무시스템(EXIMIS - 부서마감관리)을 통해 실시간으로 점검하여 일치내역이 확인된 경우에 한해서만 부서마감처리를 수행하고, 매월 여신통계 수행작업을 통해 여신통계와 계정과목·통화별 잔액 일치여부를 검증하고 있으나,

매월 수행하는 여신통계 수행작업은 내부업무시스템(EXIMIS–부서마감관리)이 아닌 일괄작업 스크립트로 수행하고 있어 전산원장 불일치* 내역에 대한 관리가 수기로 통제되고 있는 등 불일치 내역에 대한 사후관리가 체계적으로 관리되지 않고 있으므로

* 검사대상기간 중 잔액대사 불일치 내역은 없었음

월별 여신통계와 계정잔액 원장간의 잔액 검증작업 및 불일치 내역에 대한 사후관리를 시스템화하고, 전산원장 불일치가 발생할 경우 원인 및 조치내역을 시스템에 기록·관리하도록 전산원장 잔액대사 업무를 개선하시기 바람

(13) 전산자료 백업 및 소산업무 불합리

내규에 따라 전산자료의 중요도 및 보관주기 등을 고려하여 전산자료 백업 및 소산을 수행하고 주기적으로 백업 및 소산자료에 대한 적정성 등을 검증하고 있으나,

접근통제시스템 등 관련 전산자료를 별도 백업·소산하지 않아 비상상황 시 정보처리시스템 복구작업이 원활하게 수행되지 못할 우려가 있고, 소산센터(내화금고)에 소산 중인 백업테이프를 이용한 복구 테스트 및 정합성 검증을 비정기적으로 수행하고 있는 등 전산자료의 백업·소산 및 관리 업무가 다소 불합리하게 운영되고 있으므로

접근통제시스템 등에 저장된 중요 전산자료도 백업·소산될 수 있도록 백업·소산 대상을 재검토하여 확대하고, 정기적으로 소산된 백업테이프의 정합성을 검증하는 등 백업·소산 관리체계를 개선하시기 바람

(14) 오픈소스 프로그램 통제 불합리

검사착수일(2022.11.25.) 현재 전산시스템 개발 등을 위해 업무용 오픈소스 프로그램*을 다수 도입·운영하고 있으나,

* Apache, Tomcat, Postgres(DB), MySql(DB) 등

오픈소스 프로그램 사용에 대한 관리주체, 기준, 절차 등의 관리체계가 마련되어 있지 않고, 오픈소스 사용 현황 등에 대해 정기적으로 점검·관리하는 등의 통제 절차도 마련되어 있지 않아 오픈소스 프로그램 관련 운영 리스크가 발생할 우려가 있으므로

오픈소스 프로그램에 관한 도입·활용·유지보수 등 전반에 걸친 오픈소스 관리체계(내규, 절차 등)를 마련하고 오픈소스 프로그램 사용현황 등을 점검·관리하는 등 오픈소스 프로그램 통제 및 관리를 강화하시기 바람

(15) 정보유출 방지대책 불합리

① 내규에 따라 중요 전산자료 보호 및 정보유출 방지를 위해 보안USB 및 매체제어솔루션을 구축하여 저장매체를 통제하고 망연계솔루션*을 통해 내·외부망간 자료전송 내역 등을 관리하고 있으나,

* 업무용 단말기와 인터넷 단말기간 전산자료 송수신 기능 수행

보안USB를 이용하여 별도 승인절차 없이 자료이동이 가능하고 보안USB 사용 내역에 대한 적정성을 점검하고 있지 않아 내부자료가 임의로 반출될 우려가 있으며

업무용 단말기에서 인터넷 단말기로 자료전송 시 개인정보 외 전산자료에 대해서는 책임자의 승인절차가 마련되어 있지 않고, 개인정보가 포함된 전산자료는 자가승인(팀장 이상)이 가능하도록 보안정책을 운영하는 등 내·외부망간 자료전송에 관한 승인 절차가 다소 미흡하므로

보안USB, 망연계솔루션 등을 통한 전산자료 반출시 책임자의 승인을 득하도록 하고 자가승인에 관한 보완대책을 마련하는 등 전산자료 반출 관련 승인 절차를 강화하고 반출 내역에 대한 모니터링 방안을 마련하시기 바람

② 내규에 따라 업무상 연결이 필요한 특정 웹사이트에 대하여 정보보호위원회의 심의 등을 거쳐 망분리 예외대상으로 지정*하고 내부 업무용 단말기에서의 접속을 허용하고 있으나,

* 자체 위험성 평가, 정보보호위원회 승인 등 망분리 대체 정보보호통제 절차 준수

Ⓐ 등 일부 사이트를 업무망에서 허용하는 등 망분리 예외 정책을 다소 과도하게 운영하고 있으므로

업무용 단말기에서 인터넷 접속이 허용되는 사이트에 대한 필요성을 재검토하는 등 망분리 예외 정책을 재정비하시기 바람

(16) IT 및 정보보호 내규관리 강화

내규에 따라 IT 및 정보보호 부문의 효율적인 조직 운영과 업무수행을 위하여 총 5개 내규*를 마련하여 IT 및 정보보호 업무처리 기준과 절차 등을 규정하고 있으나,

* (IT) IT업무규정, IT업무세칙, IT업무기준 / (정보보호) 정보보호세칙, 정보보호기준

IT 및 정보보호 내규에 전산원장 통제, 일괄작업 통제, 외부주문에 대한 기준, 이용자정보 조회·출력 통제, 취약점의 위험 수용 등 IT 내부통제에 관한 사항이 일부 누락되어 IT 및 정보보호 정책에 관한 임직원의 준수 근거가 부족하고 업무처리의 일관성이 결여될 우려가 있으므로

IT·정보보호 관련 중요 내부통제 정책과 절차 등을 내규로 마련하고, 동 지침에 근거하여 업무를 수행할 수 있도록 IT 및 정보보호 내규관리 체계를 강화하시기 바람

(17) 운영체제 등 시스템 소프트웨어 관리 불합리

내규에 따라 안정적인 시스템 소프트웨어 운영을 위하여 유지보수업체 등으로 하여금

정기적으로 해당 제품의 보정(patch) 정보를 제공받아 점검·적용하는 등 운영중인 시스템 소프트웨어를 최신상태로 유지·운용하고 있으나,

검사종료일(2022.12.15.) 현재, 가동 중인 시스템 총 ㉮대 중 ㉯대에서 제조사 기술지원이 종료된 운영체제(OS) 및 데이터베이스(DBMS)를 사용하고 있어 동 시스템 소프트웨어에 대한 신규 취약점 보완 및 기능개선 등을 위한 보정(patch) 작업 및 기술지원이 원활하게 수행되지 못할 우려가 있으므로

기술지원이 종료된 시스템 소프트웨어를 상위 버전으로 업그레이드 혹은 교체하거나 제조사 등과 기술지원 확약을 체결하는 등 시스템 소프트웨어 장애발생을 미연에 방지하기 위한 구체적인 대응 계획을 마련하여 조속히 이행할 필요가 있음

(18) 단말기 보안관리 및 통제 불합리

내규에 따라 사용자 단말기 內 악성코드 감염 및 정보유출 방지 등을 위해 사용자는 인가된 프로그램만 사용하도록 규정하고 네트워크 접근통제(NAC) 시스템을 통하여 단말기 보안프로그램*을 설치·운영하고 있으나,

* 백신(V3), 문서보안시스템(DRM), AD(Active Directory), 출력물보안(PrintChaser), 개인정보검출(Privacy-i) 등

사용자 단말기에 설치된 비인가 프로그램 현황을 주기적으로 점검하고 있지 않아 일부 단말기에서 업무상 불필요한 프로그램이 설치된 사례가 있는 등 보안에 취약한 프로그램 등이 임의로 설치될 우려가 있고

네트워크 접근통제(NAC) 시스템의 보안정책을 차단이 아닌 탐지모드*로 운영하고 있어 필수 보안프로그램이 설치되지 않은 단말기가 내부망에 연결될 위험이 있으므로

* 내부 네트워크로 접속하려는 단말기에 사내 보안프로그램이 설치되지 않은 경우 설치 권고 (보안프로그램을 설치하지 않아도 네트워크 연결을 차단하지 않음)

사용자 단말기에 설치된 비인가 프로그램 현황을 주기적으로 점검하도록 업무절차를 강화하고 내부 네트워크로 접속하려는 단말기에 대해 보안프로그램의 정상 설치 여부를 검증하도록 네트워크 접근통제(NAC) 시스템을 개선하시기 바람

(19) 정보처리시스템 개인정보 점검·관리 불합리

① 내규에 따라 개인정보 유출로 인한 보안사고 등을 방지하기 위하여 개인정보 현황을 주기적으로 점검*하고 있으나,

* 매년 개인정보보호위원회의 개인정보 관리수준 진단 절차에 따라 업무용 PC, 데이터베이스 등에 대한 개인정보 점검을 수행

Ⓑ 등에서 생성되는 파일에 이용자 정보가 포함되어 있는지 점검하지 않고 있어 주요 정보처리시스템에 이용자 정보 등이 평문으로 보관될 위험이 있으므로

Ⓑ 등 정보처리시스템에 대한 개인정보 점검기준 및 방법을 마련하여 정기적인 점검 활동을 수행하는 등 개인정보 점검 실효성을 강화하시기 바람

② 내규에 따라 데이터 표준화 및 DB구조 관리 등을 위해 데이터 속성, 코드, 표준 용어 등을 정의*하는 메타시스템을 운영하고 있으나,

* DB테이블 컬럼(Column), 속성명, 데이터 타입·길이 등 기준정보 관리

메타시스템에서 개인정보 및 비밀번호 등을 식별·관리*하지 않아 암호화 대상에 대한 일관성 있는 관리 및 통제가 어려워 업무시스템 개발·운영 시 암호화 및 마스킹 처리가 누락될 위험이 있으므로

* DB 컬럼(Column) 별로 주민등록번호, 계좌번호, 비밀번호 등을 식별하여 '암호화·마스킹 대상'으로 지정

메타시스템에서 개인정보 및 비밀번호 컬럼(Column)을 중요 데이터 항목으로 관리하고 업무시스템 개발·운영 시 메타시스템에서 관리하는 개인정보를 기준으로 암호화, 마스킹 처리할 수 있도록 관련 업무절차와 시스템을 개선하시기 바람

(20) 전산자료 보호대책 불합리

① 내규에 따라 사용자 단말기에서 생성·저장되는 전자문서의 암호화 등을 위해 문서보안시스템(DRM)을 구축하여 주요 문서* 등은 자동 암호화되도록 관리하고 있으나,

* MS-Office 문서(엑셀, 워드, 파워포인트), 한글, PDF 등

이미지파일, 텍스트파일(txt, csv) 등은 암호화 대상에서 누락되어 있고, 전자문서 복호화에 관한 자가승인 정책을 운영하면서도 복호화된 문서에 대한 일괄 암호화를 수행하지 않는 등 문서보안 관리통제가 다소 미흡하므로

문서보안시스템(DRM)의 암호화 적용대상을 이미지파일, 텍스트파일 등으로 확대하고, 복호화된 전자문서를 정기적으로 검색 및 암호화하며 자가승인에 관한 보완대책을 마련하는 등 문서보안시스템(DRM)의 전자문서에 대한 관리·통제를 강화하시기 바람

② 내규에 따라 임직원간 업무자료 공유 등을 위해 업무용 보안파일서버를 구축·운영*하고 있으나,

* 부서별로 폴더를 생성하여 업무자료를 공유하며, 사용자 권한을 관리하고 사용 이력을 기록·보관

전자문서를 보안파일서버에 저장 시 문서보안시스템(DRM)을 통한 파일 암호화가 적용되지 않아 전산자료가 평문으로 보관될 위험이 있으며, IT 프로젝트관리 등 일부 업무에 대해서는 '네트워크 결합 스토리지(NAS)*'를 이용하여 전산자료를 공유하고 있어 사용자 권한관리 및 사용이력 기록·관리 등이 미흡하므로

* Network-Attached Storage : 네트워크를 통해 전산자료를 공유할 수 있는 대용량 저장 장치

업무자료를 보안파일서버에 저장 시 파일 암호화가 적용되도록 시스템을 보완하고, IT 개발·운영 업무를 위한 자료공유도 보안파일서버와 동등한 수준으로 통제되도록 관련 절차 및 시스템을 개선하시기 바람