경영유의사항 등 공개안

1. 금융기관명 : 우리금융캐피탈㈜

2. 제재조치일 : 2024. 6. 7.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 6건, 개선사항 21건

4. 제재대상사실

가. 경영유의사항

(1) 부동산PF대출 사업성 평가 미실시

여신전문금융업협회의「부동산PF 리스크관리 모범규준」제9조 제2항, 제3항 및 <별표1>에 따르면 자산건전성 관리를 위해 매분기 별로 부동산PF 대출 사업장별 사업성을 평가하고, 이를 반영하여 건전성 분류 및 대손충당금을 적립하여야 한다.

이에 따라 회사는 2019년 5월 부동산PF 대출 관련 사업성 평가 규정을 마련하였음에도, 사업장별 사업성 평가는 1회 실시*에 그친 사실이 있다.

* 2023년 6월에 1회 실시하였으며, 그 이전에는 개별 건에 대해 이슈(연체 등) 발생 시 비정기적(개별적) 건전성 분류만을 수행

<조치할 사항>

따라서 회사는 앞으로 부동산 PF 대출 관련하여 분기별로 전체 사업장에 대한 사업성을 평가할 수 있도록 관리하시기 바랍니다.

(2) 부동산PF 대출 리스크관리 강화

여신전문금융업협회의 「부동산PF 리스크관리 모범규준」 제2조에 따르면 부동산PF대출 사후관리를 위해 각 사업장별 모니터링을 정기적으로 실시하고, 관리대상 사업장에 대한 대응방안을 마련해야 한다.

하지만 회사는 기존 생활형 숙박시설 관련 부동산PF 대출 사업에 대하여 생활형 숙박시설을 주거용 오피스텔로 용도변경을 하지 않은 이유로 이행강제금 부과 등 조치*가 실행될 경우 대출중인 생활형 숙박시설 PF**(8건, 831억원)에 대해서 시공 포기, 분양 계획 취소, 분양률 저조, 수분양자 분양 포기 등 분양 및 시공 리스크 급증이 우려된다.

* 국토부는 2023년 10월까지 오피스텔로 용도변경 하지 않을 경우 이행강제금(공시지가 10%)을 부과할 방침(2021년 10월 발표)

** A사 등 4건 : 보통(요주의), B사 등 4건 : 양호(정상)

<조치할 사항>

따라서 회사는 부동산PF 대출 사업과 관련하여 용도변경 추진 현황, 분양률, 중도금 납부율 등을 면밀히 관리하고 충당금 추가 적립 등 대책을 마련하시기 바랍니다.

(3) 개인사업자대출 리스크관리 강화

㈎ 여신전문금융업협회의 「개인사업자대출 여신심사 가이드라인」 제13조 및 제16조에 따르면 개인사업자대출 포트폴리오 관리업종(이하 '관리업종')을 선정하여 업종별 대출현황을 모니터링하고, 한도 근접 시에는 원인을 파악하여 해당 업종에 대한 여신취급기준을 강화하는 등 적절한 조치를 취해야 한다.

하지만 회사는 관리업종 한도를 사후증액하는 과정에서 경기전망 자료 상 도소매업(관리업종의 54%)의 경기둔화 전망에도 불구하고, 도소매업 외의 업종을 포함한 업종 전망지수를 단순평균하여 경기전망이 호전되었다고 판단하여 관리업종 한도를 증액하였다.

<조치할 사항>

따라서 회사는 앞으로 업종별 익스포져를 고려하여 개인사업자대출 관리업종 한도를 설정하는 등 개인사업자대출 리스크관리를 강화할 필요가 있습니다.

㈏ 「개인사업자대출 여신심사 가이드라인」 제17조에 따르면 1억원 초과 신규 개인사업자 대출 취급시 소득대비대출비율(이하 'LTI')을 산출하여 여신심사 시 참고지표로 활용하고, LTI 구간별로 대출 추이 및 건전성 등을 모니터링하여야 한다.

하지만 회사는 검사착수일(2023. 8. 28.) 현재 1억원 초과 개인사업자 대출 취급시 LTI를 산출하여 여신심사시 높은 비율의 LTI 대출 건에 대해 LTI를 심사지표로 활용하지 않은 건이 다수 존재하는 등 LTI 활용이 미흡*한 것으로 나타났다.

* 최근 2023. 6. 19.부터 LTI를 심사지표로 활용하기 시작함

<조치할 사항>

따라서, 회사는 LTI를 여신심사 등에 적극 활용하여 높은 비율 LTI차주에 대한 상환능력에 대한 검증을 강화할 필요가 있습니다.

(4) 정보보호 관리체계 미흡

회사 내규 「J지침」에 따르면, 정보보호 조직은 보안책임자(D)와 보안책임자로부터 업무를 위임받아 세부 계획을 마련하는 보안관리자(B부장) 등으로 구성되어 있다. 정보보호 관리체계를 효율적으로 운영하기 위해서는 보안책임자가 정보보호 전략 및 주요 정책을 결정하고 보안관리자는 해당 정책을 수행하며 발생하는 문제점을 관리하는 것이 바람직하다. 또한, 정보보호 조직은 다른 부서나 이해관계자의 영향을 받지 않고 정보보호 활동을 독립적으로 수행할 필요가 있다.

하지만, 회사는 A본부 내에 B부를 배속하고 A본부장이 C와 D 이외에도 중간 관리자인 B부장까지 겸직하도록 운영하고 있다. 이에 따라 A본부장이 보안시스템 규칙의 추가, 변경, 삭제에 대한 승인 등 정보보호 부문의 일상 관리업무까지 수행하고 있어 정보보호 전략 및 주요 의사결정 등이 적기에 시행되지 않을 우려가 있다.

* 검사기준일 현재 전사 13개 본부(42개 부서) 中 A본부(3개 부서 배속)와 E본부(본부 단일 부서)만 본부장이 부서장을 겸직하고 있음

또한, 회사는 A본부의 핵심성과지표(Key Performance Indicator)를 마련할 때 디지털 전환 사업 확대 등의 사유로 정보보호 부문 평가 비중을 지속적으로 축소*하였다. 이에 따라 A본부는 IT와 정보보호 업무 간 이해 상충이 발생할 경우 IT 생산성과 효율성을 정보보호 리스크 관리보다 우선할 소지가 있다.

* A본부 핵심성과지표(KPI) 중 정보보호 비중 : (2021년) OO% → (2022년) O% → (2023년) 無

<조치할 사항>

따라서 회사는 정보보호 관리체계를 효율적으로 운영할 수 있도록 정보보호 조직·인력 운영에 관한 개선방안을 수립하시기 바랍니다. 또한, 정보보호 조직이 정보보호 리스크관리를 독립적으로 수행할 수 있도록 A본부 핵심성과지표에 정보보호 업무에 관한 항목을 반영하는 등 이해상충 방지체계를 마련하시기 바랍니다.

(5) 정보처리시스템 표준개발방법론 부재

회사는 정보화 사업을 통해 모바일뱅킹 등 정보처리시스템을 자체적으로 구축하여 운용하고 있다.

하지만 회사는 자체적인 정보처리시스템 표준개발방법론을 마련하지 않아 정보화 사업을 수행할 때마다 해당 사업수행업체의 개발방법론을 차용하고 있다.

이에 따라 일관성 없는 시스템이 구축되거나 개발·유지보수업무의 효율이 저하되고 기밀성·무결성·가용성이 충분히 테스트 되지 않은 프로그램이 운영 시스템에 반영되어 시스템 장애 등으로 이어질 우려가 있다.

<조치할 사항>

따라서 회사는 자체 정보처리시스템 표준개발방법론(시스템 아키텍처 등 포함)을 마련하여 내규에 반영하고 정보화 사업 수행 시 동 방법론에 따라 시스템 설계, 분석, 테스트 및 산출물 관리 등이 체계적으로 이루어지도록 관리하시기 바랍니다.

(6) 업무 연속성 계획 수립·운용 미흡

회사는 업무지속성 확보를 위하여 IT업무연속성 관련 비상대책을 마련하고 있으나, 아래와 같이 업무절차에 미흡한 점이 있으므로 이를 개선할 필요가 있다.

㈎ 핵심업무 선정을 위한 객관적인 절차와 기준 마련 필요

회사 내규 「O규정」, 「O지침」에서는 회사는 재해가 발생하더라도 지속적으로 수행해야 할 핵심업무를 선정하고 복구목표시간(Recovery Time Objective)과 목표복구시점(Recovery Point Objective) 등을 관리하도록 정하고 있다. 따라서 회사는 전사적 관점에서 업무영향분석(Business Impact Analysis)을 수행하여 단위업무를 도출하고 핵심 업무와 관련 시스템을 선정하는 것이 바람직하다.

하지만 회사는 전사적 관점에서 업무영향분석을 수행하지 않고 A본부가 핵심업무와 관련 시스템을 단독으로 정하고 있어 업무중단으로 인한 잠재적 손실 등의 영향도 분석 절차가 미흡하다. 또한, 핵심업무 선정을 위한 정성적·정량적 평가항목과 기준이 마련되어 있지 않아 핵심업무 선정 결과에 관한 객관성도 부족하다.

㈏ 재해복구 계획의 실효성 제고

회사 내규 「P지침」에서는 주요 전산장비에 대하여 이중화 또는 예비장치, 백업시스템을 확보하고 재해방지대책의 실효성, 적정성 등을 연 1회 이상 점검하도록 정하고 있다.

하지만 A본부는 이중화된 전산장비에 대한 전환(Fail-over) 검증을 최초 구축시에만 수행하고 있어 비상 상황 시 대기장비(Standby)로 원활하게 전환되지 않을 우려가 있다. 또한 재해복구시스템을 운용하지 않는데도 「M매뉴얼」이 재해복구시스템으로의 전환을 전제로 작성되어 있는 등 비상 대책의 실효성이 부족하다.

<조치할 사항>

따라서 회사는 전사적 관점에서 업무영향분석을 실시하고 각 업무부서가

도출한 단위 업무와 연관 시스템, 복구목표 시간 등을 F본부와 A본부가 함께 검토하시기 바랍니다. 또한 핵심업무 선정과 관련한 세부 평가항목과 객관적인 기준을 마련하시기 바랍니다.

또한, 주요 전산장비에 대한 전환 테스트를 정기적으로 실시하고 「M매뉴얼」에 마련된 재해복구계획을 재정비하여 실효성 있는 비상대책을 수립하시기 바랍니다.

나. 개선사항

(1) 부동산PF대출 건전성 평가 불합리

여신전문금융업협회의 「여신금융회사의 부동산PF 리스크관리 모범규준」 제9조 등에 따르면 여신금융회사는 개별 사업장의 사업성 및 사업진행상황 등을 종합적으로 고려하여 3단계(양호, 보통, 악화우려)로 사업성을 평가하고 이를 반영하여 부동산PF대출 관련 자산에 대한 건전성을 분류하고 적정한 대손충당금을 적립하여야 한다.

하지만 회사는 사업성이 '보통'*인 본PF 7개 사업장(7건, 861.1억원) 및 브릿지론 2개 사업장(3건, 400억원)에 대해 사업성을 '양호'로 잘못 평가하였다.

* 착공일로부터 1년 경과하였으나 실제 공정률이 계획 공정률 대비 3개월 연속 10%p 이상 하회, 분양개시일로부터 1년 경과되었으나 BEP분양율 대비 10%p 이상 하회

<조치할 사항>

따라서 회사는 사업성을 잘못 평가한 사업장에 대해 사업성 평가를 재조정하여 그에 따른 충당금(81억원)을 추가로 적립하시기 바랍니다.

(2) 부동산PF대출 분류 불합리

「여신금융회사의 부동산PF 리스크관리 모범규준」 제2조 등에 따르면 부동산PF대출은 ①특정 부동산사업 자금을 그 사업에서 발생하는 현금흐름을 상환재원으로 취급하는 대출, ②동 대출 관련 수익증권의 취득, ③그 밖에 익스포져를 발생시키는 모든 부동산PF대출 관련 행위 등으로 정의하고 있다.

회사는 ⅰ) M사 및 N사 2개 차주에 대하여 PF사업에서 발생하는 분양수익금을 담보로 대출을 취급하였고 동 대출의 상환재원이 해당 PF사업에서 발생하는 현금흐름이어서 PF대출에 해당함에도 동 대출을 부동산PF대출로 미분류(기업대출로 분류)하였으며, ⅱ) O금융투자(부동산투자신탁)가 발행한 수익증권을 인수하였고 동 부동산투자신탁은 PF대출 재원조달을 위해 설립되었으므로 회사의 동 수익증권 취득은 부동산PF대출에 해당함에도 동 대출을 부동산PF대출로 미분류(유가증권으로 분류)하였다.

한편 오산시 원동 사업장 등 1개 사업장*에 대한 대출금이 다른 PF 사업장 토지비 등의 용도로 사용되는 점을 제외하고는 기존의 PF 대출과 준공 및 분양 리스크 등 모든 리스크가 동일함에도 이를 부동산PF대출로 미분류하였다.

* 시행사의 사업이익을 담보로 시행사의 차기 사업(오산 벌음동 사업장) 부지 매입 용도로 대출(93.6억원)을 취급

<조치할 사항>

따라서 회사는 PF대출 재분류(4건, 258.6억원) 및 그에 따른 충당금(3.42억원)을 추가로 적립하시기 바랍니다.

(3) 기업대출 건전성 평가 불합리

「여신전문금융업감독규정」 제9조 제5항 <별표1> 자산건전성 분류기준에 따르면 완전 자본잠식 차주에 대한 여신은 자산건전성 분류시 '요주의'로 분류하여야 함에도, 회사는 자본잠식 유동화대출 등 5건*(318억원)에 대해 '정상'으로 분류하였다.

* 유동화대출(2건, 150억원), 브릿지론(1건, 90억원), 부실채권(NPL) 전문투자회사 대출(2건, 78억원)

<조치할 사항>

앞으로 「여신전문금융업감독규정」에 맞게 자산건전성 분류가 이루어질 수 있도록 관련 내규를 개정하고 자산건전성 분류 전산시스템을 변경하는 등 관련 업무를 개선하시기 바랍니다.

(4) 중고차 과다대출 관련 시세DB 관리 미흡

여신전문금융업협회의 「중고차 영업관행 개선 가이드라인」 제6조 등에 따르면 금융회사는 과다대출을 방지하고 중고차 시세 정보의 정확성 및 최신성 유지를 위해 내부통제 기준 및 절차를 마련해야 하나, 아래 (가), (나)와 같이 업무절차에 미흡한 점이 있으므로 이를 개선하시기 바랍니다.

(가) 중고승용차 시세DB 관리 미흡

「중고차 영업관행 개선 가이드라인」 제6조에 따르면 중고차 대출한도는 중고차 구입비용과 자체 중고차 시세DB 중 작은 금액 이내에서 산정하여야 한다.

그러나 회사가 제공받아 활용중인 중고승용차 시세DB는 해당 차종·연식의 평균 시세값으로서 개별 차량의 주행거리* 및 사고 이력**을 정확하게 반영하지 못하여 실제 중고승용차 가격보다 과도하게 높게 설정될 가능성이 있다.

* (주행거리) 주행거리가 25만km 초과 차량에 대해서만 시세에서 50% 차감함에 따라 주행거리가 20만~25만km에 해당하는 차량에 대해서는 연식 대비 주행거리가 높음에도 불구하고 시세를 그대로 반영함에 따라 실제 시세보다 시세정보 상 시세가 과다하게 되는 결과 초래

** (사고이력) 2천만원 이상 건(전체 자동차대출의 30% 수준)에 대해서만 사고 이력을 조회함에 따라 2천만원 미만 차량 사고 이력에 따른 실제 시세를 반영하는데 한계

<조치할 사항>

회사는 중고승용차 시세를 정확히 반영할 수 있도록 차량 연식보다 주행거리가 과도하게 높은 경우 초과 비율에 따라 시세 DB에서 차등 차감*하고, 사고이력 조회대상 차량범위를 확대하는 방안**을 마련하시기 바랍니다.

* (예시) 현재는 25만km 초과 차량에 대해서만 시세에서 50% 차감 → 차량 연식에 비해 실제주행거리가 평균 주행거리(연 2만km 수준)의 2배를 초과하는 경우 시세 50% 차감 등

** (예시) 조회 대상 차량 범위를 대출원금 1천만원 이상 확대 등

(나) 중고상용차 시세DB 관리 미흡

1) 「중고차 영업관행 개선 가이드라인」 제6조에 따르면 과다대출 방지를 위해 자체 중고차 시세DB를 활용하되 인터넷 상용차 거래 사이트의 실거래가격과 비교하여 중고차 시세의 적정성을 검증하고 관련 자료를 보관하여야 한다.

그러나 회사는 일부 차종의 경우 2022년식 중고상용차 시세를 2023년식 신차 가격보다 높게 설정*한 후 동 가격을 기준으로 연식에 따라 일정 비율(5%~15%)로 단순 차감하여 시세 DB를 관리함에 따라 대부분 연식에서 중고상용차 시세 DB가 실제 중고상용차 시세보다 높을 우려가 있다.

* 현대 카고 1톤 신차 가격이 2,366만원임에도 동 차량의 2022년식 시세DB는 2,570만원(200만원 초과)인 등 신차 가격을 확인할 수 있는 98종 차량 중 11종 차량의 2022년식 중고 시세가 신차(2023년식)가격 초과

<조치할 사항>

따라서 회사는 앞으로 인터넷 상용차 거래 사이트 등의 실거래 가격 반영을 의무화 하는 등 합리적인 중고상용차 시세DB 기준을 내규에 마련하시기 바랍니다.

2) 「중고차 영업관행 개선 가이드라인」 제7조에 따르면 중고차 시세 정보의 정확성과 최신성 유지를 위해 최소한 분기 1회 이상 중고차 시세정보 DB를 업데이트하여야 하나, 회사는 현재 매년 1회 시세정보 DB를 업데이트하고 있어 중고상용차 시세 정보의 정확성과 최신성 확보가 어려울 수 있다.

<조치할 사항>

따라서 회사는 앞으로 최소 분기 1회 이상 중고상용차 시세정보 DB를 업데이트하시기 바랍니다.

(5) 중고상용차 제휴점 금융사고 관련 업무 프로세스 등 불합리

여신전문금융업협회의 「중고차 영업 관행 개선을 위한 가이드라인」 제12조에 따르면 금융회사는 원칙적으로 대출금을 고객 본인계좌로 입금하여야 하지만,

고객이 중고상용차를 주요 영업수단으로 사용할 것이 객관적으로 확인된 경우에는 제휴점, 중고차 판매직원 또는 채무자가 지정하는 금융회사에 직접 지급할 수 있음에도 불구하고,

차주 소유 차량을 담보로 대출을 실행(담보대출)하거나 기존 대출 금융회사에 대출금을 직접 지급하는 방법으로 대출을 실행(환승론)할 경우 제휴점이 아닌 차주 본인 혹은 기존 대출 금융회사에 대출금을 직접 지급하는 것이 대출금 편취 등 금융사고 예방 측면에서 바람직하다.

이에 회사는 내부지침*으로 담보대출은 채무자, 환승론은 채무자와 기존 금융회사에 대출금을 지급하도록 하고 있음에도 불구하고, 본부장 전결을 통해 일부 대출 건에 대해 여전히 제휴점에 대출금을 지급하고 있음에 따라, 대출금 편취 등 금융사고 예방을 위해 내부지침 제정 취지가 몰각되고 동 지침이 형해화 될 우려가 있다.

* 중고상용차 상품별 할부금 송금방식 변경

<조치할 사항>

따라서 회사는 채무자(담보대출) 및 기존 대출처(환승론)에 대한 대출금 직접 지급 예외와 관련하여 예외 적용 최소·객관화 등을 위해 예외 사유 및 기준 절차 등을 마련하시기 바랍니다.

(6) 셀프대출 취급절차 불합리

셀프대출은 임직원 본인 또는 가족 명의 대출 심사과정에서 이해 상충* 문제가 발생함에 따라 법령** 및 내규 위반** 가능성이 상존하므로 회사는 금융사고가 발생하지 않도록 내부통제절차를 적절히 갖추어야 한다.

* 회사의 이익을 해하지 않아야 하는 대출담당자로서의 지위와 낮은 금리 등 유리한 조건의 대출을 추구하는 고객으로서의 지위 충돌

** 서류위조, 전결권 위반, 금리·한도·담보평가 부적정, 용도외 유용 등

하지만 회사는 이와 관련하여 별도의 제한규정을 마련하지 않은 채 셀프대출*을 취급함에 따라 2019년 4월부터 2020년 5월까지 기간 중 동 사 직원이 부친 등의 명의로 자동차 대출(2건, 0.8억원)을 취급(기안)한 후 자동차 매각대금을 편취(관련 서류 위조 등)하는 등 금융사고가 발생하였다.

* 임직원 및 가족(배우자, 본인·배우자의 직계존비속, 형제자매 등)에 대한 대출 중 임직원 본인이 기안자, 중간결재자 또는 전결권자로 직접 관여한 대출

<조치할 사항>

따라서 회사는 앞으로 셀프대출 취급 시 임직원 본인은 심사·결재라인에서 제외하고, 준법감시인 대상 신고의무를 부여하도록 하는 등 관련 내규를 마련하시기 바랍니다.

(7) 금리인하요구권 운영기준 미흡

「여신전문금융업법」 제50조의13 제1항에 따르면 차주는 소득재산 증가나 신용등급 또는 개인신용평점 상승 등 신용상태 개선이 나타났다고 인정되는 경우 금리인하를 요구할 수 있다.

하지만 회사 내규 「금리인하요구권 운영기준」에서는 금리인하 수용으로 인한 금리 재산정 시 복수의 신용상태* 개선이 발생하여도 중복 적용이 불가하여 금리인하 폭을 제한하거나, 신용도 외에 소득요건을 추가하면서 전결권을 상향한 본부장** 예외 승인을 얻도록 함으로써 회사가 금리인하 요구를 과소 수용할 우려가 있다.

* 소득재산 증가 : 소득 증가(취업, 승진, 이직, 전문자격 취득 등), 재산 증가(자산 증가, 부채 감소)
신용도 상승 : 신용평가회사의 개인신용평점 상승
기타 : 차주가 신용상태 개선으로 판단하는 사항(고객요청)

** 통상 금리인하요구 승인은 지점장 전결 사항

<조치할 사항>

따라서 회사는 앞으로 자동차금융 관련 금리인하요구권 운용 시 금리인하요구를 과도하게 제한하여 과소 수용될 우려가 있는 관련 내규*를 정비하는 등 관련 업무를 개선하시기 바랍니다.

*「금리인하요구권 운영기준」

(8) 중도상환 고객에 대한 청약 철회 안내 미흡

여신전문금융업협회의 「여신금융회사 표준 여신거래기본약관」 제4조의2에 따르면 금융회사는 채무자가 청약 철회의 의사 표시를 명확하게 하지 않을 경우 청약 철회에 대해 설명하고 채무자의 의사를 확인하여 처리하여야 하며, 이에 따라 회사는 2019년 6월 고객의 청약 철회권 보장 강화*를 위해 ①청약 철회가 가능함을 별도로 추가 안내**한 후, ②중도상환신청서를 징구***하도록 하는 내용의 내부지침을 마련하였다.

* 대출계약 체결 후 14일 이내 중도상환 요청 고객 대상
** 팝업, 문자 발송, 구두 설명 등으로 고객의 의사(청약철회 또는 중도상환)를 명확히 확인
*** 향후 고객민원 방지를 위해 별도의 신청서 필수 징구

하지만 회사는 2020년 1월 1일부터 2021년 11월 26일 기간 중 중고차 대출계약 체결 후 14일 이내 중도상환차주 대상(13명)에게 청약 철회가 가능함을 추가 안내하지 않았고, 2020년 1월 13일부터 2023년 3월 21일 기간 중 중도상환 고객(32명)으로부터 중도 상환신청서를 징구하지 않았다.

<조치할 사항>

따라서 회사는 앞으로 대출고객이 중도완납 의사를 표시하는 경우 청약 철회 관련 추가 안내 등이 누락되지 않도록 관련 프로세스 등을 개선하시기 바랍니다.

(9) 이사회 내 위원회 운영 규정 미흡

회사 내규 「이사회규정」 제7조 제1항 제7호에서 '중요 규정의 제정 및 개폐에 관한 사항'을 이사회에서 결의하도록 정하고 있고, 제7조 제1항 제7호 바목에서 리스크관리규정을 중요 규정의 하나로 열거하고 있다.

그러나 회사는 제7조 제1항 제7호 바목 단서조항에서 '리스크관리위원회 규정이 정한 바에 따라 리스크관리위원회에 리스크관리규정의 제정 및 개폐에 관한 사항을 위임할 수 있다'고 정하는 등 하위규정에서 이사회 결의사항의 위임에 대해 정하고 있다.

<조치할 사항>

따라서 회사는 앞으로 이사회의 결의사항을 위임하는 경우 「이사회규정」에 직접 정하도록 관련 내규를 정비하시기 바랍니다.

(10) 금융사고 보고 절차 관리·감독 미흡

「금융기관 검사 및 제재에 관한 규정」 제41조 등에 따르면 금융기관은 금융사고 발생 시* '지체없이' 금융감독원장에게 사고 보고를 하여야 한다.

* 소속 임직원이 스스로 위법·부당행위를 함으로써 당해 금융기관 등에 손실을 초래하거나 금융질서를 문란하게 한 경우로서 형법과 관련된 범죄혐의가 있는 경우

그러나 회사는 2020년 8월 7일 금융사고에 대한 제보를 접수한 후 특별감사를 실시하여 범죄혐의를 확인하고도 금융감독원에 지체없이 보고하지 않았다.

<조치할 사항>

따라서 회사는 앞으로 금융사고 보고가 지연 및 누락되지 않도록 금융사고 보고 절차 관련 관리·감독을 강화하시기 바랍니다.

(11) IT자체감사 업무 불합리

회사 내규 「Q지침」에 따르면 IT자체감사자는 IT영역의 제반 활동을 적정하게 수행하는지를 점검하기 위해 정기감사는 연간 1회 이상, 일상감사는 상시적으로 실시하여야 한다.

하지만 A본부는 연간 자체감사계획을 수립하는 절차를 마련하지 않고 있으며, 자체감사인이 퇴직 등의 사유로 2022년 종합감사와 3·4분기 일상감사를 실시하지 않았다. 또한, IT자체감사자가 전자금융사고의 근본적인 원인과 재발방지 대책 등에 대한 적정성을 검증하지 않아 동일한 유형의 전산사고가 반복적으로 발생*하고 있다.

* 검사대상기간 중 신용정보 기관인 P사의 전산장비 문제로 대출한도 산정 지연이 총 4건 발생

<조치할 사항>

따라서 회사는 연간감사계획을 수립하는 절차를 내규에 반영하시기 바랍니다. 또한, IT자체감사자가 사고 책임부서와는 별도로 전자금융 사고원인과 재발방지 대책 등의 적정성을 일상감사 등을 통해 검증하시기 바랍니다.

(12) 정보처리시스템 사업관리 불합리

회사 내규 「R지침」에서는 정보보호위원회가 정보기술부문 계획서*에 관한 사항을 심의·의결하고 대표이사에게 보고하도록 정하고 있다. 따라서 회사는 정보기술부문 계획에 따라 실효성 있는 IT사업 계획을 수립하고 예산을 관리하는 것이 바람직하다.

* 정보기술부문의 추진목표 및 추진전략, IT사업 추진계획 및 예산 등 포함

하지만 A본부는 IT사업 취소·변경에 대한 재심의 절차를 마련하고 있지 않아 당해 연도에 계획된 IT사업이 취소되거나 차년도로 이월되는 비율이 40.6%로 다소 높고, 최근 3년간 IT자본예산의 평균 집행률도 평균 48%에 불과하다. 이에 따라 중요 IT사업에 차질이 발생하거나 IT예산이 비효율적으로 집행될 가능성이 있다.

<조치할 사항>

따라서 회사는 계획된 IT사업을 추진하지 않거나 연기하는 경우에는 정보보호위원회 등의 의사결정기구에서 변경 사유의 타당성을 재심의·의결하도록 IT사업 및 예산관리 절차를 강화하시기 바랍니다.

(13) IT·정보보호 부문 내규관리 체계 불합리

회사 내규 「N규정」에 따르면, '규정'은 회사의 전반적인 조직·업무에 관한 사항을 정의한 것이고 '규칙'은 규정에서 위임된 사항의 시행이나 회사업무 전반에 영향을 주는 업무에 관한 것이며, '지침'은 규정·규칙에서 위임된 사항과 개별 부서에서 일상적으로 실시하고 있는 업무절차로 정의하고 있다.

따라서 회사는 상위 내규에서 하위 내규에서 규정할 사항을 위임하는 등 내규 간 위임관계를 마련하여 업무수행에 대한 근거와 권한을 명확히 규정할 필요가 있다.

하지만 A본부는 IT·정보보호 부문 업무처리 기준과 절차를 00개 내규로 정하면서 상위 규정에서 정하지 않은 업무절차를 하위 규정에서 임의로 제정·운용하거나, 근거를 명확히 마련하지 않고 업무를 수행하는 등 내규 관리체계가 적절하지 않다.

* (IT) G규칙, H지침 등 0개
  (정보보호) I규정, J지침 등 00개

또한, 회사업무 전반에 영향을 주는 업무를 「J지침」, 「K지침」, 「L지침」, 「M매뉴얼」 등 A본부장 전결로 개정할 수 있는 지침이나 「N규정」에서 규정하고 있지 않은 매뉴얼로 관리하고 있다.

<조치할 사항>

따라서 회사는 상위 규정에 IT·정보보호 부문의 업무수행에 대한 근거와 권한을 명확히 규정하시기 바랍니다. 또한, 구체적인 업무절차와 방법을 하위 규정에서 정하는 경우에는 위임 근거를 마련하여 임직원이 동 지침에 근거하여 업무를 수행할 수 있도록 내규관리 체계를 재정비하시기 바랍니다.

(14) 정보처리시스템 감리업무 관리 불합리

회사는 정보처리시스템의 안전성 및 효율성 확보를 위하여 감리 대상, 감리인 자격, 감리 절차 등에 대한 자체 감리기준을 수립하고 있으나 아래와 같이 정보처리시스템 감리업무에 미흡한 점이 있으므로 이를 개선할 필요가 있다.

(가) 외부업체에 의한 정보처리시스템 감리 절차 마련 필요

회사 내규 「S지침」에서는 감리 대상·조직·시행 등 감리 관련 업무절차를 정하고 있다.

하지만 이 지침은 내부직원에 의해 정보처리시스템 감리(이하 “내부감리”)가

수행되는 경우를 위주로 작성되어 있어 외부업체에 의한 감리수행(이하 “외부감리”) 시 필요한 업체 선정기준(고려사항), 감리항목, 관리체계 및 보고 절차 등이 규정화되어 있지 않다.

이에 따라 외부업체에 의한 정보처리시스템 감리가 체계적으로 수행 및 관리되지 않을 우려가 있다.

(나) 정보처리시스템 감리대상 판단 불합리

현재 회사는 내부감리를 수행하지 않고 있으며 외부감리는 전산운영위원회를 통해 정보화 사업에 대해 심의·의결을 하면서 자체 기준*을 활용하여 수행 여부를 함께 결정하고 있다.

* 내규「H지침」내 ‘정보시스템 감리대상 판단기준’ ①정보시스템 특성(대고객 핵심 서비스 여부, 신기술 적용 여부 등), ②사업비 규모(10억 원 초과 여부), ③사업 특수성(금융지주 공동구축 여부 등)

하지만 회사는 상기 자체 기준 중 ‘사업비 규모‘를 주로 고려함으로써 사업비가 10억 원을 초과하는 경우에만 외부감리를 수행하고 있다.

이에 따라 사업비가 10억 원 이하인 대고객 및 내부 핵심 업무 관련 정보화 사업은 정보처리시스템 감리가 수행되지 않고 있으므로 사업관리가 소홀하게 되는 경우 심각한 오류 및 일정 지연 등이 발생하여 대·내외 업무에 지장을 초래할 우려가 있다.

<조치할 사항>

따라서 회사는 정보화 사업별로 적용 가능한 정보처리시스템 감리유형(내부, 외부 등)을 정하고 각 감리유형별로 필요한 업무절차를 구체적으로 마련하여 관련 내규에 반영하시기 바랍니다.

또한 정보화 사업추진 시 ‘정보시스템 감리대상 판단기준’ 내 항목을 균형 있게 고려하여 감리수행 여부를 판단하고 정보화 사업이 대고객 및 내부 핵심 업무에 해당하는 경우에는 내부 또는 외부 감리를 실시하도록 업무를 개선하시기 바랍니다.

(15) 프로그램 변경관리 통제 불합리

회사는 내규 「T지침」에 따라 프로그램 개발·변경·삭제 관련 승인, 테스트 및 운영환경 배포·검증, 일괄작업 관리에 대한 업무절차를 마련하고 IT서비스관리 시스템(이하 'ITSM')을 통해 프로그램 변경요청에 대한 승인, 테스트 및 제3자 검토 등을 수행하고 있다.

하지만 회사는 프로그램 변경요청 및 요청사항 접수시에만 팀장 등 책임자가 승인하고 종결시에는 책임자가 처리내용의 적정 여부를 확인하지 않고 있다.

또한, 검사대상기간 중 프로그램 변경요청 2,818건(18.6%, 전체 15,071건)은 프로그램 변경 전에 변경될 내용을 ITSM에 기록하고 있으나 테스트 결과 등 처리결과는 기록하지 않아 변경 관리가 다소 미흡하다.

이에 따라 프로그램 세부 변경 내용이 확인되지 않거나 불충분한 테스트로 인해 오류가 발생하는 등 관련 업무가 비효율적으로 수행될 우려가 있다.

<조치할 사항>

따라서 회사는 책임자가 ITSM을 통해 프로그램 변경 요청·접수·완료 시 처리내용의 적정성 등을 확인 후 승인하고 담당자 및 책임자의 승인 이력도 모두 표시되도록 조치하시기 바랍니다.

또한 처리내용 및 테스트 결과 등 중요 항목은 필수 입력항목으로 지정하여 프로그램 변경 관련 주요 내용이 누락되지 않도록 개선하시기 바랍니다.

(16) 일괄작업 통제 및 관리 불합리

회사 내규 「T지침」 제17조에서는 장애 및 긴급상황 등의 사유로 인해 별도로 일괄작업을 수행해야 할 때는 작업요청서에 대해 부서장의 사후 승인을 득하도록 정하고 있다.

하지만 IT담당자가 긴급 일괄작업 수행에 관해 작업요청서에 작업내용을

지나치게 요약하여 기록하고 있어 부서장의 사후검토 시 긴급 수행에 대한 정당성 확인이 곤란할 우려가 있다.

또한 동 내규에 긴급으로 수행 가능한 일괄작업 대상 및 세부 절차 등이 마련되지 않아 일괄작업이 무분별하게 남용되거나 체계적으로 수행되지 않을 우려가 있다.

<조치할 사항>

긴급으로 수행 가능한 일괄작업 대상 및 세부 절차를 내규에 마련하고 사후검토 시 정당성 및 절차 준수 여부 등에 대해 철저히 확인하시기 바랍니다.

(17) 전산원장 변경통제 불합리

전산원장 변경 시 현업담당자는 IT서비스관리시스템(ITSM)을 통해 작업요청서를 등록하고 IT담당자(개발자)는 동 요청서를 접수 후 소속 부서장의 승인을 받아 원장변경관리시스템(DMS)을 통해 변경하도록 정하고 있다.

하지만 IT담당자는 작업요청서에 따른 변경작업을 수행해야 하는데도 업무 편의를 위해 기존 작업요청서를 재사용*하여 다른 변경작업을 처리하는 경우**가 있어 전산원장 변경이력의 추적관리가 어렵고 작업이 임의로 수행될 우려가 있다.

* 2020. 1. 1.~2023. 6. 30. 원장 변경 총 4,748건 중 1,160건이 기존 작업 요청서 재사용
** 당초 요청사항은 정보 수정이었으나, 동 요청 건을 재사용하여 수정, 원상복구, 삭제 수행 등

또한 변경작업 완료 후 IT담당자가 원장변경관리시스템의 처리결과를 기록*하면서 추상적으로 작성하거나 지나치게 요약하고 있어 원장변경 이력 관리 및 정당성에 대한 제3자 검토가 제대로 수행되지 않을 우려가 있다.

* 원장변경관리 시스템 내에 일정한 규격 없이 작성자 임의로 처리결과 작성

<조치할 사항>

따라서 회사는 현업담당자가 요청한 사항에 대한 변경작업만 수행될 수 있도록 기존 작업요청서를 재사용하지 못하게 하는 등 IT서비스관리시스템(ITSM)을 수정·보완하고 내부감사자 등이 처리결과를 제대로 확인할 수 있도록 전산원장 변경통제를 강화하시기 바랍니다.

(18) 전산자료 보호대책 불합리

회사는 비인가자에 의한 중요정보 유출, 도난 등의 피해를 방지하기 위해 내규 「L지침」 등을 마련하고 망연계솔루션, 문서보안시스템(DRM) 등 정보보호 시스템을 운영하고 있으나, 아래와 같이 전산자료 보호 대책이 다소 미흡하므로 이를 개선할 필요가 있다.

(가) 공유폴더 관리 미흡

회사는 업무인계 및 부서자료 공유 목적 등으로 파일서버(NAS*)를 이용해 공유폴더를 구축·운영하고 있으며 임직원은 보안정책관리시스템을 통해 소속 부서장 및 준법감시부 승인을 받아 공유폴더를 이용하고 있다.

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

공유폴더를 사용할 때는 비인가자에 의한 내부자료 유출 및 변조 등을 방지하기 위해 최대 사용기한 등을 설정하고 부서 이동 등 인사변동시에도 권한 회수가 이루어지도록 관리 절차를 갖춰야 한다.

하지만 회사는 공유폴더를 운영하면서 최대 사용기한 등 공유폴더와 관련된 기본정책을 마련하지 않고 있으며 인사변동시에도 부서 공유폴더에 대한 권한 회수를 하지 않은 사례가 있다. 또한 공유폴더 내 전산자료 저장 시 문서보안시스템(DRM)을 통한 파일 암호화가 적용되지 않는 등 전산자료 보호대책이 다소 소홀하다.

(나) 정보보호시스템 관리·통제 소홀

회사는 중요정보 유출 방지 등을 위해 망간 자료전송 시 망연계솔루션을 통해 책임자(부서장 이상) 승인 후 자료를 외부로 반출하도록 정하고 있다.

하지만 일부 직원*에게 망연계솔루션 자가승인 권한을 부여한 사례가 있는 등 관리·통제가 다소 소홀하다.

* 내부직원 1명, 외부직원 3명

<조치할 사항>

따라서 회사는 임직원 간 업무자료 공유가 필요한 경우에는 공유폴더가 아닌 사용자 및 권한관리, 파일 반출입 이력, 파일 암호화 등 사용통제가 가능한 웹디스크 시스템을 도입하여 전산자료에 대한 보호대책을 강화하시기 바랍니다.

또한 내·외부 직원에게 부여된 망연계솔루션 자가승인 권한을 모두 회수하고 권한 부여 및 파일 전송 내역의 적정성을 정기적으로 점검하는 등 관리·통제를 강화하시기 바랍니다.

(19) IP주소 부여·관리 불합리

회사 내규「I규정」제21조에서는 업무영역의 네트워크를 물리적 또는 논리적으로 분리하고 각 영역 간 접근통제를 적용하도록 정하고 있다. 따라서 회사는 개발·운영·테스트 등 업무영역별로 네트워크를 분리하여 IP주소를 할당하여야 한다.

하지만 회사는 개발서버와 일부 운영서버에 동일 대역의 IP주소를 할당하고 있어 개발서버에서 외부침입 또는 악성코드 감염 등의 보안사고가 발생할 경우 운영 서버에까지 피해가 확산될 위험이 있다.

* 전체 운영서버 ◈대 중 ▣대(○○.○%)가 개발서버와 동일한 IP대역에 혼재되어 할당

또한, 회사는 PC 등 단말기 보안정책을 내부·외부직원별로 분리하여 적용하고 있는데, 위와 같이 IP주소 대역이 잘못 할당된 사례가 있어 IP주소 대역을 기준으로 보안정책을 적용할 경우 보안정책이 잘못 적용될 우려가 있다.

<조치할 사항>

따라서 회사는 서버 유형별(운영·개발·테스트 등) 및 단말기 유형별(내·외부직원, 직무 등)로 IP주소 할당정책을 수립하고 현재 운영 중인 전산장비에 부여된 IP주소를 일제히 점검하여 정책에 맞게 정비하시기 바랍니다.

(20) 외부주문 관리 및 통제 불합리

회사는 정보보호 운영업무를 외주업체(Q사)에 위탁하고 안정적인 서비스 수준 보장 등을 위해 외주업체와 서비스수준협약(SLA)을 체결하여 업무지시 이행 수준 등 14개 평가지표에 대해 매월 서비스 수준을 평가하고 있다.

하지만 B부는 정보보호 운영업무를 수행하는 외주직원(2명)에게 방화벽, 매체제어 등 정보보호시스템의 관리자 권한을 부여하였는데도 외주직원의 업무 수행내역* 등에 대한 적정성을 점검하는 절차를 마련하고 있지 않다.

* 특권계정 생성·권한변경, 보안정책 변경 및 예외처리, 전산자료·데이터 전송 이력 등

이로 인해 우리금융캐피탈㈜의 요청 및 승인 없이 외주직원이 임의로 권한을 부여하거나 보안정책을 예외 처리하는 등 외주직원에 의한 임의의 작업이 수행될 우려가 있다.

<조치할 사항>

따라서 회사는 외주직원에 의한 IT 사고 예방 등을 위해 서비스 수준 평가 시 관리자 권한을 보유한 외주직원의 작업내역에 대한 적정성을 평가*하는 등 보안업무에 대한 외부주문 관리·통제를 강화하시기 바랍니다.

* 보안작업 절차를 준수하지 않은 임의의 작업 건수 등

(21) 무선통신망 통제 불합리

회사 내규 「I규정」 제21조 및 「L지침」 제7조에서는 비인가 무선접속장비(AP : Access Point)의 접속통제 등을 위해 무선침입방지시스템(WIPS*)을 설치·운영하도록 정하고 있다. 이에 따라 B부는 본사 및 전산센터에 총 ▲대의 무선침입방지시스템을 설치·운영하고 있다.

* WIPS(Wireless Intrusion Prevention System) : 비인가 무선 네트워크를 차단하는 시스템

하지만 회사는 임원회의 목적 등으로 임원실에 무선통신망을 운영하면서도

무선침입방지시스템을 적용하지 않고 있다. 또한 전산센터 내 관제실에 무선침입방지시스템을 설치·운영하면서도 일부 무선통신망*에 대해서는 차단 정책을 적용하지 않는 등 무선통신망에 대한 관리·통제가 다소 미흡하다.

* 동 전산센터(○층)를 이용하고 있는 타 회사에서 업무목적으로 설치·운용 중인 무선통신망

이에 따라 비인가 무선접속장비에 의한 내부자료 유출 등 IT보안사고가 발생할 우려가 있다.

<조치할 사항>

따라서 회사는 임원실에 무선침입방지시스템을 적용하여 허용된 사용자만 무선통신망에 접속할 수 있도록 조치하고 전산센터 내 무선통신망 사용을 금지하는 등 IT보안사고 예방을 위해 무선통신망 관리·통제를 강화하시기 바랍니다.