경영유의사항 등 공개안

1. 금융기관명 : ㈜하나은행

2. 제재조치일 : 2025. 8. 28.

3. 제재조치내용

제재 대상	제재 내용
기관	• 경영유의사항 14건
	• 개선사항 49건

4. 제재대상사실

가. 경영유의사항

(1) 내부자본 한도관리 관련 업무절차 강화

은행은 내부자본의 효율적 관리와 원활한 업무수행을 위하여 내규 「RM2 내부자본」를 운영하고 있다. OOO위원회는 동 내규에 따라 내부자본의 총 한도, 리스크 유형별 한도 및 사업그룹별 한도의 설정 및 변경에 대한 사항을 결의하며, ▶▶▶는 한도 준수 여부를 확인하고 한도 소진율을 모니터링 지표로 설정하여 점검하여 이를 매월 OOO위원회, 매분기 OOO위원회에 보고한다.

그러나 은행의 내부자본 한도관리 업무절차 중 모니터링 지표의 단계별 업무절차와 한도초과 예상 시 업무절차 간 상충가능성이 있고, 내부자본 적정성 비상계획 단계별 업무절차 및 사업그룹별 한도초과 예상 시 대응절차가 구체적으로 마련되어 있지 않다.

<조치할 사항>

따라서 은행은 비상계획 업무절차의 한도 임계치를 조정하여 업무절차 간 일관성을 확보하고, 조기경보체계의 취지에 맞도록 단계별 업무절차를 구체화하며, 사업그룹별 한도초과 예상 시 업무절차를 내규에 명확화하시기 바랍니다.

(2) 부동산 PF 사업성 평가 절차 강화

은행은 관련 내규 및 모범규준 등에 따라 분기별로 부동산 PF여신에 대한 ①사업성 평가를 진행하고, 동 결과를 ②자산건전성 분류와 연계하고 있다.

그러나 ①은행 내규에 사업성 평가기준이 명확하게 규정되어 있지 않고, ②모범규준상 평가기준을 엄정하게 적용하지 않는 등 평가가 관대하게 이루어지는 경향이 있으며, ③평가 결과에 대한 근거가 기록·보관되지 않으므로 동 평가 업무체계를 강화할 필요가 있다.

<조치할 사항>

따라서 은행은 부동산 PF 사업성 평가 관련 평가기준 및 근거를 명확히 하고, 평가내용을 문서화하여 보관하는 등 동 평가 업무체계를 강화하기 바랍니다.

(3) 브릿지론 취급절차 강화

은행의 2023. 9월말 기준 PF 브릿지론 잔액은 약 □조 □□□억원(□□개 사업장)으로 전년말(□,□□□억원) 대비 +□,□□□억원 증가(□□□.□%↑)하는 등 자산규모가 급격히 성장하고 있다.

그러나 이 중 □,□□□억원(□개 사업장)에서 인허가 지연·사업계획 변경 등으로 사업이 지연되거나 대출만기가 연장되는 등 리스크가 심화되고 있다.

<조치할 사항>

따라서 은행은 PF 브릿지론 관련 리스크를 철저히 관리할 수 있도록 PF 브릿지론 취급 가이드라인을 마련하여 신규 취급 및 연장 절차를 강화하시기 바랍니다.

(4) 신용 위험가중자산 관리체계 개선

은행은 매년말 차년도 사업계획에 따라 신용 위험가중자산(이하 '신용RWA') 관리목표를 설정하고 이를 사업그룹별로 배분하여 각 그룹별 신용RWA 관리목표를 수립·관리하며, 각 그룹별 신용RWA 사용 현황 등을 OOO위원회에 정기적으로 보고하고 있다.

그러나 신용RWA 관리목표 설정, 현황 보고, 관리목표 초과 시 대응계획 등 관련 업무에 대한 내규가 마련되어 있지 않고, 관리목표 초과 시 해당 그룹이 신용RWA 감축계획을 자체 수립하여 리스크부서 실무자와 협의하는 등의 관리 절차를 운영하고 있지 않으며, 은행과 사업그룹별 신용RWA 관리목표 초과 상황도 빈번히 발생하는 등 관리체계가 미흡하다.

<조치할 사항>

따라서 은행은 신용RWA 관리목표 설정, 현황 보고, 관리목표 초과시 대응 절차 등에 관한 사항을 내규로 명문화하고, 관리목표 초과 예상 시 목표준수 방안 등을 마련하며, 관리목표 초과 시 세부관리 방안 등을 OOO위원회에 보고하는 등 신용RWA 관리를 강화하시기 바랍니다.

(5) 자금용도외유용 확인 및 관리 강화

은행은 내규 「LA8.3 자금용도의 사후점검」에 의거하여 원화기업대출의 용도외 유용 여부를 점검하고 있고, 내규 「LB21.1」에 의거하여 외화대출의 실수요 자금 여부를 점검하고 있다.

그러나 외화대출의 경우 해외 실수요 자금 여부를 대출 취급 담당자의 상급자가 별도로 확인하는 절차가 없으며, 대출 취급 후 증빙서류와 용도외유용 여부를 점검하지 않고 있다.

또한 용도외유용 점검 부서가 여신 감리부서에 용도외유용 모니터링 결과를 제공하고 있지 않으며, 여신 감리과정에서도 여신의 상환능력 위주로 점검하고 있어 대출의 용도외유용에 대한 감리가 미흡하다.

<조치할 사항>

따라서 은행은 외화대출 실수요 증빙 확인과 자금의 용도외유용의 사후점검 프로세스를 도입하고, 대출 용도외유용 사후점검 모니터링 결과를 여신 감리 부서에 제공하며, 기업대출 용도외유용에 대한 특별감리를 정례화하는 등 대출의 용도외유용 관리체계를 개선하시기 바랍니다.

(6) 담보인정비율 산정기준 명확화

은행은 여신 취급 한도 및 금리 결정, 자산건전성 분류와 대손충당금 산출 등에 활용되는 담보인정비율을 명확한 원칙과 기준에 따라 산정하고 운용의 적정성을 주기적으로 점검해야 한다.

그러나 은행은 담보인정비율을 산정 및 고시하는 방법 등에 관한 내규 없이 업무관행에 따라 산정 및 고시하고 있고, 오류 산출이나 자의적인 담보인정비율 조정 등의 위험을 방지하기 위한 검증 절차가 마련되어 있지 않다.

<조치할 사항>

따라서 은행은 담보인정비율의 산정 방법과 고시 주기, 지역·용도 구분 기준, 전결권 등을 내규에 명문화하고, 담보인정비율에 대한 주기적인 적정성 점검방안을 마련하는 등 담보인정비율이 합리적으로 운용될 수 있도록 유의하시기 바랍니다.

(7) 국외 영업점 전담감정기관에 대한 점검 강화

은행 내규 「LH1 국외여신의 일반원칙」에 따라 국외 영업점은 □개 이상의 전담감정기관을 심사부서의 사전 승인 후 담보물의 감정을 실시하고, 연 □회 전담감정기관에 대한 점검을 실시해야 한다.

그러나 명문화된 점검 기준이 없어 각 영업점은 자체 기준에 따라 감정기관의 규모·인원·재무제표 등 형식적인 항목만 점검하는 한편, 과거 감정사례 검토 등 감정오류 방지를 위한 점검절차가 미흡하고, 영업점 점검 결과에 대한 본부 차원의 점검 절차가 없는 등 사후관리 절차의 실효성이 미흡하다.

<조치할 사항>

따라서 은행은 국외 전담감정기관에 대한 통일된 점검기준을 마련하고, 점검결과에 대한 본부 주도의 정기점검을 실시하는 등 전담감정기관이 적절하게 운용될 수 있도록 관련 업무에 유의하시기 바랍니다.

(8) 유가증권 자산건전성 분류의 적정성 검증 강화

은행은 「은행업감독규정」 제27조에 따른 자산건전성 분류 시 적정성·객관성 확보를 위하여 독립된 검증기능 유지 등 건전성 분류 관련 내부통제체제를 구축하여 적정히 운영하여야 한다.

그러나 일부 유가증권에 대해서는 OOO부 등 취급 부서에서 수기로 건전성을 분류함에 따라 시스템을 통한 건전성 분류 사유 및 근거를 확인하기 어려워 분류 적정성에 대한 제3자 검증이 제한적이며, 착오 분류의 위험도 있다.

<조치할 사항>

따라서 은행은 전산화한 시스템을 통해 유가증권 자산건전성 분류 업무를 수행하여 적정성 검증에 필요한 분류 근거 등을 명확히 하고 검증을 강화하는 등 관련 업무절차를 개선하시기 바랍니다.

(9) 가계대출 총량관리 내부통제 체계 강화

은행은 「가계대출 총량관리 내부통제」 매뉴얼에 따라 가계대출의 건전성을 관리하기 위해 분기마다 가계대출 관리계획, 총량관리 이행현황, 예상리스크 등 중요사항을 경영협의회에 보고하고, 사전에 정해진 한도소진율에 따라 유관부서와 협의하여 단계별 비상조치계획을 수립하고 이행해야 한다.

그러나 매뉴얼 이행을 위한 내부통제절차 및 전결기준이 은행 내규에 명문화되어 있지 않고, 상품수준별 관리방안이 마련되지 않았으며, 담보대출 등 일부 상품의 대출잔액이 관리목표를 초과하는데도 실무협의회 개최 등 매뉴얼에 따른 조치가 실시되지 않았다.

또한 은행은 2022. 4분기 ~ 2023. 2분기 기간중 경영협의회 보고를 하지 않거나(총 □회), 보고한 경우에도 상품별 관리목표·한도소진율 등 필수정보 없이 단순 총량기준의 대출실적만 보고하였다.

<조치할 사항>

따라서 은행은 총량관리 매뉴얼 운영에 대한 근거를 내규에 반영하고, 총량관리 방안을 상품수준별로 마련하며, 정기적으로 가계대출 총량관리 실무협의회를 개최하여 논의사항 등을 경영협의회에 충실히 보고하고, 이에 따라 상품별·채널별 비상조치계획을 실행하는 등 가계대출 총량관리를 위한 내부통제 업무를 충실히 운영하시기 바랍니다.

(10) 자기자본투자 모니터링 및 사후관리 강화

은행은 내규 「투자관리세칙」에 따라 자기자본투자 현황을 매 반기별로 OOO위원회 등에 보고하고, 손실 허용한도 초과 시 OOO위원회에 보고하여 매각 등 사후관리 방안을 논의해야 한다.

그러나 은행은 자기자본투자 현황 보고 시 직접·간접투자로만 구분한 투자현황, 거액 신규 승인내역, 손실 허용한도를 초과하는 건 등에 대해서만 보고하고 있을 뿐 포트폴리오 세부 현황에 대한 상세 모니터링 및 관련 보고를 수행하고 있지 않다.

또한 손실 허용한도 이외의 별도 모니터링 기준이 없어 투자 대상의 부실 징후를 조기에 인지하고 적시성 있게 대응하기 어렵다.

<조치할 사항>

따라서 은행은 자기자본투자 현황 모니터링 및 관련 보고 시 상세 포트폴리오 현황을 반영하도록 운영하며, 부실 징후를 조기에 인지하고 보고할 수 있도록 세부 시나리오·등급 등 모니터링 기준 및 단계별 조치사항 등을 마련·운영함으로써 자기자본투자 모니터링 및 사후관리를 강화하시기 바랍니다.

(11) OOO위원회 운영 강화

은행 내규「내부통제규정」등에 따라 임직원의 내부통제 관심 및 의식향상, 은행내 금융사고와 부당한 업무처리 발생 예방을 위하여 그룹장으로 구성된 OOO위원회를 구성하여 운영하고 있으나 아래와 같이 미흡한 점이 확인되었다.

㉮ OOO위원회 위원의 확대 필요

정부·금융기관 등 고객 관리·단기금융업무 및 지역내 영업추진 지원 등을 담당하여 OOO위원회에서 논의되는 안건과 밀접한 업무 연관성이 있는 △△△장, ▽▽▽장 등(이하 '☆☆☆장')이 위원에 포함되어 있지 않아 위원회 운영의 효율성이 저해될 우려가 있다.

㉯ OOO위원회 위원의 회의 참여도 제고

2023년 개최된 □차례 위원회에 ◎◎◎장 등 일부 위원들이 특별한 사유가 없음에도 동 위원회에 불참한 사실이 있다.

<조치할 사항>

따라서 은행은 앞으로 OOO위원회에 ☆☆☆장을 위원으로 포함시키고, 위원들이 직무 수행상 불가피한 경우를 제외하고는 동 위원회에 참여하게 하는 등 관련 운영 업무를 강화하시기 바랍니다.

(12) 자금관리업무 관련 내부통제 강화

은행은 영업점이 업무수탁자 또는 대리인의 지위에서 계약상대방이 제시하는 자금이체요청서에 의해 자금을 집행하고 집행내역을 관리 및 통지하는 등의 업무(이하 '자금관리 업무')를 수행하고 있으며,

동 업무를 수행하는 과정에서 발생할 수 있는 위험요인을 관리할 수 있도록 자금인출 증빙서류 수신 및 보관방법, 자금인출요청서 진위여부 확인방법 등의 업무절차를 마련하고 준수 여부를 점검할 필요가 있다.

하지만 은행은 동 업무와 관련한 구체적인 업무절차를 마련하지 않고 있고, 자금인출요청서를 부점 공용메일로 수령하지 않거나 전산시스템에 등재하지 않는 등 자금관리 업무 관련 내부통제상 미흡한 점이 확인되었다.

<조치할 사항>

따라서 은행은 자금인출요청서 위변조 방지를 위한 자금인출 증빙서류 수신

및 보관방법 등을 포함한 자금관리 업무 관련 절차를 마련하고, 자금관리 계약을 관리하기 위한 전산상 통제를 강화하는 한편, 명령휴가 및 자점감사 등을 통해 업무절차 준수여부를 점검하는 절차를 마련하시기 바랍니다.

(13) 금리리스크 관리방안 마련

2022년 이후 시장금리 상승에 따른 요구불예금 감소, 고정금리대출 증가 등의 영향으로 은행의 기본자본 대비 금리리스크량(△EVE) 비율이 지속적으로 높은 수준을 유지함에 따라 은행은 이를 관리하기 위해 2023. 7월부터 기본자본 대비 금리리스크량 비율을 한도관리 지표로 추가하고 한도를 □.□%로 설정하였다.

하지만 동 한도는 금리리스크량(△EVE) 비율의 하향을 유도하기에는 실효성이 부족하며, 이로 인해 한도관리 지표에 추가된 이후에도 기본자본 대비 금리리스크량 비율은 지속적으로 높은 수준을 유지하고 있다.

<조치할 사항>

따라서 은행은 실효성 있는 한도 설정을 통해 중·장기적으로 기본자본 대비 금리리스크량(△EVE) 비율을 관리하고, 단기적으로는 동 비율을 완화하기 위해 자산·부채 듀레이션갭을 축소하는 등 금리리스크 관리 계획을 마련하여 금리리스크 지표를 안정적으로 관리하시기 바랍니다.

(14) 정보기술부문(IT) 감사업무 강화

㉮ IT검사역 전문성 강화

은행 내규「감사규정」에 따르면 ♥♥♥는 ♠♠♠의 효율적인 업무수행을 위한 본부단위의 보조기구로서, 원활한 감사업무를 수행할 수 있는 전문성 있는 인원과 적정인원을 유지하여야 한다.

또한 전문성이 있는 인원을 유지하기 위해 내규에 따라 검사역은 감사업무를 수행하는데 필요한 지식과 경험을 가지고 있는 자 또는 해당 업무 분야에서 □년 이상 근무한 경력이 있는 자를 임명함을 원칙으로 하고 있다.

그러나 검사종료일(2023. 12. 8.) 현재 ♥♥♥ 산하 ♣♣♣에 두고 있는 IT전담 검사역 □명 중 □명을 제외한 나머지 □명의 검사역은 IT업무 분야에서의 경력이 전무하거나 □년 미만(□년 □개월)으로 IT업무 수행 경험이 적어 IT감사의 실효성과 전문성이 저하될 우려가 있다.

<조치할 사항>

따라서 은행은 IT감사업무의 원활한 운영 및 IT부문의 내부통제 강화를 위해 IT업무 수행 경험이 있는 적정한 감사인력을 확보하여 IT감사업무의 실효성 및 전문성을 강화하시기 바랍니다.

㉯ 정보처리 위탁업무에 대한 감사 강화

은행은 내규 「♠♠♠규정」에 따라 IT감사를 IT부문의 안전성과 건전성을 평가하는 일련의 과정으로 규정하고, 내규 「감사규정」에 따라 IT 및 정보보안업무에 대해 종합감사 및 수시감사 등 현장감사를 정기적으로 실시하고 있다.

하지만 은행은 계열회사인 ◇◇◇ 등 외부회사에 다수의 정보처리시스템 운영 업무를 위탁하고 있는데도 정보처리 위탁업무에 대해서는 감사를 실시하지 않고 있어, 정보처리업무 제3자 위탁 리스크에 따른 정보처리시스템의 안정성이 저하될 우려가 있다.

<조치할 사항>

따라서 은행은 정기적으로 실시하는 종합감사 및 수시감사 등을 통해 정보처리 위탁계약의 적정성, 위탁업무의 모니터링(서비스수준평가·백업 등 비상대책) 등 정보처리 위탁업무에 대한 감사를 수행할 수 있도록 감사업무범위를 확대·강화하시기 바랍니다.

㉰ IT 자체감사 수행체계 불합리

은행은 내규 「내부통제규정」에 따라 효율적인 내부통제를 위하여 업무의 기능적 분리, 책임의 명확화, 직무간 상호견제와 균형을 이루어야 하며, 해당 부점장의 책임하에 자체감사를 수행해야 한다.

하지만 은행은 ◁◁◁가 총괄하는 ▷▷▷ 산하에 별도의 자체감사조직(팀)인 ♡♡♡을 두고, ◁◁◁의 명령하에 ♧♧♧ 산하 부서의 업무까지 자체감사를 수행하여 ◁◁◁에게 결과를 보고하는 체계로 운영하고 있어, ◁◁◁와 ♧♧♧ 업무 간의 책임 명확성, 상호견제가 불분명해질 우려가 있다.

<조치할 사항>

따라서 은행은 ◁◁◁와 ♧♧♧ 간의 상호견제와 책임의 명확성을 확보할 수 있도록 업무별로 자체감사를 운영하는 등 자체감사 체계에 대해 개선·보완하시기 바랍니다.

나. 개선사항

(1) 사외이사 평가제도 및 ◆◆◆ 운영의 실효성 제고

(가) 사외이사 평가제도 관련 미흡

내규 「사외이사 운영 규정」 등은 사외이사 연임(재임)을 위해 후보를 추천할 경우 사외이사 평가를 통해 업무수행 능력이 '우수'하다는 점이 입증되어야 함을 규정하고 있다.

그러나 객관적 평가지표가 없는 가운데 검사대상기간 중 모든 사외이사에 대한 평가결과가 최고등급으로 도출되는 등 평가의 변별력이 낮아 평가 결과를 사외이사 연임에 활용하겠다는 제도의 취지가 구현되기 어렵다.

(나) 사외이사에 대한 자료제공 미흡

「금융사지배구조법」 제18조 및 동법 시행령 제15조는 은행이 ◆◆◆ 회의자료 등을 회의 개최 2주일 전까지 사외이사에게 제공하되, 은행 정관 또는 ◆◆◆규정 등에서 사전제공 기한을 달리 정할 수 있도록 규정하고 있다.

그러나 은행 내규에 사외이사에 대한 자료 사전제공 시점을 명확하게 규정하지 않았고, 2022년 이후 개최된 ◆◆◆(산하 위원회 포함) 총 □□회 중 □□회(□□.□%)는 회의 개최 □일 전에 자료가 제공되지 못한 사실이 있다.

<조치할 사항>

따라서 은행은 사외이사 평가시 객관성·변별력 제고를 위해 계량화가 가능한 항목에 대해서는 정량평가를 도입하고, ◆◆◆(산하 위원회 포함) 개최 □일전까지 사외이사에게 안건자료가 제공될 수 있도록 관련 내규를 마련하시기 바랍니다.

(2) 은행 고문제도 운영의 합리성 제고

은행은 고위직 출신 퇴임 임원에게 경영활동에 대한 자문을 받을 목적으로 고문(자문위원)제도를 운영하고 있다. 전임 임원의 경영지식 활용이라는 제도의

취지와 고문의 실질적인 영향력 등을 고려할 때 건전한 자격을 갖춘 자가 고문으로 선임되어야 하나, 관련 내규인 「자문위원 운영 규정」상 고문의 자격요건은 추상적·선언적으로 규정되어 있어 자격요건으로 작용하기에 구체성이 미흡하다.

또한 대표이사 출신의 고문에게 높은 수준의 자문료가 지급되고, 고문의 자문 내용이 경영진의 의사결정에 참고될 수 있는 점을 감안할 때, 고문계약 체결이 회사와 주주의 장기적 이익측면에 부합할 수 있는지 여부 등에 대하여 ◆◆◆에서 심의될 필요가 있으나, 현행 내규에는 고문계약 체결에 대한 ◆◆◆ 사전결의 절차가 제도화되어 있지 않다.

<조치할 사항>

따라서 은행은 고문의 자격요건을 관련 법규 및 지주 내규를 준용하여 구체화하고, 대표이사 출신의 고문 선임 시 ◆◆◆ 사전결의를 제도화하시기 바랍니다.

(3) 은행 ◈◈◈위원회 등 소개영업 업무체계 개선

은행은 지주 내 자회사간 영업망을 상호활용하여 시너지를 강화할 목적으로 「관계회사간 손님 소개업무 지침」(이하 '내규')을 두어 소개영업을 영위 중이며, 「소개상품 선정 위원회 규정」(⊙⊙⊙ 내규) 등에 따른 '◈◈◈위원회'(이하 '위원회')를 운영하여 소개상품 및 소개 제한상품을 결의하는 소개영업 업무체계를 갖고 있으나, 아래 (가) ~ (다)의 미흡점이 확인되었다.

(가) 위원회 위원 구성 미흡

위원회 위원 중 은행 소개영업 소관 부서장인 ◐◐◐ 및 준법감시 관련인원이 포함되어 있지 않아 소개영업 관련 내부통제 및 체계적인 관리방안 등이 위원회에서 적정히 논의되기 어렵다.

(나) 위원 출석저조에 따른 위원회 결의기능 약화

위원회 부결요건의 하나로 은행 위원 전원출석·전원반대가 규정되어 있는 등 은행 위원의 참석이 위원회 결의기능 등 운영에 중요함에도 은행 ▣▣▣은 검사대상기간 중 개최된 위원회에 전부 불참한 사실이 있다.

(다) 소개영업 실적에 대한 업무체계성 미흡

위원회가 선정한 '소개 제한 상품'은 소개영업으로 판매되는 경우에도 은행의 소개실적으로 인정되지 않으나 은행 내규에는 이러한 내용이 명시되어 있지 않아 소개실적 인정배제에 대한 업무의 체계성이 미흡하다.

<조치할 사항>

따라서 은행은 ▨▨▨ 등을 위원회 위원에 추가하고, 위원회 위원들의 참석률 제고 및 부결방법 개선을 통해 위원회의 결의기능을 강화하며, 소개실적 불인정 업무 근거를 내규에 명확히 하는 등 소개영업 관련 업무체계를 개선하시기 바랍니다.

(4) 직원 성과평가지표(KPI) 관리 강화

은행 내규「영업점 종합경영평가 세칙」은 특정 금융상품 판매실적 등과 직원 성과평가지표(KPI)가 연계되는 것을 방지하도록 규정함으로써 직원성과 평가지표 수립 시 특정 상품·서비스에 대한 과도한 가점이 배정되어 불건전영업행위가 유발될 가능성을 관리하고 있다.

그러나 본점 및 영업점에 대한 성과평가지표에 대해 영업과 무관한 제3자를 통한 점검 또는 평가지표에 대한 사전협의 등 검증절차를 마련하지 않아 불건전영업행위 방지를 위한 성과평가지표의 관리·통제체계가 미흡하다.

<조치할 사항>

따라서 은행 ▤▤▤ 등에서 성과평가지표와 특정 상품 판매실적과의 연계에 따른 불건전영업행위 유발 가능성 등을 정기적으로 평가하고, 그 평가결과를 OOO위원회 등에 보고토록 개선하는 등 성과평가지표 관리를 강화하시기 바랍니다.

(5) 임원 장기성과 평가지표 개선

은행은 지주 내규「하나금융그룹 보수 및 성과평가 규정」등에 따라 임원

성과평가 시 장기성과와 수익성, 건전성이 중요하게 반영될 수 있도록 성과평가지표를 적용하고, 리스크 연계를 위해 건전성 관련 지표를 일정 수준 이상 반영하여야 한다.

그러나 은행이 임원의 장기성과급(성과연동주식)을 결정함에 있어 총 3개의 장기성과지표(수익성·주가·건전성)만을 사용하고 있으면서도 건전성 비중이 수익성 및 주가에 비해 상대적으로 낮은 경향이 있어, 임원이 장기적으로 지주의 건전성을 제고하도록 유도하기에 미흡하다.

<조치할 사항>

따라서 은행은 임원이 단기적 수익만이 아닌 장기적 측면에서 지주의 건전성 제고 노력을 기울일 수 있도록 장기성과 지표 내 건전성 지표 비중을 현행보다 상향하시기 바랍니다.

(6) 내부통제 혁신방안 등 금융사고 예방대책 추진 미흡

은행은 내규「내부통제규정」및「금융사고 예방요령」등에 따라 금융사고 예방을 통한 내부통제 업무를 수행해야 하고 '국내은행 내부통제 혁신방안'(2022. 11. 14.)에 따라 장기근무자 관리, 명령휴가 운영 및 직무분리 등을 실효성 있게 추진하여야 하나 아래 (가)~(라)의 미흡점이 확인되었다.

(가) 고위험 업무 직무분리 관련 미흡

은행은 내규「내부통제규정」등에 따라 고위험 업무의 세부직무를 분리하고 동일인이 해당 세부직무를 겸직하지 못하도록 하되, 직원이 □명 이하인 소규모 부점의 경우에는 부점장의 판단하에 예외적으로 이를 허용하고 있다. 또한 준법감시부서는 직무분리 실시현황을 상시점검하고 필요한 경우에는 해당 부점장에게 개선을 요구해야 한다.

그러나 부점장의 판단하에 겸직을 예외적으로 허용하는 경우 해당 부점에서는 ▤▤▤에 대한 별도 통보 없이 업무별 소관부서와 사전협의한 후 ▥▥▥에 겸직금지 전산제어 해제 요청을 하고 있어 ▤▤▤가 전체 부점에 대한 겸직 여부 및 적정성을 적시에 확인하기 어렵다.

또한 직무분리 관리시스템을 인사관리시스템에 통합 운영하고 있어 직무분리 적정성 점검 시 ▥▥▥ 제공자료를 활용하고 있으나 겸직 적정성을 '수기'로 확인하는 등 효율성이 낮다.

(나) 내부고발제도 관련 내규 미흡

1) 관련 법규 요구사항의 내규 반영 미흡

「금융회사 지배구조 감독규정」 제11조 등은 은행에 '내부고발자 제도의 운영'에 관한 내부통제기준 마련의무를 부여하고, 회사에 중대한 영향을 미칠 수 있는 위법·부당한 행위를 인지하고도 회사에 제보하지 않는 사람에 대한 불이익 부과 등 동 내부통제기준에 포함되어야 할 내용을 규정하고 있다.

그러나 은행은 내부고발 관련 내규인 「내부직원 고발 및 고발자 보호에 관한 규정」에 위법·부당한 행위를 알고도 회사에 제보하지 않는 사람에 대하여 불이익을 부과하는 내용을 적정히 반영하지 않았다.

2) 내부고발자 포상금 지급기준 구체성 부족

은행 내규 「내부직원 고발 및 고발자 보호에 관한 규정」 [별표 1]에는 포상이 가능한 내부고발 종류를 명시하고 있으며 포상과 관련하여 부정행위 신고의 경우 '손실방지 기여액'을 기준으로 포상금을 산정토록 규정하고 있다.

그러나 내부고발 대상인 직무분리와 같은 사고예방 조치 소홀 또는 상사의 위법·부당한 지시 등의 경우에는 '손실방지 기여액' 산정이 모호하여 포상이 이루어지지 않을 우려가 있어 이에 대한 임직원의 내부고발 유인이 부족하다.

(다) 동일부서 장기근무자 인사관리 체계 관련

1) 채무·투자현황 확인 업무 미흡

은행은 내규 「장기근무 관리매뉴얼」 제5조에 장기근무가 필요한 경우 긴급한 업무처리 등 장기근무의 불가피성, 채무·투자현황 확인 등을 통한 사고위험 통제 가능성 등 확인하여야 할 내용을 규정하고 있다.

그러나 장기근무 승인을 받은 대상자 중 일부에 대하여만 채무·투자현황을 확인하여 상기 확인의무를 미흡하게 이행한 사실이 확인되었다.

또한 채무·투자현황을 확인한 경우에도 금융투자 여부(Y/N)만을 파악하고 구체적인 투자현황 파악은 이루어지지 않는 등 사고위험 통제 가능성을 확인하기 위한 동 제도의 실효성이 부족하다.

2) 장기근무자 비율 관리 미흡

내규 「장기근무 관리매뉴얼」에서 장기근무자는 순환근무 대상 직원 중 □% 이내 또는 □□명 이하로 관리하도록 규정하고 있다.

그러나 장기근무자 관리 비율이 2023.2분기 인사 이후 새롭게 장기근무자로 분류될 직원의 증가로 상승 추세에 있는 등 관리 비율의 안정적 관리가 이루어지지 않을 우려가 있다.

(라) 명령휴가제도 운영 업무 미흡

1) 명령휴가 실시대상자에 대한 감사 대상 기간 개선

은행은 내규 「금융사고 예방요령」에 명령휴가 실시대상자에 대한 직무감사 대상 기간을 □개월로 규정하고 있으나, 명령휴가를 연 □회 실시하고 감사기준일 □개월 이전의 미흡 사항은 확인하지 못하는 등 직무감사 수행 시 점검 필요사항에 대한 확인이 미흡하게 이루어질 우려가 있다.

2) 명령휴가 실시대상자에 대한 감사 실시 및 사후관리 불철저

은행은 내규 「금융사고 예방요령」에 명령휴가 실시대상자에 대한 직무감사를 □영업일 이상 연 □회 이상 실시하는 등 실시 방식을 규정하고 있다.

그러나 은행은 장기근무직원에게 □영업일 중 □영업일만 직무감사를 실시하고 있고, 점검결과에 대하여도 최소 □일 최대 □□□일 이후 보고하는 등 사후관리가 불철저하다.

3) 위험직무자 선정 불철저

은행은 내규 「금융사고 예방요령」에 ①영업점은 출납·PB·RM 등을, ②본점은 자산운용·자금관리 담당 등을 위험직무자로 분류하도록 규정하고 있음에도, 원화출납(영업점·본점), 자금운용·관리(본점) 일부 직원을 위험직무자 분류에서 누락하였다.

<조치할 사항>

따라서 은행은 (가)고위험업무 겸직 적정성을 적시에 효율적으로 확인할 수 있는 업무절차 및 관련시스템을 마련하는 한편, (나)위법·부당한 행위를 알고도 은행에 제보하지 않는 사람에 대한 불이익 부과 등 고발 관련 법규 요구사항을 내규에 적정히 반영하고, 내부고발자 포상금 지급기준을 구체화하시기 바랍니다.

또한, (다)장기근무자에 대한 채무·투자현황 확인업무 및 장기근무자 비율 관리를 강화하는 한편, (라)명령휴가 감사대상기간을 확대하고, 장기근무자 등 명령휴가 실시대상자에 대한 직무감사 및 사후관리를 충실히 수행하며, 위험직무자 설정업무를 강화하는 등 금융사고 예방 관련 업무를 개선하시기 바랍니다.

(7) 임직원 금융투자상품 매매신고제도 불합리 개선

은행은 「자본시장과 금융투자업에 관한 법률」(이하 ‘「자본시장법」’)에 따라 임직원의 미공개중요정보 이용행위 등 불공정거래행위 및 투자자와의 이해상충을 방지하기 위하여 내규 「임직원의 금융투자상품 매매신고 및 관리 세칙」(이하 ‘내규’)을 마련하였으며 이에 따라 신고대상 임직원은 금융투자상품 매매거래 시 거래의 규모·횟수 제한, 본인의 실명계좌를 통한 거래 등을 준수하도록 규정하고 있으나 아래 (가)~(나)의 미흡점이 확인되었다.

(가) 금융투자상품 매매 신고대상 임직원 기준 모호에 따른 대상자 누락

△△△ 등 금융투자업직무 및 ▽▽▽ 등 미공개 중요정보 취득가능 직무에 있는 임직원은 내규에 따라 금융투자상품 매매 신고대상에 포함되며 관련 부서장이 대상자를 등록한다.

그러나 등록대상자의 기준이 모호하여 부서장의 임의적인 판단에 따라 신고대상으로 등록하지 않거나 수시 인사이동으로 인하여 신고대상임에도 적시에 등록하지 못하는 사례가 확인되었다.

(나) 금융투자상품 매매신고 적정성 점검 미흡

은행 ▤▤▤는 내규 등에 따라 신고대상 임직원이 제출한 금융투자상품 매매신고서의 내용에 대하여 매매규모 및 횟수 적정성, 신고된 계좌를 통한 거래여부 등을 점검하고 있다.

그러나 신고내용을 수기로 점검하여 매매규모 및 횟수의 적정성 확인에 장시간이 소요되고, 신고하지 않은 증권계좌를 통한 거래는 확인하지 못하고 있다.

<조치할 사항>

따라서 은행은 금융투자상품 매매신고 대상자가 신고대상에서 누락되지 않도록 신고대상 부서의 직원의 업무분장내역과 신고대상자 등록현황을 대조하는 한편, 신고내용의 정확성을 효율적으로 점검할 수 있는 시스템을 마련하시기 바랍니다.

(8) 약관 제·개정시 보고·공시·통지 업무 내부통제 강화

은행은 약관 제·개정시 「은행법」 제52조, 「전자금융거래법」 제24조 등에 따른 감독당국 보고·공시·고객통지 업무를 수행해야 하며, 현재 각 약관의 소관부서가 동 업무를 담당하여 처리하고 있다.

그러나 은행 ▤▤▤는 각 부서의 약관 관련 업무에 대해 내부감사를 충분히 수행하지 않는 등 관련 내부통제 활동이 미약하고, 약관 제·개정 시 보고·공시·통지 누락 여지가 있어 관련 업무체계를 체계화할 필요가 있다.

<조치할 사항>

따라서 은행은 약관 제·개정 시 감독당국 보고 및 고객통지업무에 대한 내부감사를 주기적으로 실시하는 한편, 업무시스템을 개선하여 약관 보고·공시·통지 업무 프로세스에 대한 내부통제를 강화하시기 바랍니다.

(9) 반복적 위규행위 방지를 위한 내부감사 실효성 강화

은행은 담당 임직원의 업무처리 미흡 또는 내부통제 미흡 등으로 인해 법·규정 위반 가능성이 높은 사실이 발생하였다는 것을 임직원이 인지하였을 경우, 추가적인 법·규정 위반을 방지하기 위해 적시에 내부감사를 실시하는 등 내부통제 강화 조치를 취함으로써 반복적 위규행위 발생을 방지하여야 한다.

그러나 현업부서에서 명시적·반복적으로 위규행위가 발생하고 있음에도 ▤▤▤ 등 내부감사 담당부서에서 이를 보고받지 못하여 동일한 위규행위가 수년간 반복된 사례가 확인되었고,

명시적·반복적으로 발생한 위규행위 사례를 내부감사 계획에 반영하는 기준도 마련되어 있지 않는 등 내부감사 활동을 통해 향후 유사한 위법행위가 반복적으로 발생하는 것을 방지하기 위한 제반여건 구축이 미흡하다.

<조치할 사항>

따라서 은행은 각 부서에서 위규행위 발생 가능성이 높은 사안에 대하여 내부감사 담당 부서 앞 보고를 강화토록 내규를 정비하고, 내부감사 담당부서 업무계획에 반복적 법규 위반이 발생 가능한 경우에 대한 대응책을 반영하시기 바랍니다.

(10) 국외점포 주요 현안사항 대응체계 강화

은행은 내규 「IB1 국외점포」, 「국외점포 준법감시업무 세칙」 등에 국외점포의 현지법규 준수, 감독당국 대응 등 준법감시(Compliance) 관련 주요 현안사항에 대해 국외점포로부터 보고를 받고, '국외점포 준법감시 현안사항 파악 및 지원', '국외점포 준법감시 준수상황 점검' 등의 업무를 수행토록 하고 있다.

그러나 은행은 국외점포의 준법감시 주요 현안사항에 대한 적시 대응 체계를 마련하지 않아 국외점포에서 모행에 준법감시 관련 문제를 주요 현안사항으로 거듭 보고하였음에도 불구하고 모행의 적시 대응이 이루어지지 않은 사실이 있다.

<조치할 사항>

따라서 은행은 국외점포의 준법감시 관련 주요 현안사항 접수시 모행의 적시 대응을 위한 단계별 대응체계를 마련하는 한편, 모행의 국외점포에 대한 내부감사 대상 선정기준에 국외점포의 준법감시 관련 현안사항을 반영하여 국외점포 주요 현안사항 대응체계를 강화하시기 바랍니다.

(11) 국외점포 준법감시계획 수립 및 평가 실효성 강화

은행은 내규 「국외점포 준법감시업무 세칙」상 국외점포의 준법감시업무 모니터링을 위해 은행의 目目目 內 '▨▨▨'을 지정하고, '국외점포 준법감시 경영평가' 기준의 세부항목으로 '점포별 연간 준법감시계획 이행 충실도'를 포함시켜 반기별 평가를 실시하는 등 국외점포의 준법감시계획 이행을 독려하고 있으나, 아래 (가)~(나)의 미흡점이 확인되었다.

(가) 실효성 있는 국외점포 준법감시계획 수립 기준 부재

은행은 매년 국외점포의 준법감시계획을 제출받아 각 국외점포별 연간 준법감시 활동의 주안점을 설정하고 이를 매년 갱신토록 하고 있으나, 각 국외점포는 전년 계획을 그대로 답습하거나 추상적으로 기재·제출함에 따라 해당 연도의 준법감시 현안을 반영하지 못하고 있는 사례가 확인되는 등 실효성 있는 국외점포 준법감시계획 수립기준이 마련되어 있지 않다.

(나) 국외점포 준법감시계획 이행 여부 평가 미흡

은행은 상기 세칙 등에 따라 반기별로 '점포별 연간 준법감시계획 이행 충실도'를 평가하고 있으나, 동 평가가 실질적인 이행 여부를 반영하지 못하고 있는 사례가 있는 등 국외점포 준법감시계획 이행 여부에 대한 평가업무의 실효성이 미흡하다.

<조치할 사항>

따라서 은행은 국외점포별 준법감시 관련 주요현안이 각 점포의 준법감시계획에 반영될 수 있도록 준법감시계획 수립 기준을 도입하여 각 국외점포 준법감시계획 수립에 적용하며, 국외점포 준법감시계획 이행평가 대상기간 중 발생한

현지 감독당국 제재 및 금융사고 발생 사실 등 준법감시 관련 주요 사항을 국외점포별 준법감시계획 이행평가에 반영하기 위한 매뉴얼을 도입하는 등 국외점포 준법감시 활동의 실효성을 강화하시기 바랍니다.

(12) 부동산 PF 사전·사후 관리 절차 개선

은행은 내규 「LK3 심사 및 승인」에 따라 ⊗⊗⊗ 대상 여신 중 □□□억원 이상인 부동산 PF 관련 특수여신은 ▢▢▢가 집중하여 취급·관리하고, 그 외 여신은 영업점에서 취급하고 있다.

그러나 영업점이 취급하는 부동산 PF 여신은 ①그룹·은행 내 익스포저 한도 관리 및 대외보고 시 ▢▢▢ 관리 자산만을 대상으로 함에 따라 부동산 PF 익스포저에 반영되지 않으며, ②▢▢▢ 관리 자산만을 전산을 통해 관리하여 별도 사후관리가 이루어지지 않는 등 리스크 관리가 미흡하고, ③영업점 취급 여신 중 특수목적법인 차주에 대해 특수모형이 아닌 비외감·외감모형을 통해 심사를 진행하여 재무평가를 함에 있어 재무제표 신뢰성 검증 불만족 사유를 평가하지 않고 대출을 실행한 사례가 확인되었다.

<조치할 사항>

따라서 은행은 ①PF대출에 대한 한도 협의 및 배정 절차를 신설하고, ②비집중화 여신에 대한 사후관리 강화 방안을 마련하며, ③부동산 PF 관련 심사절차를 강화하는 등 부동산 PF 사전·사후 관리 절차를 개선하시기 바랍니다.

(13) 여신 포트폴리오 한도 관리 업무체계 개선

은행은 내규 「여신업무정책」에 따라 동일인 및 동일차주와 사업, 국가 등 각 포트폴리오별 신용공여 한도를 설정하여 관리하고 있다.

그러나 은행은 ①한도 소진율에 따른 구체적인 대응절차를 마련하고 있지 않고, ②동일법인 여신 세부한도 설정을 위해 신용등급과 환율을 고려한 산정 기준을 운영하면서도, 동 기준과 신용등급 구간별 일괄 최저한도 중 더 큰 값을 한도로 설정하도록 운영함에 따라 신용등급과 환율을 고려한 보수적인 한도 설정이 이루어지지 않을 우려가 있으며, ③전략적 해외 진출국가의 여신 한도

산정 시 전체 현지법인들의 평균 위험가중자산를 적용하여 국가 간 한도설정이 차등화되지 않는 미흡점이 있다.

<조치할 사항>

따라서 은행은 ①여신 포트폴리오 한도 소진율 단계별 관리 방안을 내규에 구체적으로 명시하고, ②동일법인 여신 세부한도 설정을 위한 신용등급 구간별 일괄 최저한도를 세분화하는 등 최저한도를 적정하게 설정하며, ③전략적 해외 진출국가 한도설정 시 국가별 한도를 합리적으로 차등화하여 여신 포트폴리오 한도 관리 업무를 개선하시기 바랍니다.

(14) 여신 심사 관련 위원회 운영 개선

은행은 내규 「▦▦▦규정」, 「▨▨▨규정」에 의거 ▦▦▦와 ▨▨▨를 구성, 재적위원의 ▫분의 ▫이상의 출석과 참석 위원의 ▫분의 ▫ 찬성으로 승인을 결정하는 방식으로 거액 여신 심사를 실시하고 있다.

그러나 ①▦▦▦는 위원들의 표결 처리로 승인 가부를 결정하여 적절한 견제장치가 없고, ②▨▨▨ 내 ♨♨♨ 소속인원이 적어 보수적으로 여신 심사를 결정하기 어려우며, ③▦▦▦ 및 ▨▨▨ 각각의 승인대상 여신을 심사하기 위한 요소인 RoRWA 또는 ROAA의 심사 가이드라인과 사전협의 절차의 근거가 명확하지 않는 등 상기 위원회의 구성·운영이 미흡하다.

<조치할 사항>

따라서 은행은 ①▦▦▦ ☏☏☏에게 거부권을 부여하고, ②▨▨▨ 내 리스크 관리 분야 인원의 비중을 확대하며, ③양 위원회 승인대상 여신의 RoRWA 및 ROAA 심사 가이드라인 등을 내규화하는 등 상기 위원회의 구성과 업무 체계를 개선하여 운영하시기 바랍니다.

(15) 기업여신 가산금리 결정 프로세스 개선

은행은 내규 「LA5 금리결정 및 적용」 및 '기업여신금리 가이드라인'에 영업

점장 전결 여신의 금리 가이드라인을, 내규 「RoRWA/신ROAA 가이드라인」에 ▦▦▦ 및 ▨▨▨ 전결 여신의 기업여신 가산금리 관련 기준을 두고 있다.

그러나 본부(▩▩▩) 전결 여신에 대해서는 가산금리 결정 기준 및 관련 내규가 없고, 금리 감면사유가 각 영업 그룹별로 관리됨에 따라 금리감면 시 지역별·협약별 편차가 발생하는 등 업무의 체계성이 부족하다.

<조치할 사항>

따라서 은행은 본부 전결여신의 가산금리 결정 프로세스에 대한 내규를 신설하여 금리감면 근거, 기준 및 사유를 체계적이고 명확하게 관리하시기 바랍니다.

(16) 자산건전성 분류기준의 적정성 검증 프로세스 개선

은행은 「은행업감독규정」 제27조 등에 따라 차주의 채무상환능력을 감안하여 자산건전성을 분류하며, 동 업무의 적정성·객관성 확보를 위하여 필요한 내부통제체제를 구축·운영하여야 한다.

은행은 채무상환능력 평가를 위해 자율적으로 신용평가모형을 운영하고 있고, 모형의 평가결과에 따른 평가등급별로 자산건전성 분류를 맵핑(mapping)하여 자산건전성 등급을 부여하고 있는바, 자산건전성 분류가 적정하게 이루어지기 위해서는 신용평가모형에 따른 평가등급과 자산건전성 분류 단계 간 유의적 관계(매핑기준)에 대한 모니터링 및 주기적인 검증이 실시되어야 한다.

그러나 은행은 자체 설정한 신용평가모형에 따라 자산건전성 분류를 실시하면서, 평가등급과 자산건전성 분류 단계 간 매핑기준에 대한 점검 기준 및 절차가 부재하다.

<조치할 사항>

따라서 은행은 신용평가등급과 자산건전성 분류 단계 간 매핑기준에 대한 점검 기준을 마련하고, 이를 토대로 독립된 감리 조직의 주기적 점검을 실시하여 자산건전성 분류기준의 적정성 검증 프로세스를 개선하시기 바랍니다.

(17) 대손충당금 산정 방식 개선

은행은 국제회계기준(IFRS)에 따른 대손충당금 산정 시 리스크측정요소(Risk Components) 적용 기준 등 산정 방식을 합리적으로 운용하여 대손충당금 산출의 정확성을 제고하여야 하나, 아래 (가)~(다)의 미흡점이 확인되었다.

(가) 부도시손실률(LGD) 산출 시 회수데이터 활용 범위 확대

은행은 LGD 추정 시 내부 회수데이터를 활용하고 있으나 데이터 정제 요건에 따라 회수데이터 상당수를 LGD 추정 대상에서 제외하여 결과값의 대표성이 미흡하다.

<조치할 사항>

따라서 은행은 내부 회수데이터의 적재 방식 개선, 과거 회수데이터 정비, 데이터 정제 요건 개선 등 LGD 추정 시 회수데이터 활용 범위 확대를 통해 결과값의 대표성 제고 방안을 마련하시기 바랍니다.

(나) LGD 산출을 위한 회복률 추정 방식 개선

은행은 LGD 추정 시 부도사유가 해제되어 정상거래가 재개되는 차주를 회복으로 정의하고 해당 비율(이하 '회복률')을 적용하고 있으나, 가계여신의 경우 신용·예적금·부동산 등 담보종류에 따라 회복률을 산정하는 반면, 기업여신의 경우 담보종류와 무관하게 단일 회복률을 산출하여 LGD 추정 시 일률적으로 적용하여 기업여신 회복률 추정에 담보종류별 회복률이 반영되고 있지 않다.

<조치할 사항>

따라서 은행은 기업여신의 담보종류별 회복률 분석 등을 통해 현행 회복률 적용 방식의 적정성을 점검하고, 점검 시 담보종류별 회복률에 유의적 차이가 확인될 경우 담보종류별로 회복률을 산출하여 적용하는 등 기업여신 관련 LGD 산출을 위한 회복률 추정 방식을 개선하시기 바랍니다.

(다) 대손충당금 개별평가 시 낙찰가율 적용기준 개선

은행은 대손충당금 산출을 위한 담보물 평가 시 감정평가액에 적절한 낙찰가율을 곱하여 예상 처분가액을 산출하나, 평가방식(개별평가·집합평가)에 따른 낙찰가율 적용기준을 상이하게 운영하는 등 기준 운영의 일관성이 부족하다.

<조치할 사항>

따라서 은행은 대손충당금 평가방식의 일관성을 확보하기 위하여 대손충당금 개별평가에도 집합평가와 동일한 낙찰가율 적용기준을 적용하시기 바랍니다.

(18) O·A방식 수출채권 매입업무 점검 프로세스 개선

은행은 내규「FE6 소구조건부 OAT 수출대금채권 매입」등에 따라 송금방식(이하 "O·A방식")*으로 수출채권 매입 시 철저한 서류 검토를 통해 중복·허위매입을 방지하고 이상거래에 대한 적절한 사후관리를 통해 손실을 예방하여야 하나, 아래 (가)~(나)의 미흡점이 확인되었다.

* 수출자가 물품선적 후 선적서류를 직접 수입자에게 송부하고 추후 수입자로부터 송금받는 수출채권(Open Account)으로, 수출자는 해당 채권을 은행에 매각(현금화)

(가) 수출채권 매입 시 서류검토 절차 개선

상기 내규에 따르면 수출채권을 매입하는 경우 수출거래의 실재성 확인을 위해 수출채권 매입의뢰서·수출신고필증 등을 전부 징구하고, 위·변조 및 매입의뢰서상 기재사항과의 일치 여부 등을 검토한 후 매입해야 한다.

그러나 은행은 수출채권 매입 체크리스트를 형식적으로 운영중으로, 매입의뢰서 등 일부 서류가 누락되었음에도 수출채권 매입을 실행하는 등 사전 점검절차가 미흡하여 중복・허위매입을 사전에 방지하지 못할 위험이 있다.

<조치할 사항>

따라서 은행은 수출채권 매입 시 체크리스트를 기존 팝업 방식에서 항목별 점검 방식으로 변경하여 점검 여부와 발견된 특이 사항을 기재토록 하는 등 체크리스트의 실효성을 제고하고, 필수서류의 징구 여부를 관리하고 미징구 사유에 대한 사후 점검

등을 통해 수출채권 매입 관련 서류 누락 방지책을 마련하시기 바랍니다.

(나) 수출채권 매입 사후관리 강화

상기 내규에 따르면 수출상이 자기자금 결제(제3자 결제 포함)를 반복하는 경우 그 사유 등을 구체적으로 확인하고, 추가매입 신청 시 매입 적정성을 신중히 검토한 후 추가매입을 취급하여야 한다.

그러나 은행은 자기자금 결제가 반복적으로 일어나는 업체에 대해 추가적 검토나 통제 절차 없이 수출채권을 지속적으로 추가 매입한 사례가 확인되었다.

또한 자기자금 결제 건에 대한 점검 절차가 없고, 반복적으로 자기자금을 결제하는 고객에 대한 구체적인 대응 매뉴얼 없이 영업점에서 이상거래에 따른 위험을 자체판단토록 하는 등 수출채권 매입에 대한 사후관리 절차가 미흡하다.

<조치할 사항>

따라서 은행은 사유가 불분명한 반복적인 자기자금 결제 등 이상거래에 대한 사후관리 대응 매뉴얼을 마련하고, 이상거래 고객에 대한 추가 매입 시 매입의 적정성에 대한 검토 프로세스와 추가 매입 제한 조건을 정하여 전산 제어하는 등 통제 절차를 강화하며, 사후적으로 제3자가 업무 처리의 적정성을 점검할 수 있는 프로세스를 마련하는 등 수출채권 매입 사후관리를 개선하시기 바랍니다.

(19) 채무재조정 여신의 변경조건 관리 프로세스 개선

「채무자 회생 및 파산에 관한 법률」에 따라 회생계획안 인가 결정 등 채무재조정 조건이 확정되는 경우 은행은 내규「LF23 회생절차」등에 따라 변경된 상환조건에 따라 원리금 상환 등 사후관리 업무를 수행해야 한다.

그러나 은행은 채무재조정에 따라 변경된 상환조건을 전산시스템에 반영하지 않고 개별 차주의 사후관리 담당 직원이 변경된 조건을 수기 관리하고 있어 수행업무에 대한 제3자 검증에 제한적이며, 상환금 오류 및 부당처리의 위험도 있다.

<조치할 사항>

따라서 은행은 채무재조정에 따라 조정된 여신 상환조건을 전산시스템에 반영토록 개선하고, 상환금 처리의 적정성 및 변제계획 이행 여부에 대한 점검 절차를 마련하여 채무재조정 여신의 변경조건 관리를 강화하시기 바랍니다.

(20) 개인사업자 대출 관리 프로세스 개선

(가) 개인사업자 대출 한도관리 미흡

은행은 내규 「LE18 여신포트폴리오 한도관리」에 따라 개인사업자 대출의 한도를 관리하고, 한도소진율이 관리기준을 초과하는 경우 여신 취급기준 및 한도배정 절차 강화 등 관련 조치를 수행하여야 한다.

그러나 상기 내규상 개인사업자 한도소진율에 따른 구체적인 단계별 관리방안이 부재하고, 2023년 중 특정업종의 한도소진율이 관리기준을 초과하였음에도 유관부서 실무자간 구두협의만 수행하는 등 조치가 미흡하였다.

<조치할 사항>

따라서 은행은 개인사업자 대출의 한도소진율에 따른 구체적인 관리방안 및 주체를 내규에 명문화하고, 관리기준 초과 시 관리방안을 마련하여 OOO위원회에서 보고·의결하는 등 개인사업자 대출 한도관리체계를 개선하시기 바랍니다.

(나) 임대소득 심사 미흡

은행은 내규 「개인사업자대출 여신심사 모범규준」 및 「개인사업자대출 여신심사 가이드라인 업무매뉴얼」에 따라 RTI 산정 시 객관적 증빙에 기초하여 추정임대소득을 사용하고, 여신 심사과정에서 RTI 규제 관련 전결기준을 준수해야 한다.

그러나 은행은 별도의 증빙 없이 또는 공신력이 부족한 탁상감정 등을 단독으로 사용하여 임대소득을 추정하고, 규제관련 전결기준을 미준수하는 등 임대소득의 심사과정이 미흡하여 개인사업자 대출이 부적정하게 취급될 우려가 있다.

<조치할 사항>

따라서 은행은 임대소득 추정 시 정식 감정평가를 활용하는 등 관련 내부통제 절차를 개선하고, RTI 규제 관련 전결기준을 충족하는 경우에만 취급될 수 있도록 전산시스템을 개선하며, 임대소득 심사와 관련된 구체적인 심사항목 및 모니터링 방법을 마련하시기 바랍니다.

(다) 감리 미흡

은행은 내규 「LA9 신용감리」에 따라 여신 취급 프로세스의 적정성을 점검해야 하고, 신용위험이 급격히 증가할 것으로 예상되는 부분에 대하여는 수시감리를 통하여 점검하여야 한다.

그러나 은행은 개인사업자대출 연체율이 상승하고 있음에도, 감리 시 대출실행 이후의 여신 상환능력 변동 등을 위주로 점검하고, 대출실행 이전의 여신 상환능력 확인을 위한 소득심사 프로세스의 적정성에 대한 점검은 실시하지 않았다.

<조치할 사항>

따라서 은행은 개인사업자대출 취급 시 RTI 취급기준의 준수여부를 확인하는 점검 가이드라인을 마련하고, 필요시 개인사업자대출과 관련하여 대출취급 전 소득심사 프로세스의 적정성에 대한 점검 등을 포함하여 수시감리를 실시하시기 바랍니다.

(21) 시세없는 담보물건 평가의 관리 프로세스 개선

은행은 영업점에서 시세없는 담보물건에 대하여 시가를 추정하는 경우 내규 「LC4 부동산」에 따라 현장방문·인근 부동산 탐문가격 등을 통해 객관적인 조사자료를 보완하여 가격을 추정해야 한다.

그러나 은행은 객관적인 조사자료를 보완하는 구체적 방법에 대하여 영업점의 자율에 맡기고 있으며, 담보물 시가추정 불철저에 따른 자체징계 사례도 확인되었다.

<조치할 사항>

따라서 은행은 시세없는 담보물건에 대하여 탁상감정가격을 단독사용하지 못하도록 전산통제하고, 담보별 구체적인 보완방법을 영업점 안내 및 심사 시 필수 점검 항목에 반영하는 등 시세없는 담보물건 평가 관련 업무를 개선하시기 바랍니다.

(22) 외부 기술신용평가서 등에 대한 적정성 평가절차 개선

은행은 외부 기술신용평가서의 신뢰성을 확보하기 위해서 내규 「LE27 기술신용대출 취급기준」에 따라 기술평가 인프라·기술평가 절차 및 결과물에 대한 품질관리활동을 실시하여 점검해야 한다.

그러나 상기 내규상 기술신용평가서 및 평가업체에 대한 품질관리절차 및 점검결과에 따른 조치방안이 구체적으로 명시되어 있지 않아 평가서에 유사한 오류가 반복적으로 발생한 사실이 있다.

<조치할 사항>

따라서 은행은 기술신용평가서 및 평가업체에 대한 구체적인 품질관리절차 및 점검결과에 따른 조치방안을 내규에 명문화하여 외부 기술신용평가 관리절차를 개선하시기 바랍니다.

(23) 내부회계관리제도 변화관리 프로세스 개선

은행은 회계정보의 작성 및 공시와 관련된 효과적인 내부통제를 설계 및 운영하기 위해 「내부회계관리제도 모범규준」 및 내규 「내부회계관리세칙」에 따라 프로세스 변화사항의 영향을 파악하여 통제기술서 등 관련 문서에 반영해야 한다.

그러나 부동산 PF관련 프로세스 변경, 감독당국 지적사항 관련 개선항목 등 일부 변화사항이 통제기술서에 반영되지 않는 등 프로세스 변화사항 관리업무가 미흡하게 운영된 사례가 있다.

<조치할 사항>

따라서 은행은 현업부점에서 내규 제개정 사항 등에 대한 전체 리스트를 받아 점검하고, 신규업무 해당여부 및 기존통제와의 연관사항을 명확히 문서화하는 등

변화관리 프로세스 업무절차를 개선하시기 바랍니다.

(24) 신용평가시스템 적합성 검증 프로세스 개선

은행은 신용평가시스템 운영 시 「은행업감독업무시행세칙」 [별표3] 제202호 및 제206호 등에 따라 견실한 적합성 검증 체계 및 기준을 마련하여야 한다.

그러나 은행 내규 「RM11 적합성 검증」은 모형의 부적합 판단 기준을 단일기준으로만 관리하는 경우가 있고, 성능저하 여부를 적합성 검증 지표의 초과 상태가 '□년 연속' 지속된 경우로 정의하고 있어 성능저하를 적시에 포착·관리하는데 한계가 있다.

또한 적합성 검증 결과 개선 권고사항에 따른 개선 결과를 OOO위원회에 보고토록 하고 있으나 내규상 명시적인 점검기한이 없어 개선 권고사항의 이행이 지연될 우려가 있다.

<조치할 사항>

따라서 은행은 양적 검증 개선범위에 도달하지 않더라도 모형의 분포 변화 및 성능 저하를 조기에 포착하여 관리할 수 있도록 단계적 양적 검증 판단기준을 마련하고, 개선계획 제출기한 및 이행현황 점검기한을 내규에 명시하는 등 신용평가시스템 적합성 검증 업무의 실효성을 제고하시기 바랍니다.

(25) 기업신용평가 비재무모형 통제절차 개선

은행은 2021. 3. 금융감독원으로부터 기업신용평가모형의 변경승인을 득하여 규제자본 산출 등에 활용 중으로, 승인 당시 비재무평가의 변별력을 안정적으로 유지할 수 있도록 모니터링을 강화하고 등급조정률을 적정한 수준으로 유지할 것을 권고받았다.

그러나 은행의 ♩♩♩ 및 ♪♪♪ 등 일부 모형의 변별력이 여전히 부적합 판단기준을 하회하는 경우가 확인되며, 비재무 최종등급 산출 이후 재평가를 통한 등급상향 시 평가이력·횟수 관리가 미흡하는 등 비재무모형의 평가등급 통제절차를 개선할 필요가 있다.

<조치할 사항>

따라서 은행은 비재무모형 변별력 제고 등을 위해 지속적인 모니터링을 실시하여 추가적 통제절차를 마련하는 한편, 적합성 검증지표 수준에 대한 단계적 관리기준을 강화하시기 바랍니다.

(26) 재산상 이익제공 보고 관련 업무 개선

은행은 「은행법」 제34조의2 등 관련법령 및 내규 「재산상 이익의 제공 및 수령에 관한 세칙」에 따라 은행이용자 등에게 재산상 이익을 제공하거나 받고자 하는 경우 제공일자 및 경제적 가치 등을 준법지원시스템을 통해 준법감시인에게 사전보고하여야 하며, 소요금액을 사전에 확정하기 어려운 경우 등 부득이한 사유로 사전보고가 곤란한 경우에는 사후에 보고할 수 있다.

또한 동 내규에 따라 재산상 이익 제공규모에 따라 □□억원을 초과하는 경우 집행부서의 적정성 점검 및 ◆◆◆ 사전승인, □백만원 초과 및 □□억원 이하의 경우 目目目의 적정성 점검, □백만원 이하의 경우는 적정성 점검 및 평가를 생략하고 있다.

그러나 은행은 내규상 사후보고 대상인 소요금액 확정이 어려운 경우 등 부득이한 사유에 대하여 구체적인 예시 및 세부기준을 두지 않아 보고사유에 대한 특별한 고려 없이 다수건을 사후보고 하였으며, 대부분의 부실점 이익 제공이 예산관리시스템에 결재상신하는 시기에 사후보고가 이루어지는 등 사후보고 관련 미흡한 점이 확인되었다.

또한 적정성 점검 대상인 건별 □백만원 초과건에 대하여 사후보고함으로써 재산상 이익이 제공된 이후에야 적정성 검토가 이루어지는 사례도 확인되는 바, □백만원 초과건에 대한 적정성 점검의 실효성 및 적시성을 확보할 필요가 있다.

<조치할 사항>

따라서 은행은 준법감시인에게 사후보고가 가능한 경우를 구체적으로 한정토록 내규를 개정하고, 부실점에서 제공한 이익에 대해 내규상 사후보고의 원칙적 기한(□개월)을 준수할 수 있도록 업무체계를 구축하며, 건별 경제적 가치가 □

백만원을 초과 제공하는 경우 적정성 검토가 사전에 이루어질 수 있도록 사전보고 대상으로 명시하는 등 재산상 이익제공 관련 업무체계를 개선하시기 바랍니다.

(27) 금고 입찰 등 출연금 수익성 분석 관련 업무 개선

은행은 내규 「출연금관리규정」 및 「출연금관리세칙」에 따라 대학·병원·지방자치단체·공공기관 등에 현금 및 현물 일체를 제공하려는 경우 예상 이익을 분석하여 출연금 약정기간에 대한 수익성을 평가하고, 출연금 제공 이후 무형자산으로 분류된 경우 매년 상반기 중 손상징후 점검표를 작성하여 이를 출연금 심의위원회에 보고해야 한다.

그러나 은행은 출연금 약정기간에 대한 수익성 평가 시 입점을 위한 예상 이익이나 손상 징후와 관련된 특정 항목이 중복 또는 제외되었음에도 이를 점검 또는 인지하지 못한 채 적정성 검토를 실시한 사실이 있다.

또한 출연금 손상징후를 판단하면서 미래 현금흐름을 적절한 할인율로 할인한 현재가치를 사용해야 하나 할인율을 산정 및 적용하는 절차가 없다.

<조치할 사항>

따라서 은행은 각 부실점에서 작성한 수익성 분석자료 검토 시 항목의 중복이나 제외가 발생하지 않도록 관련 기초자료를 제공받아 교차 점검하는 등 사후점검 체계를 강화하고, 수익성 분석자료 작성 요령에 대한 주기적 교육을 실시하며, 출연금 손상징후를 판단하면서 미래 현금흐름에 대한 적절한 할인율을 사용할 수 있도록 관련 내규를 개선하시기 바랍니다.

(28) 국외점포 외화유동성 관리 강화

은행은 자산평잔 규모에 따라 국외점포를 □개 그룹으로 구분하고 그룹별로 외화유동성 관리지표 및 OOO위원회 보고주기를 다르게 운영하고 있어, 국외점포별 유동성리스크 모니터링 업무의 통일성 및 비교가능성이 부족하다.

또한 국외점포 외화유동성 평가 주관부서가 ★★★에서 ♬♬♬로 변경되었으나

♬♬♬의 관련 책임 및 역할이 내규에 명시되어 있지 않다.

<조치할 사항>

따라서 은행은 외화LCR 평가 점포를 지속적으로 확대하여 장기적으로 통일된 유동성 관리지표 한도설정 및 관리체계를 구축을 지속 추진하고, 모든 국외점포의 외화LCR 및 현지규제비율을 OOO위원회에 매월 보고하여 외화유동성 관리의 통일성을 제고하고, 리스크 관련 내규상 ♬♬♬의 외화유동성 관리 책임과 역할을 명시하는 등 국외점포 외화유동성 관리체계를 개선하시기 바랍니다.

(29) 유동성리스크 관련 지표 관리체계 강화

은행은 내규 「유동성리스크」에 유동성리스크 관련 지표별 관리방안을 규정하고 있으며, 유동성 규제비율의 안정적인 준수를 위해 각 규제비율별로 내부관리한도를 설정하여 관리·운영하고 있다.

그러나 은행은 각 유동성 규제비율별로 내부관리한도 관리방법 및 내규 반영여부 등이 상이하며, 예대율의 경우 내부관리한도가 규제비율과 동일한 수준으로 설정되어 있어 규제비율의 안정적 준수를 위한 내부관리한도 운영 취지에 부합하지 않는다.

<조치할 사항>

따라서 은행은 예대율 및 중장기외화자금조달비율에 대해서도 내부관리한도를 내규상 명시하고, 한도 하회시 OOO위원회에 보고토록 규정하며, 예대율에 대해서도 규제비율보다 엄격한 내부관리한도를 설정하시기 바랍니다.

(30) 대고객 파생상품 관련 사후관리 절차 강화

은행은 대고객 파생상품 판매 시 「자본시장법」 등 관련 법규를 준수할 수 있도록 내규 「대고객거래」 등을 통해 대고객 파생상품의 판매기준 및 절차 등을 마련하여 운영중이나, 동 판매기준과 절차가 법령에 따라 준수되고 있는지 일부 거래를 발췌하여 점검한 결과 아래 (가)~(나)의 미흡점이 확인되었다.

(가) 일부 판매서류의 미기재·공란 및 전자문서관리시스템(EDMS) 미저장

내규「대고객거래」등에 의하면 은행은 파생상품 거래 시 기본계약서, 손실한도약정서와 위험회피목적 확인서류 등을 징구해야 하나, 기본계약서 등 일부 서류의 서명일 및 교부일을 미기재하거나, 은행 및 대리인 확인란이 공란인 사례 등이 확인되었다. 또한 판매서류는 스캔되어 전자문서관리시스템에 등재 및 저장되어야 함에도 서류 스캔(Scan)본이 전자문서관리시스템에 적정하게 등재·저장하지 않은 사례도 확인된다.

(나) 외환파생상품 거래한도의 기타증빙제도 점검 미흡

내규「기업투자자 외환파생상품 연간 거래한도 등록」4.기타 증빙항목 중 금지사항, 사후관리사항 이행여부 등을 점검하도록 규정하고 있으나, 이에 대한 점검이 면밀히 이루어지지 않아 향후 고객과의 분쟁·민원이 발생할 우려가 있다.

<조치할 사항>

따라서 은행은 영업점 징구서류에 대한 사전점검 메뉴얼을 마련하고 점검이 완료된 서류는 전자문서로 저장하여 본점 부서에 집중하는 등 전자문서관리시스템을 통한 사전검토 절차를 구축하며, 판매서류 사전점검 관련 사항을 자점감사 항목에 반영하고, 전자문서가 미등재된 경우 영업점 성과평가에 반영하는 한편, 금지사항 등에 대한 점검업무를 강화하는 등 개선 방안을 마련하시기 바랍니다.

(31) 해외투자 의사결정 절차 개선

은행은 해외 현지법인에 대한 신규 투자결정 시 발생 가능한 투자손실, 평판리스크 등의 영향을 고려하여 잠재 부실요인, 성장가능성 등에 대해 충분히 검토하여야 한다.

그러나 은행은 내규「◆◆◆ 규정」등에서 해외 현지법인 지분 취득 시 신규 취득·유상증자를 구분하지 않고, 건당 출자금액만을 기준으로 해외투자 의사결정 전결기준을 운영하고 있다.

이에 따라, ●●●의 결정만으로 경영권 지배목적의 지분취득 및 법인 설립, 추가 유상증자가 가능하여, 해외투자 시 발생 가능한 투자손실 및 잠재 부실 요인 등에 대한 ◆◆◆ 차원의 검토없이 해외 현지법인이 은행 자회사로 편입되는 등 면밀한 사전검토가 부재한 해외투자가 지속·반복될 우려가 있다.

<조치할 사항>

따라서 은행은 해외현지법인 신규투자 의사결정 시 ◆◆◆ 결의사항으로 하는 방안을 마련하여 해외 현지법인에 대한 투자 의사결정이 ◆◆◆ 중심으로 논의될 수 있도록 전결기준을 개선하시기 바랍니다.

(32) 대출 상환시 근저당설정 유지의사 확인절차 개선

은행은「금융소비자보호법」제20조 및 동법 시행령 제15조,「금융소비자 보호에 관한 감독규정」제14조 제6항 제10호에 따라 근저당이 설정된 금전제공계약의 금융소비자가 채무를 모두 변제한 경우에 해당 담보를 제공한 자에 근저당 설정을 유지할 것인지를 확인해야 한다.

그러나 은행은 전산통제가 미흡하거나 사후 내부통제 절차가 마련되어있지 않아 금융소비자가 채무를 모두 변제하였음에도 불구하고 근저당 설정 유지여부를 확인하지 않을 우려가 있어 개선이 필요하다.

<조치할 사항>

따라서 은행은 금융소비자가 채무를 모두 변제하는 경우 근저당 설정 유지 여부를 확인하도록 전산통제를 강화하고, 근저당 설정 유지의사 확인절차가 적절히 이행되었는지 ◇◇◇ 등 소관부서가 사후점검하는 등 업무절차를 개선하시기 바랍니다.

(33) 제3자 담보제공자 보호 운영절차 개선

은행은 내규「담보총칙」등에 따라 대출 만기연장 시 제3자 담보제공자의 동의여부를 확인하고 있으며, 이를 위해 대출서류를 본부에 집중하는 경우 제3자 담보제공자 동의서 징구여부를 점검하고 있다.

그러나 제3자 담보제공자 동의서의 실제 징구여부를 전산에서 확인할 수 없어 사후 점검 및 누락여부 적발·보완이 불가능하며, 전산상 제3자 담보제공자의 동의를 얻지 않았더라도 대출 만기연장이 가능하여 제3자 담보제공자를 보호하기 위한 내부통제체계가 미흡하다.

<조치할 사항>

따라서 은행은 대출 만기연장 시 제3자 담보제공자 동의서 징구여부가 확인되어야 대출 연장실행이 가능토록 전산통제 절차를 구축하고, 제3자 담보제공자 동의서 징구 여부에 대한 사후점검 및 보완 등 내부통제를 강화하는 등 관련 업무절차를 개선하시기 바랍니다.

(34) 대출모집법인에 대한 내부통제 개선

은행은 내규 「대출모집인제도 운영 및 관리지침」에 따라 소속 대출모집법인에 대한 교육·광고물 승인·영업실태 점검 등 내부통제 활동을 수행하고 있다.

그러나 오프라인 대출모집법인에 대한 내부통제 절차 및 운영이 일부 미흡하고,

온라인 대출모집법인에 대하여도 내부통제 점검결과 보고 시 구체적인 점검 내용에 대한 기록·관리가 미흡하고, 다수의 점검항목을 '적정'으로만 평가하는 등 점검을 형식적으로 실시한 사례가 확인되었다.

<조치할 사항>

따라서 은행은 대출모집법인 관련 내규를 보완하여 내부통제 절차를 보완하고 대출실시 전·후 적정서류 징구여부 등에 대한 모니터링을 강화하는 한편, 대출모집법인 대상 직접 교육, 현장점검 등을 실효성 있게 수행하는 등 관련 업무절차를 개선하시기 바랍니다.

(35) 비시장성 공정가치 평가 회계처리 개선

은행은 회계처리 누락이 발생하지 않도록 회계시스템 및 사후관리 절차를 마련하고 적정하게 운영해야 한다.

은행의 비시장성 유가증권에 대한 공정가치 평가 시 관련 금액 입력은 ■■■에서 수기로 입력하고 있음에도 동 금액의 기표 오류 여부에 대한 비시장성 유가증권 보유부서의 확인 절차가 없어 기표를 누락한 사례가 확인되었다.

<조치할 사항>

따라서 은행은 비시장성 유가증권 평가 등 수기기표의 적정여부에 대한 제3자 점검절차를 마련하여 정기적으로 점검결과를 회계부서에 보고하는 등 비시장성 공정가치 평가 회계처리가 적정히 이루어질 수 있도록 관련 내부통제를 개선하시기 바랍니다.

(36) 광고성 문자전송 시스템 및 절차 개선

은행은 「신용정보법」 제40조 등에 따라 동의한 고객에게만 광고성 정보를 전송하기 위하여 광고문자·정보문자 여부를 지정하여 적정 고객에게만 문자가 발송되도록 전산시스템을 구축하였다.

그러나 은행은 광고문자임에도 정보문자로 지정하여 마케팅 수신에 동의하지 않은 고객에게도 광고문자 발송이 가능하도록 시스템을 운영함에 따라 부적정한 광고성 문자전송이 이루어질 우려가 있다.

<조치할 사항>

따라서 은행은 광고성 문구(광고·심의필 등)가 포함된 문자 전송 건이 정보문자로 지정하여 마케팅 수신에 동의하지 않은 고객에게 발송될 수 없도록 관련 전산시스템 및 절차를 개선하고 적정여부에 대한 사후검증 절차를 마련하시기 바랍니다.

(37) 부동산 담보신탁 대출의 우선수익자 수익권 범위 개선

「금융소비자 보호에 관한 감독규정」 제14조 제6항 등에 의하면 은행은 금융소비자 또는 제3자로부터 담보를 취득하는 계약과 관련하여 해당 계약서에 피담보채무를 특정하지 않거나 해당 계약서상의 담보가 장래 다른 채무도 담보한다는 내용으로 계약하여서는 아니 된다.

그러나 은행은 부동산 담보신탁 대출 취급 시 신탁계약의 수익권증서를 담보로 취득하면서 우선수익자의 피담보채무 범위가 미특정되거나 포괄적으로 해석될 여지가 있도록 계약서 내용을 불명확하게 관리하고 있다.

<조치할 사항>

따라서 은행은 부동산 담보신탁 대출 취급 시 피담보채무가 특정된 신탁계약의 수익권증서만을 담보로 취급할 수 있도록 계약서 내용을 명확히 하고, 수익권증서의 피담보채무 범위와 여신거래계약상 대출의 종류와 일치 여부를 확인하는 등 관련 업무체계를 개선하시기 바랍니다.

(38) 부동산 담보신탁 절차 개선

「신탁법」 제36조 등에 의하면 수익자와 수탁자 간 이해상충 방지를 위해 수탁자는 누구의 명의로도 신탁의 이익을 누리지 못하되 예외적으로 수탁자가 공동수익자 중 1인인 경우에 한해 수탁자의 이익향수를 허용한다. 따라서 은행은 대출 연계 부동산 담보신탁 취급시 공동수익자가 실제 존재하는지 여부를 확인하여야 한다.

그러나 은행은 부동산 담보신탁을 취급하는 과정에서 동 수익권증서를 담보로 대출 예정인 계열 금융회사를 공동수익자로 지정하는 경우에도, 계열 금융회사가 실제로 대출을 실행하였는지 여부를 확인하는 절차를 운영하고 있지 않아, 수탁자인 은행이 사실상 단독수익자가 되는 등 「신탁법」을 준수하지 못할 우려가 있다.

<조치할 사항>

따라서 은행은 부동산 담보신탁을 취급시 공동수익자가 계열 금융회사로 지정되는 경우 등에 채권·채무관계에 대한 확인을 강화하는 등 업무절차를 개선하시기 바랍니다.

(39) 전산자료 소산업무 관리 미흡

(가) 영업점 대면 상품판매 녹취파일 소산 필요

은행은 내규 「고난도 금융투자상품 영업행위 준칙」 등에 고난도 금융투자

상품의 제조, 판매, 사후관리 등 일련의 업무 과정에서 고객을 보호하기 위해 구체적으로 준수하여야 할 업무의 방법과 절차를 정하고 있다.

또한 영업점 직원이 고객에게 고난도 금융투자상품을 판매하는 경우 상품 내용 설명 및 판매과정 녹취 의무 등의 이행을 보장하기 위하여 '영업점 대면 상품판매 녹취시스템'을 구축하여 운영하고 있으며, 동 시스템으로 녹취한 파일에 대해 주기적으로 백업하여 보관하는 등의 전산자료 보호대책을 마련하고 있다.

그러나 은행은 '영업점 대면 상품판매 녹취시스템'으로 녹취한 대면녹취 파일을 전산센터에 위치한 녹취시스템 서버 및 백업 서버 내에만 보관하고 있으며, 동 녹취파일에 대해 소산하지 않고 있어 전산센터에 재해 상황이 발생할 경우 대면 녹취 파일의 복구가 적시에 어려울 가능성이 있다.

<조치할 사항>

따라서 은행은 '영업점 대면 상품판매 녹취시스템'으로 녹취된 파일 등 중요 전산자료를 주기적으로 소산하여 안전하게 보관할 수 있도록 하는 등 대면녹취 파일에 대한 소산업무 운영방식을 개선하시기 바랍니다.

(나) 소산 테이프 폐기 절차 마련

은행 내규「백업 및 소산 절차」등에 따르면 은행은 전산자료의 중요도 및 보관주기 등을 고려하여 전산자료에 대해 백업 및 소산을 실시하여야 하고, 보존기한이 경과한 소산 테이프는 재활용하거나 재활용이 불가능한 경우에는 해당 매체를 폐기하여야 한다.

그러나 은행은 재활용이 불가능한 미사용 소산 테이프에 대한 폐기 절차를 마련하지 않아 2016. 6. 외환은행과 하나은행의 합병으로 KEB하나은행의 전산시스템이 통합된 이후 미사용 테이프 및 불량 테이프 등을 장기간 폐기하지 않은 채 보관하고 있는 등 소산 테이프 관리가 미흡하다.

<조치할 사항>

따라서 은행은 보존기한이 경과한 미사용 테이프와 불량 테이프 등에 대하여 폐기

대상 여부를 주기적으로 점검 및 폐기하는 절차를 마련하여 운영하는 등 소산 테이프 관리 업무를 개선하시기 바랍니다.

(40) IT업무 연속성 계획의 실효성 미흡

(가) 재해복구훈련 계획 미흡

은행 내규 「전산업무규정」에 따르면, 회사는 재해 등 비상사태의 발생에 대비하여 비상대책시스템 운영계획 등이 포함된 전산시스템 비상대책을 수립하여야 하며, 재해 등 비상사태 발생 시 신속한 조치를 위해 연 □회 이상 전산시스템 비상대책에 대한 훈련테스트를 수행하여야 한다.

이에 따라 은행은 재해 등 비상사태 발생 시 신속한 조치를 위해 복구 목표시간을 □시간 이내로 설정하여 재해복구 비상계획 및 재해복구시스템 가동절차 등을 점검하는 재해복구 모의훈련을 실시하고 있다.

하지만 은행은 재해복구 모의훈련 시 금융결제원 등 중요 대외기관과의 연계업무를 훈련대상에서 제외하고 있으며, 하나원큐 앱을 통한 그룹사 통합인증 업무는 연계기관(▲▲▲ 산하 □개 계열사)과 직접 테스트하지 않고 단순히 인증서버를 재기동하는 훈련으로 대체하여 재해복구 훈련 시 제반업무 수행의 정합성을 담보하기 어렵다.

또한 재해복구 모의훈련은 재해 등으로 인한 주전산센터 마비에 대비하고 업무지속성을 확보하기 위하여 주전산센터에서 재해복구센터로 전환하는 훈련임에도, 은행의 비상대책위원회 및 핵심업무 복구반 인력 대부분이 주센터에서만 재해복구훈련을 실시하고 있는 등 재해복구훈련의 실효성이 미흡하다.

<조치할 사항>

따라서 은행은 중요 대외기관과의 연계 업무를 재해복구훈련 대상에 포함하고, 그룹사 통합인증 업무 등 중요 업무에 대해서는 계열사와 실제 서비스 테스트를 수행할 수 있도록 훈련계획을 보완하는 한편, 비상대책위원 등이 대체업무 공간으로 이동하여 재해복구훈련을 하는 등 재해복구훈련의 실효성을 높일 수 있도록 훈련 방법 등을 개선하시기 바랍니다.

(나) IT-BCP 업무 매뉴얼 정비

은행 내규「금융전산분야 현장조치 행동매뉴얼」및「ICT 부문 상황별 BCP행동요령」등에 따라 은행은 재해 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 업무연속성 확보대책의 적정성 등을 매년 □회 이상 점검하고 있다.

하지만 은행은「ICT 부문 상황별 BCP행동요령」에 네트워크 및 정보보안 부문의 업무 관련 사항과 백업 데이터 관리 및 데이터 복구 방안이 누락되어 있는 등 IT업무 연속성 계획의 실효성이 미흡하다.

<조치할 사항>

따라서 은행은「ICT 부문 상황별 BCP행동요령」에 네트워크 및 정보보안 부문의 주요 업무 내용과 백업 데이터 관리 및 데이터 복구 방안 등을 반영하여 IT부문에 대한 BCP 업무 매뉴얼을 합리적으로 정비하시기 바랍니다.

(41) IT계약업무 절차 미흡

은행은 디지털 신사업의 신속한 개발 및 IT사업 추진의 효율화 등을 위해 2021. 9. 카탈로그 계약 방식을 도입하여 IT계약을 관리하고 있으나, 아래 (가)~(바)의 미흡점이 확인되었다.

(가) 제안요청서 미발송 및 제안공고 미실시

은행 내규「계약업무세칙」에 따르면, 회사는 경쟁입찰을 실시하는 경우 경쟁입찰에 참가하려는 자로 하여금 입찰 전에 물품의 제조 또는 구매, 용역계약을 체결하고자 하는 때에는 입찰자로 하여금 입찰 전에 당해 물품의 품질·성능·효율 등이 표시된 품질 등의 표시서 또는 제안서 등을 제출하도록 한다.

또한「카탈로그 계약 운영 세칙」에 의하면 통상적인 개발 기술자 등급별 단가를 확정할 수 있는 개발용역 등에 대해서는 내규「IT자원도입세칙」에 정한 절차에 따라 카탈로그 계약을 위한 계약업체를 선정하여야 하며, 동 세칙에 따라 종합평가제 방식에 의한 도입을 추진하는 경우 가격과 품질을 종합적으로 고려하여 업체를 선정하여야 한다.

그러나 은행은 카탈로그 계약업체를 선정하는 과정에서 사전에 등록된 카탈로그 업체를 대상으로 제안요청서를 발송하지 않고 있으며, 카탈로그 업체를 대상으로 하는 제안공고 절차를 거치지 않는 등 일부 계약 업무 절차를 간소화하여 운영하고 있어 IT계약의 투명성이 저하될 우려가 있다.

<조치할 사항>

따라서 은행은 카탈로그 계약업체 선정 시 카탈로그에 등록된 업체를 대상으로 제안요청서를 필수적으로 발송하고, 동 업체에 충분한 제안공고 기간을 부여하는 등 계약 업무 절차를 개선하시기 바랍니다.

(나) 카탈로그 계약 평가항목 세분화 필요

은행 내규 「카탈로그 계약 운영 세칙」에 따르면, 회사는 카탈로그 계약업체를 선정하면서 품질 평가가 필요한 경우 평가위원을 구성하여 카탈로그 계약 대상 업체에 대해 적격성을 평가하여야 하며, 적격성 평가는 IT자원의 품질 확보를 위해 기술 능력에 대한 평가가 □□□분의 □□ 이상이어야 한다.

그러나 은행은 카탈로그 계약업체에 대한 적격성 평가 시 유사 프로젝트 수행 경험 등 □개 평가항목으로 적격성을 평가하고 있으나, 기술 능력을 평가할 수 있는 항목이 부족하고 평가 항목의 세부 기준을 구체적으로 정의하지 않아 평가 기준이 다소 미흡하다.

<조치할 사항>

따라서 은행은 평가위원이 카탈로그 계약 대상 업체의 IT사업 및 특성 등을 고려하여 내실 있는 평가를 수행할 수 있도록 카탈로그 계약 적격성 평가 항목을 세분화·구체화하는 등 평가 기준을 강화하시기 바랍니다.

(다) 제안설명회 미개최 및 대면평가 미실시

은행 내규 「IT자원도입세칙」에 따르면, 회사는 전체시스템 운영에 미치는 영향이 적고 시장조사, 구축사례, 사전기능검증(POC) 등을 통해 IT자원 선정이 가능하다고 판단되는 경우를 제외하고는 객관적이고 공정한 평가를 위해 제안

업체별로 제안설명회를 개최하여야 한다.

또한 은행은 내규「카탈로그 계약 운영 세칙」에 따라 카탈로그 계약업체를 선정하면서 품질 평가가 필요한 경우 평가위원을 구성하여 카탈로그 계약 대상 업체에 대하여 적격성을 평가하여야 한다.

그러나 은행은 카탈로그 계약 건은 제안설명회를 개최하지 않을 수 있다고 판단하여 모든 카탈로그 계약의 적격성 평가 과정에서 제안설명회를 개최하지 않았고, 카탈로그 계약 대상 업체에 대한 적격성을 대면이 아닌 서면으로 평가하여 적격성 평가의 객관성 및 공정성을 담보하기가 어렵다.

<조치할 사항>

따라서 은행은 카탈로그 계약 적격성 평가위원과 제안참가자가 참석하는 제안설명회를 필수적으로 개최하고, 적격성 평가위원들이 동 설명회 참가업체를 대상으로 대면 평가를 하도록 하는 등 평가절차를 개선하시기 바랍니다.

(라) 업체선정 방법 불합리

은행 내규「카탈로그 계약 운영 세칙」등에 따르면, 사업부서는 그룹포탈 게시판 등을 통하여 공지된 카탈로그 계약 대상 업체와 협의를 통해 카탈로그 계약을 추진할 수 있으며,「계약업무세칙」등에 따라 종합평가에 의한 계약을 하는 경우 제안참가자에 대한 평가를 위한 평가위원을 선정하고 선정된 평가위원이 제안참가자별로 평가한 후 ▨▨▨에게 평가표를 밀봉하여 제출하여야 한다.

그러나 은행은 카탈로그 계약 대상 업체선정 방법을 구체적으로 정하고 있지 않아 카탈로그 계약 담당자가 평가위원에게 평가요청 이메일을 송부하고, 동 평가위원들로부터 받은 적격성 평가표를 취합하여 계약 담당자가 업체선정을 하는 등「계약업무세칙」에 의한 종합평가 계약방식과 비교 시 카탈로그 계약의 업체 선정방식은 객관성을 보증한다고 보기 어렵다.

<조치할 사항>

따라서 은행은 카탈로그 계약 업체를 대상으로 적격성 평가를 하는 경우에도

적격성 평가위원이 제안참가자별로 평가하여 평가표를 밀봉하여 ▨▨▨에게 제출하도록 하고, 평가 결과를 目目目가 공문으로 회신받아 계약대상 업체를 선정할 수 있도록 카탈로그 계약 업체선정 절차를 개선하시기 바랍니다.

(마) 카탈로그 등록업체 및 계약정보 미공시

은행 내규 「카탈로그 계약 운영 세칙」에 따르면, 회사는 카탈로그 계약 대상 정보를 그룹포탈 게시판 등을 통해 내부 공지하고, 카탈로그 계약의 투명성과 공정성을 확보하기 위해 계약 등록업체 정보를 수시로 은행 홈페이지에 게시하여야 한다.

그러나 은행은 카탈로그 업체가 신규로 등록되는 경우에만 계약 등록업체 정보를 회사 홈페이지에 게시하고, 2021. 9. 카탈로그 계약 도입 당시 홈페이지에 제안요청서를 한 차례 공고한 이후 회사의 변화된 디지털 환경 등을 반영하여 제안요청서 내용을 최신화하거나 재공고를 하지 않고 있어 카탈로그 계약 등록업체 정보 및 제안요청 내용이 대외적으로 적시에 공개되지 않고 있다.

또한 카탈로그 계약은 공개모집을 통해 입찰 요건에 부합하는 카탈로그 등록 대상 업체를 미리 선정하고, 등록된 카탈로그 업체들로 제한하여 계약을 체결하고 있는 점 등을 고려하면 카탈로그 계약 현황을 외부로 투명하게 공개하는 것이 바람직하나, 은행은 카탈로그 계약 체결현황 등을 공개하지 않고 있어 계약의 투명성이 훼손될 우려가 있다.

<조치할 사항>

따라서 은행은 카탈로그 등록업체 현황 및 계약체결 현황을 주기적으로 대외 홈페이지에 공시하고, 변화된 디지털 환경 등을 반영하여 제안요청서를 주기적으로 재공고 하는 등 관련 업무 절차를 개선하시기 바랍니다.

(바) 부정당업자의 입찰참가자격 제한사유 관리 강화

은행 내규 「계약규정」, 「계약요령」 및 「계약업무세칙」 등에 따르면, 회사 계약 담당자는 경쟁의 공정한 집행이나 계약의 적정한 이행을 해칠 염려가 있거나 그 밖에 입찰 참가가 부적합하다고 인정되는 자에게는 □개월 이상 □년 이하의

범위에서 입찰참가자격을 제한해야 하고, 입찰참가자격이 제한된 자와 수의계약을 체결하면 안된다.

그러나 은행은 부정당업자의 입찰참가 제한사유, 제한기간 등을 체계적으로 관리하는 절차를 마련하지 않는 등 IT계약업무 처리과정에서 부정당업자에 대한 제한내역 관리를 소홀히 함으로써 부정당업자가 입찰에 참가하여 IT계약업무의 공정성이 저해될 가능성이 있다.

<조치할 사항>

따라서 은행은 입찰업체 중 입찰참가자격 제한기준에 의하여 입찰참가자격 제한사유가 발생하는 경우 해당 부정당업자의 입찰참가자격을 제한하거나, 동 업체와 수의계약이 체결되는 것을 미연에 방지하기 위하여 부정당업자의 입찰참가자격 제한사유 등을 전산화하여 관리하시기 바랍니다.

(42) 통신망 안전성 강화대책 불합리

은행은 인터넷·모바일뱅킹 등 전자금융서비스를 제공하기 위하여 인터넷 전용회선과 전산센터 전용회선 등 주요 통신망을 이원화하여 구축·운영하고 있다.

그러나 은행은 국내 전산센터와 해외지점 간 전용회선을 이중화 구성하였으나, 통신망 사업자가 단일 사업자(▼▼▼)로만 구성되어 있고, 보증기관 사고통지 및 대위변제 업무 처리를 위해 기술보증기금과 연결된 전용회선의 경우 단일 회선으로 운영하고 있어 단일 사업자(▼▼▼)의 통신망 장애 또는 단일 회선으로 연결된 대외기관 전용회선 장애 시 전자금융서비스가 중단 또는 지연될 우려가 있다.

<조치할 사항>

따라서 은행은 국내 전산센터와 해외지점 간의 주요 구간별 통신망에 대해서는 통신망 사업자를 이원화하고, 단일 회선으로 연결된 주요 대외기관 간 전용회선은 이중화 구성하는 등 통신망 안전성 강화대책을 마련·운영하시기 바랍니다.

(43) 테스트데이터 관리 절차 미흡

은행 내규「전산개발표준화절차」,「정보보안업무절차」에 따라 은행은 개발·테스트 시 메타관리시스템에 등록한 변환규칙에 따라 이용자 정보를 변환 사용하고, 테스트 종료 시 변환된 데이터를 삭제한다.

그러나 은행은 데이터베이스 테이블을 신규로 생성하거나 컬럼 속성을 변경하는 과정에서 개인정보 유형, 테스트데이터 변환 여부 등 개발자가 입력한 메타정보의 적정성에 대해 DA담당자, 정보보호 담당자가 개인정보 여부, 변환 대상 설정 등이 적절한지 검토하는 절차가 없어 데이터 변환이 일부 누락될 수 있고, 암호화된 비밀번호 등 일부 주요정보는 필수 변환 대상으로 지정하지 않아 미변환된 주요정보가 외부로 유출될 우려가 있다.

<조치할 사항>

따라서 은행은 암호화된 비밀번호 등 이용자 정보 변환 대상 항목을 확대 운영하고, 테이블 신규 생성 및 변경 과정에서 개인정보 유형, 변환 대상 여부 등의 판단 적정성에 대해 DA담당자 등 제3자가 검증하는 등 업무 절차를 개선하시기 바랍니다.

(44) 프로그램 개발·변경 시 품질관리 절차 미흡

은행 내규「전산업무세칙」에 따라 IT신규 개발 및 프로그램 유지보수 사유가 발생하는 경우 현업부서는 프로젝트관리시스템을 통해 ◀◀◀에 개발을 요청해야 하고, 개발 담당 부서장은 현업부서의 요청사항을 검토하여 개발요건을 정의한 후 IT시스템 개발 및 테스트 등 일련의 프로그램 개발·변경 절차를 운용하고 있다.

그러나 은행은 사소한 오류 수정 등 단순 프로그램 개발 건은 현업부서의 요청 없이 ◀◀◀에서 자체적으로 개발사항을 프로젝트관리시스템에 등록하여 프로그램을 변경·배포하고 있으며,

◀◀◀ 자체개발 건 중 일부는 변경사유를 명확하게 기록·관리하지 않고, 일부는 특별한 사유 없이 개발기간을 장기간(□개월) 이상으로 설정하고 있어 프로그램 변경·관리에 대한 사후추적이 어려운 상태로 운영되고 있다.

또한 내규「전산개발표준화절차」에 따른 제3자 검증테스트 결과가 개발테스트 문서와 동일하거나 이전 테스트 결과서를 재사용하는 등 검증테스트 절차를 형식적으로 운영하고 있어 검증 미흡 시 프로그램 장애가 발생할 우려가 있다.

<조치할 사항>

따라서 은행 ◀◀◀는 프로그램 자체 개발 시 개발 사유·범위·기간·인수테스트 여부 등을 구체적으로 기록하고, 정기적인 점검 절차를 마련하는 등 품질관리 절차를 보완하며, 제3자 검증테스트의 품질과 실효성이 확보되도록 검증 기준과 방법 등을 구체화하여 담당자들에게 관련 교육을 정기적으로 실시하시기 바랍니다.

(45) 전산장애 관리 미흡

은행 내규「전산장애관리세칙」에 따라 장애관리자는 장애 발생 시 주요 유관부서 통보, 장애처리담당자에 대한 문제해결 요청, OOO협의체 운영 등 장애관리업무를 총괄하고, 내부적으로 장애관리기록부를 운용하고 있으며 장애 발생 건에 대해서는 부서장 이상 결재를 받아야 한다. 아울러, 계열사인 ◇◇◇에서 발생하는 장애에 대해서도 ◇◇◇ 장애관리부서에서 발송하는 공문을 접수하여 OOO협의체의 안건으로 상정하는 등 장애관리 대상을 계열사까지 확대·포함하고 있다.

그러나 은행은 장애관리 관련 내규에 장애기록관리 담당자만 지정되어 있고, 전산장애내역에 대한 기록 및 사후관리 절차 등을 명시하지 않아 전산장애에 대한 사후관리 및 조치가 미흡할 우려가 있다.

또한 ◇◇◇에서 발생하는 장애는 장애관리기록부에 기록·관리하지 않고, 일부 장애 건의 경우 내규「전산장애관리세칙」에 따른 부서장 이상 전자결재를 받지 않은 사례가 있어 장애 관리가 일부 미흡하며, 민원 발생 가능성이 있는 서비스 지연 장애 건의 경우 각 업무팀 자체 판단만으로 부서장에 대한 장애 보고 여부를 결정하고 있어 장애 보고가 누락될 가능성이 있다.

<조치할 사항>

따라서 은행은 장애기록관리 절차를 내규에 구체적으로 반영하고, ◇◇◇에서

발생하는 장애에 대해서도 은행에서 발생하는 장애 수준으로 장애 기록·관리를 하며, 내규 「전산장애관리세칙」에 따른 전산장애 건에 대한 부서장 보고가 누락되지 않도록 보고체계를 강화하는 등 업무 절차를 개선하시기 바랍니다.

(46) 일괄작업 통제절차 불합리

은행은 내규 「전산업무수행세칙」에 따라 모든 일괄작업에 대해 작업 내용을 기록·관리하고 있으며, 일괄작업 시 오류가 발생한 경우 오퍼레이터가 업무 담당자에게 연락하여 조치하고 있다.

그러나 은행은 일부 작업에서 반복적으로 발생하는 오류를 책임자에게 매일 보고하고 있으나, 동 오류 최소화를 위한 절차나 방안을 마련하지 않는 등 일괄작업의 반복 오류를 관리하지 않아 오류 발생 시 적절한 조치를 하지 못해 사고로 이어질 우려가 있다.

<조치할 사항>

따라서 은행은 반복적으로 발생하는 일괄작업 오류에 대해 오류 유형 및 사유 등을 포함한 내역을 관리하고, 주기적으로 일괄작업 오류내역을 분석하여 오류 개선방안을 마련하는 등 일괄작업 관리 및 통제를 강화하시기 바랍니다.

(47) Open API 시스템 보안성 미흡

은행은 내규 「Open API 서비스」에 따라 금융서비스 및 데이터를 표준 API로 이용기관에 제공하는 'Open API 시스템'을 구축·운영하고 있으나, 아래 (가)~(나)의 미흡점이 확인되었다.

(가) 고객정보 암호화 대상 확대 필요

은행은 내규 「정보보안 업무세칙」 등에 따라 온라인대출모집법인 등 외부 제휴기관과 API를 이용하여 주민등록번호, 고객번호, 계좌번호 등의 정보를 송수신하는 경우 AES128 알고리즘으로 안전하게 암호화하거나 마스킹 처리를 하고 있다.

그러나 은행은 고객의 휴대전화번호, 고객명, CI 정보 등의 개인정보는 암호화

대상에서 제외하고 있어 외부 제휴기관과 API를 이용하여 정보를 송수신하는 과정에서 불필요하게 고객정보가 노출될 우려가 있다.

<조치할 사항>

따라서 은행은 Open API 시스템을 통해 외부 제휴업체와 정보를 송수신하는 경우 휴대전화번호, 고객명, CI정보 등의 고객정보를 암호화 대상에 포함하는 등 고객 정보보호 대책을 강화하시기 바랍니다.

(나) Open 플랫폼 서비스 방화벽 정책 강화

은행은 내규「Open API 서비스」등에 따라 특정상황의 경우 동 서비스를 중지하거나 제한하기 위해 Open 플랫폼 GW(Gateway) 서버에서 접속 IP를 White-List 방식으로 통제하고 있다.

그러나 은행은 GW 서버에서만 접속 IP를 제한하고, 방화벽에서는 IP를 제한하지 않아 서비스 이용이 허용되지 않은 자가 내부 통신망에 접근이 허용되어 외부공격 등에 노출될 우려가 있다.

<조치할 사항>

따라서 은행은 Open 플랫폼 웹서버 및 통신망에 접근이 허용된 외부 제휴기관만 접근 가능하도록 외부 제휴기관의 IP를 서버뿐만 아니라 방화벽에도 등록하는 등 Open 플랫폼 서비스의 방화벽 정책을 강화하시기 바랍니다.

(48) 단말기 보안 통제 미흡

은행은 내규「정보보안 업무세칙」에 따라 네트워크 접근통제(NAC)를 통해 임직원이 사용하는 단말기에 문서보안시스템(DRM), 매체제어시스템(DLP), 관리자 권한 관리(AD) 등 필수 보안프로그램을 설치하도록 운영하고 있다.

또한 자동화 기기(ATM) 테스트, 해외 영업점 환경 테스트 등의 업무 목적 및 업무프로그램과 보안프로그램 간 충돌 등 현업부서 요청에 의해 보안프로그램 설치를 예외 처리할 경우 보안프로그램 적용 예외 사유, 부점 자체 통제방안, 예외 사용기한 등을 신청서에 작성 후 ◈◈◈가 검토·승인하고 있다.

그러나 ◈◈◈는 동 신청서의 부점 자체 통제방안이 다소 미흡하게 작성되었는데도, 이를 충분히 검토하지 않고 승인하고 있어 특별한 사유 없이 보안프로그램이 미설치된 단말기에서 정보 유출, 악성코드 감염 등의 문제가 발생할 우려가 있다.

<조치할 사항>

따라서 은행은 현업부서 등에서 단말기의 보안프로그램 설치 예외를 신청하는 경우 부점 자체 통제방안 및 예외 사유 등에 대한 적정성 검토 절차를 충실히 수행하는 등 단말기 보안 통제를 강화하시기 바랍니다.

(49) 전산자료 반출 관리 미흡

은행은 내규 「정보보안 업무절차」에 따라 보조기억매체(USB)에 자료를 저장하여 외부로 반출하는 경우 읽기만 가능하도록 보호조치를 적용하고, 매체제어시스템(DLP : Data Loss Prevention)을 통해 보조기억매체에 자료를 저장한 후 허용된 인원만 동 매체에 접근이 가능하도록 관리하고 있다.

그러나 은행은 문서편집을 목적으로 문서파일에 대한 암호화 조치를 예외처리하는 경우가 있으며, 동영상 파일 등은 보조기억매체에 저장 시 암호화 등 별도의 보호조치를 하지 않아 해당 전산자료가 저장된 보조기억매체를 분실 또는 도난당할 경우 전산자료가 비인가자에게 유출될 우려가 있다.

<조치할 사항>

따라서 은행은 문서파일에 대한 암호화 처리 예외 건 및 동영상 파일 등을 외부에 반출 시 암호화 등 적절한 보호조치가 적용되도록 하여 전산자료가 비인가자 등 제3자에게 유출되지 않도록 전산자료 반출 및 통제를 강화하시기 바랍니다.