경영유의사항 등 공개안

1. 금융회사명 : 삼성카드㈜

2. 조치일 : 2024. 1. 26.

3. 조치내용

대상	내 용
기관	경영유의 5건, 개선 14건

4. 조치대상사실

가. 경영유의사항

(1) 개인사업자 대상 여신성 상품 심사기준 강화

회사는 개인카드 회원이 의약품, 유류 등의 물품구매 또는 대금지급 등의 사업목적을 위해 한도 증액을 요청하면 해당 사업의 매출규모 등을 감안하여 예외한도(최대 OO억원)를 부여하고 있으나*,

* 사실상 약사 등 개인사업자를 대상으로 한 여신성 상품으로 관련 심사기준(자격 및 한도기준) 등은 내부 품의로 마련·운용

예외한도를 매출액과 소득금액 중 큰 금액으로 인정하거나, 소득금액 산출을 위한 신고소득이 현저히 낮은 경우 개인카드 회원이 소득을 축소 신고한 것으로 가정하여 유리한 추정소득을 인정하는 등 일부 예외한도 심사기준이 불합리하게 마련·운용되고 있으므로

앞으로 개인사업자에 대하여 여신성 상품을 제공할 경우 해당 사업자의 신용상태를 평가하고 영업이익 기준을 원칙으로 하여 추가한도를 결정하는 등 관련 심사기준을 강화하고 이를「개인회원 한도관리 지침」 내규에 반영하시기 바람

(2) 비여신성 자산에 대한 신용리스크 관리 강화

「여신전문금융업감독규정」 제12조제2항에 따라 회원과의 여신거래에 의해 발생된 채권을 대상으로 신용리스크 한도를 설정하고 매분기 리스크한도 소진율 등의 점검결과를 리스크관리위원회에 보고하고 있으나

마케팅 활동 등에 따른 제휴업체와의 계약에서 발생하는 거액 미수금을 회수하지 못하는 등* 비여신성 자산의 신용리스크가 확대되고 있으므로

* 제휴사(A) 부담금 미입금 사고(금액 OOO억원) : 회사가 마케팅 비용을 선부담하고 2개월 후 제휴사로 부터 후취 정산하는 구조로 미상환 리스크를 고려하지 못해 발생

신용리스크 관리의 측정대상을 비여신성 자산으로 확대하고 거래상대방의 계약불이행으로 인한 리스크 부담을 일정수준 이하로 유지하는 등 비여신성 자산에 대한 신용리스크 관리를 강화하시기 바람

(3) 자문역·고문제도 운영 및 관리 절차 미흡

내규「직제규정」 제6조에 따라 자문역·고문 제도를 운영*하고 있는데, 위촉기간 및 자문범위 등 제도운영에 관한 구체적 사항을 세부적으로 정하고 있지 않아 임의적으로 운영될 우려가 있으므로

* 2019년 이후 자문역 O명, 고문 O명 위촉하였고, 검사종료일 현재 자문역 O명 재임중

앞으로 자문역·고문 제도에 관하여 위·해촉 절차, 위촉기간, 자문범위, 보수 등 세부사항을 포함한 내규를 마련하고, 활동실적에 대한 정기적인 취합·보고 절차를 수립하는 등 자문역·고문제도에 대한 구체적인 운영·관리절차를 마련하시기 바람

(4) IT부문 내규관리 강화

검사착수일(2023.5.22) 현재 IT·정보보호 부문의 효율적인 조직 운영과 업무수행을 위하여 총 OO개 내규를 마련하여 IT부문 업무처리 기준과 절차 등을 규정하고 있으나

내규 '사규 운영 및 관리지침' 및 '위임전결규정' 등에서 정하지 않은 업무가이드 등 내규를 임의로 제정·운용하거나 근거를 명확히 마련하지 않고 업무를 수행하는 등 회사의 경영방침 및 규범이 준수되지 않는 경우가 있고

내규와 관련된 일부 중요 문서양식(보고서, 체크리스트. 기준 등)은 내규화되지 않고 실무자 등이 개별 관리하고 있어 표준화되지 않거나 적시에 변경사항 등이 반영되지 않을 우려가 있으므로

현행 IT·정보보호 부문 내규의 제정/개정/폐지 및 업무 수행에 대한 근거 및 권한 등을 '사규 운영 및 관리지침' 등 관련 상위 내규에 마련하고 내규 종류별 정의 및 용도 등을 명확히 구분함으로써 내규가 체계적으로 구성되도록 정비하며

내규 관련 중요 문서양식은 해당 내규에 부속시켜 표준화하고 효율적으로 관리되도록 하는 등 내규 관리체계를 강화하시기 바람

(5) 통합 금융플랫폼 운영리스크 관리체계 강화

계열사(A·B·C)와 금융플랫폼 공동 구축 협약서를 체결하여 협약기관간 비용·수익 정산, 소유권·지식재산권 등에 관한 사항을 정하고 ㉮ 등 계열사 모바일 앱에서 운영하던 서비스를 통합 금융플랫폼(모니모)으로 이관하고 있으나

회사의 전산시스템에 장애·재해 등이 발생하여 모니모 접속이 중단될 경우 계열사에서 모니모로 이관한 서비스*를 지속하기 위한 대체 수단이 마련되어 있지 않아 통합 금융플랫폼 운영업무에 관한 업무지속성이 담보되지 않을 위험이 있고

* ㉮, ㉯ 등 OO개 서비스

계열사에서 모니모 관련 프로그램 또는 전산 인프라를 변경하는 경우 삼성카드가 테스트 결과 및 영향도 평가에 관한 자료를 제출받아 사전에 검증하지 않고 서비스의 정상 동작 여부만 사후적으로 확인하고 있어 프로그램 또는 전산 인프라 변경의 안전성을 객관적으로 검증하기 어려우므로

회사의 전산시스템 장애로 모니모 접속이 중단될 경우 계열사에서 이관한 서비스를 지속하기 위한 대체 수단* 등을 마련하고, 계열사에서 모니모 관련 프로그램 또는 전산 인프라를 변경하는 경우 삼성카드가 테스트 결과 및 영향도 평가에 관한 자료를 제출받아 체크리스트 등을 통해 사전 검증하는 절차를 마련하시기 바람

* (예시) 계열사의 모바일 웹서비스 등으로 연결하는 접근경로 제공

나. 개선사항

(1) 신용카드 발급시 본인확인 절차 강화

회사는「여신전문금융업법」제14조 제2항에 따라 신용카드 발급 시 본인이 신청한 것인지 확인하고 있으나, 아래와 같이 일부 미흡한 사항이 있으므로 신용카드 발급 시 본인확인 절차를 강화하시기 바람

① 모집인을 통한 신용카드 발급신청시 가입신청용 태블릿상 신분증 촬영이 어려운 경우 ARS를 통해 주민등록번호를 입력하는 방식으로도 신용카드 발급이 가능한 바, ARS를 통한 본인확인절차가 명의도용의 취약지점이 되는 점을 감안하여 신분증 촬영 방식으로 일원화할 필요

② 디지털 채널(Web, App)을 통한 신청 시 실명확인 및 휴대폰 인증만으로 제3자의 카드수령을 허용하고 있으나, 알뜰폰 인증의 경우 명의를 도용한 전화가입 사례가 상대적으로 빈번한 점을 감안하여 중첩적인 확인 절차*를 적용할 필요

* 신분증 진위확인, 1원 송금, 영상통화, 본인 지정배송 중 택 2

③ 추가적인 본인확인이 필요한 유의심사* 과정에서 신청서 기재정보(결제은행, 카드 수령지, 결제일 등)만을 확인하고 있는 바, 타 금융기관의 최근 금융거래 정보(신용평가사 집적) 등을 확인하여 실효성을 제고할 필요

* 태블릿으로 카드 신청 시 휴대폰 미인증 고객 중 신청서 상의 휴대폰 번호와 KCB 휴대폰 번호가 불일치 하는 경우 유의 심사 진행

(2) 카드상품 수익성 분석 관리 강화

여신전문금융업협회의「카드상품 수익성 분석체계 가이드라인」제4조 등에 따르면 회사는 카드상품 수익성 분석과 관련하여 합리적인 세부산정 기준을 마련·운용하여야 함에도

2022.1.1.~ 2022.12.31 기간 중 ㉮ 카드 등 7개 리뉴얼·사업자 전용 카드의 사업성 분석시 3개 카드에 대해서는 '全카드 평균 회원서비스비용률(OO%)'을 적용하였

으나, ㉯ 제휴카드 등 4개 카드에 대해서는 합리적인 이유 없이 '유사카드 평균 회원서비스비용률(OO%)'을 적용하는 등* 세부적인 수익·비용 산정기준이 마련하지 않고 비용 산정비율을 자의적으로 적용한 사례가 있었으므로

* ㉯ 제휴카드에 대해 '全카드 평균 회원서비스비용률' 적용할 경우 수익성이 적자로 전환 (손실률 OO%)

앞으로 상품개발시 합리적인 수익성 분석이 이루어질 수 있도록 구체적인 산정기준(매뉴얼 등)을 마련·운영하는 등 관련 업무를 개선하시기 바람

(3) 리볼빙서비스 수수료율 비교 안내 강화

리볼빙서비스(일부결제금액이월약정, 이하 '리볼빙') 상품설명서에서 리볼빙과 유사한 성격을 띤 다수 유사상품[1]의 수수료율을 비교 안내하여 고객의 상품 선택권과 권익을 보장하고 있으나,

신용평점에 대한 구분 없이 전체 평균수수료율만을 안내함에 따라 고객 입장에서 자신의 신용평점 수준에서 가장 유리한 수수료율 상품을 선택하기 어려운 실정[2]이므로

1) 분할납부서비스, 현금서비스, 카드론
2) 리볼빙의 경우 우량고객 중심으로 영업하고 있어 현재 비교 안내 체계에서 사실과 다르게 유사상품 대비 수수료율이 현저히 낮아 보이는 현상 발생 가능

실제로 고객이 자신이 속한 신용평점 대에서 자신에게 가장 유리한 상품을 선택할 수 있도록 신용평점 구간별 수수료율 데이터를 함께 안내하는 방식으로 리볼빙 상품설명서를 개선할 필요

* (예시) ① 전체 평균 수수료율, ② 신용평점 900점 초과군 평균 수수료율, ③ 700점 초과 900점 이하군 평균 수수료율, ④ 700점 이하 평균 수수료율

(4) 전화마케팅(TM) 통화품질 관리 업무 강화

내규「전화마케팅 지침」등에 따라 A팀·B팀·C팀(이하 '영업부서')과 D팀·E팀(이하 'QA부서')이 각각 전화마케팅 위탁업체(이하 'TM업체')의 표준스크립트 준수 여부, 불완전판매 여부 등을 점검하고 있으나, 일부 미흡사항이 있어 아래와 같이 전화마케팅(TM) 통화품질 관리 업무를 강화하시기 바람

① 부가상품 TM의 불완전판매 점검 강화

2023.1월부터 카드회원을 대상으로 부가상품(쇼핑케어) TM을 수행하고 있으나 QA부서에서 금융상품이 아니라는 이유로 해당 TM에 대한 점검을 실시하지 않고 있어 불완전판매 등으로 인한 카드회원의 피해가 우려되므로 QA부서에서도 부가상품 TM에 대한 불완전판매 여부를 점검할 필요

② 음성인식 기술(STT-TA) 활용을 통한 모니터링 수준 제고

영업부서별 TM 모니터링 적발률이 음성인식 기술(STT-TA)* 도입 여부에 따라 큰 차이가 나타나고 있으므로** 검사종료일 현재 STT-TA를 도입하지 않은 영업부서(B팀, C팀)는 STT-TA 도입 일정을 구체화하고 추진할 필요

* 음성텍스트변환(Speech To Text), 텍스트분석(Text Analysis)을 하여 스크립트 준수 여부를 쉽게 점검가능
** STT-TA를 도입한 카드론 TM의 모니터링 적발률은 OO%이나, STT-TA를 미도입한 카드신규발급 TM의 경우 적발률이 OO% 수준

③ 표준스크립트 미준수 건에 대한 정기적 분석 및 활용 방안 마련

영업부서가 TM업체의 표준스크립트의 준수 여부를 확인하고 미흡한 사항에 대해 TM업체에 개선을 요구하고 있으나 TM업체의 오류 발생률에는 큰 변동이 없으므로, 정기적으로 표준스크립트 미준수 사례를 분석하고 오류가 빈번한 항목에 대해 테마 점검 또는 교육을 실시하는 방안을 마련할 필요

④ 부가상품 TM업체의 품질 평가업체에 대한 관리 강화

외주업체가 부가상품 TM업체의 표준스크립트 준수 여부를 평가하고 있으나* 해당 외주업체가 충분한 평가 결과를 제공하지 않을 우려가 있어, 해당 외주업체에 대한 평가기준을 마련하고 평가결과에 따라 관련 수수료를 차등 지급할 필요

* 'TM업무'와 'TM업무 평가'를 모두 외주화

(5) IT부문 감사업무 불합리

내규「감사위원회 직무규정」에 IT부문 종합감사를 정기적으로 실시하도록 정하고 있으나 검사대상기간 중 종합감사는 실시하지 않고 특별감사만을 실시*하고

* IT자산관리실태 등 특정 테마를 선정하여 연간 1~2회(회당 10~30영업일) 실시

내부감사는 IT부문(정보보호 포함) 자체감사결과 검토 위주로 업무를 수행함으로써 IT부문 자체감사에 크게 의존하고 있으며

IT부문 연간 자체감사계획은 CIO에게 보고되고 있으나 동 계획의 내용이 매년 거의 동일하고 내용도 개괄적으로 기재하고 있으므로

IT부문 종합감사를 정기적으로 실시하고 일상감사 대상도 확대하는 등 내부감사업무를 강화하고 IT부문 연간 자체감사 계획도 내실 있게 수립하시기 바람

(6) IT·정보보호 부문 자체감사 독립성 확보

IT·정보보호 부문은 자체감사자를 지정*하여 정기·비정기·상시감사를 실시하고 그 결과를 소속 부서장 및 임원(CIO, CISO)에게 보고하고 있으나

* (IT부문) IT경력 O~OO년 이상 직원 O명
(정보보호부문) 정보보안전문가 등 전문자격 보유 IT경력 O~OO년 이상 직원 O명

동 자체감사자는 감사업무 이외에 IT품질, 보안정책 수립·운영 등 타 업무도 담당하고 있으며 소속 부서장 및 임원에게 인사고과*를 받고 있어 소속 부서 및 본인의 소관 업무에 대한 자체감사업무가 독립적·객관적으로 수행되지 않을 우려가 있으므로

* (A) B팀 C소속으로 , 甲, 乙에게 인사고과 받음
(D) E 소속으로 丙, 丁에게 인사고과 받음

IT·정보보호 부문 자체감사자의 독립성 및 객관성을 확보할 수 있도록 조직 개편 및 인력운영 개선 방안을 마련하시기 바람

(7) IT업무 연속성계획 수립·운영 불합리

내규「사업연속성계획(BCP)」에 따라 각 부서는 정기적(연 2회)으로 소관 업무에 대해 핵심업무 선정 여부를 검토하고 BCP위원회는 이를 토대로 사업영향분석 및 부서별 의견청취 등을 통해 핵심업무를 최종 선정하고 있고

검사착수일(2023.5.22) 현재「전자금융감독규정」에 따른 핵심업무는 최우선 핵심업무(OO개), 중요도가 높은 일반업무는 우선 핵심업무(OO개), 그 밖의 업무는 일반업무(OOO개)로 구분하여 선정하였으며

최우선 핵심업무 및 우선 핵심업무는 복구목표시간*을 정하고 이에 맞춰 재해복구센터 등에 관련 시설, 시스템 및 절차를 마련하였으나

* (최우선 핵심업무) 재해선포 후 3시간 이내, (우선 핵심업무) 재해선포 후 24시간 이내

일반업무는 업무별로 복구목표시간을 정하지 않았고 우선 핵심업무는 복구목표시간이 24시간 이내인 일반업무*임에도 핵심업무라는 명칭을 사용함으로써「전자금융감독규정」에 따른 핵심업무와 혼선이 발생할 우려가 있으므로

* ㉮, ㉯ 등 OO개

BCP위원회를 통해 업무는 핵심업무와 일반업무로만 명료하게 구분하고 일반업무에 대해서도 복구목표시간을 정해서「사업연속성계획(BCP)」에 반영하는 등 IT업무연속성 계획을 합리적으로 개선하시기 바람

(8) 오픈소스 프로그램 관리체계 마련

회사는 내규「전산관리규정」 제6조에 따라 유관부서와 협업하여 전산시스템 개발·관리 및 빅데이터 분석 등을 위해 업무용 오픈소스 프로그램*을 다수 도입·운영하고 있으나

* ㉮ 등 OO개 오픈소스 소프트웨어를 시스템 개발·운영환경에 활용

오픈소스 프로그램 사용에 관한 관리주체, 활용 절차 등의 관리체계가 마련되어 있지 않고 오픈소스 사용현황도 수기로 관리하고 있으며

형상관리시스템을 통한 프로그램 배포시 오픈소스 취약점 점검 기능을 적용하고 있지 않고 라이선스 정책 준수 여부 등에 대해서도 정기적으로 점검하지 않는 등 통제 절차도 미비하여 오픈소스 프로그램 관련 운영리스크*가 발생할 우려가 있으므로

* (보안 리스크) 공개된 소스코드로 인한 중요 취약점 노출, 패치 무결성 훼손 등
(법적 리스크) 오픈소스 라이선스 사용 저작물의 상업적 이용 등

오픈소스 프로그램에 관한 도입·활용·유지보수 등 생명주기 전반에 걸친 관리체계를 내규로 마련하고 오픈소스 프로그램별 라이선스 정책 준수여부 등을 정기적으로 점검하며 오픈소스 코드에 대한 취약점 점검을 수행하는 등 오픈소스 프로그램 관리·통제 절차를 강화하시기 바람

(9) 프로그램 관리통제 불합리

내규「어플리케이션변경관리 가이드」 제18조에 따라 프로그램을 운영시스템으로 이관하는 경우 승인자와 합의자가 자동으로 설정되도록 형상관리시스템을 운영하고 있으나

일부 솔루션 프로그램*은 운영시스템으로 이관 시 합의자가 자동으로 설정되지 않아 합의절차가 생략**되는 등 운영시스템 적용에 관한 적정성 검토가 다소 미흡할 우려가 있으므로

* 자체 형상관리시스템(㉮)을 통하지 않고 운영시스템으로 이관되는 프로그램 등
** 합의자 누락 66건 존재

솔루션 프로그램을 운영시스템으로 이관하는 경우에도 합의자 검토가 누락되지 않도록 프로그램 변경통제 관리자를 별도로 지정하는 등 프로그램 관리통제 절차를 강화하고 관련 시스템을 재정비하시기 바람

(10) 정보처리시스템 모니터링 불합리

① 안정적인 IT서비스 운영을 위하여 담당자(오퍼레이터 등)는 서버, 네트워크 등 시스템별 관리 도구*를 통해 영역별 모니터링을 수행하고 시스템 임계치 초과 등 이벤트 발생 시 비즈니스 및 인프라 관제 시스템(㉮)을 통해 담당자(오퍼레이터 등)에게 자동으로 알림메세지를 발송하고 있으나

* ㉯,㉰ 등 개별 관제 솔루션

담당자가 각자 맡은 시스템 영역에 대해서만 개별 모니터링하고 있어 이벤트나 이상징후 발생 시 종합적인 상황판단이 어렵고 담당자 부재 시 일부 영역의 모니터링이 미흡해질 우려가 있으므로

정보처리시스템의 성능·사용량 및 추이를 종합적으로 모니터링하기 위한 IT 통합 모니터링 시스템을 구축하는 등 시스템 성능 관리체계를 개선하시기 바람

② 주전산센터 내 서버용 CCTV(O층 OO대, O층 OO대)를 설치·운용하고 있으나 종합상황실 등에서 CCTV 정상작동 여부에 대해 모니터링하고 있지 않아 CCTV 고장 발견 지연으로 사고 발생 시 영상녹화가 제대로 이루어지지 않을 위험이 있으므로

종합상황실에 CCTV 통합관제 시스템을 설치·운영하여 서버실 관제를 강화하시기 바람

(11) 개인정보 표준화 관리 불합리

내규「데이터 표준 및 모델관리 가이드」 제3장에 따라, 데이터 속성(Attribute), 유형(Type), 표준용어 등을 관리하는 메타데이터 관리시스템을 통해 전사 데이터베이스의 구조를 관리하고 데이터 표준화를 수행하고 있으나

메타데이터 관리시스템에서 데이터베이스에 개인정보가 포함되었는지를 상세하게* 식별·관리하고 있지 않아 암호화 및 마스킹 대상에 대한 일관성 있는 관리·통제가 어려우므로

* 주민등록번호, 계좌번호 등이 포함된 컬럼(Column)을 기준으로 암호화·마스킹 대상을 분류·관리하지 않고 항목명 및 도메인명으로 관리

메타데이터 관리시스템에서 주민등록번호, 계좌번호 등이 포함된 컬럼(Column)을 중요 데이터 항목으로 관리하고 정보처리시스템 개발 시 메타데이터 관리시스템을 기준으로 암호화·마스킹 처리하도록 업무절차를 보완하고 시스템을 개선하시기 바람

(12) 모바일 서비스 보안관리 불합리

내규「개발보안 가이드」C.4 등에 따라, 모바일 전자금융서비스 설계·구현 시 소스코드 난독화, 앱 위·변조 방지 등 모바일 보안시스템을 적용하고 있으나

㉮는 악성앱 탐지시스템이 누락되어 있어 피싱앱·스파이앱(전화·문자 가로채기 등) 탐지가 미흡할 우려가 있고, ㉯와 ㉰는 앱백신과 원격제어툴 탐지시스템이 적용되어 있지 않아 악성코드 감염, 원격제어 등의 보안 위협에 노출될 위험이 있으며

㉱, ㉲는 웹페이지 위·변조 방지시스템을 적용하지 않아 스크립트 위변조 공격 등에 취약할 우려가 있고, ㉳ 등 일부 웹사이트는 단말기 정보수집을 통한 부정접속 여부를 검증하지 않는 등 보안로그 탐지체계가 다소 미흡하므로

대고객 서비스를 중심으로 악성앱 탐지시스템 및 앱백신, 웹페이지 위·변조 방지시스템 등 모바일 보안시스템을 확대 적용하고, 보안로그 탐지체계를 강화하는 등 모바일 서비스에 대한 보안관리 체계를 마련하고 관련 시스템을 개선하시기 바람

(13) 전산자료 보호대책 불합리

① 내규「정보보호지침」B.5.3 등에 따라, 중요 전산자료 보호·정보유출 방지를 위해 매체제어시스템을 구축하여 저장매체를 통제하고 네트워크 폴더를 통한 전산자료 공유를 차단하고 있으나

일부 사용자들이 업무자료 공유 목적으로 네트워크를 통해 파일·폴더를 공유*하고 있어 공유폴더를 통한 악성코드 전파 등의 침해 위협이 발생할 수 있고 전산자료 공유에 관한 사용자 권한관리 및 사용이력 기록이 다소 미흡하므로

* 검사착수일 현재, OO개 단말기가 소속 부서장 승인 및 IT보안팀 합의를 받아 공유폴더 이용 중

임직원 간 업무자료를 공유할 경우에는 공유폴더 사용을 제한하고 사용자 권한관리 및 사용이력 기록이 가능한 웹디스크 시스템 등을 활용하는 등 전산자료 공유에 관한 통제를 강화하시기 바람

② 업무망 단말기에서 인터넷망 단말기로 전산자료를 전송하는 경우 망간

자료전송시스템을 통해 개인정보·악성코드 포함 여부 등을 자동으로 검출하고 책임자(부서장)의 승인도 받고 있으나

비밀번호가 설정된 파일에 대해서는 개인정보·악성코드 검출 기능이 동작하지 않고 있고 전산시스템 개발·운영 업무를 수행하는 계열사(A)의 경우에는 담당자가 인터넷망 단말기로 자료전송을 신청하고 현장대리인이 승인하는 등 망간 자료전송에 관한 통제 절차가 다소 미흡하므로

비밀번호가 설정된 파일도 개인정보 및 악성코드 검출 기능이 동작하도록 관련 시스템을 개선하고 망간 자료전송에 관한 승인은 내부 책임자가 담당하도록 업무절차를 보완하시기 바람

(14) 침해사고 대응훈련 불합리

내규「정보보호지침」B.6.3조 등에 따라, 서버 해킹, 분산서비스거부(DDoS : Distributed Denial of Service) 공격 등에 대한 대응능력 확보를 위하여 침해사고 대응훈련을 연 1회 실시하고 있으나

매년 하나의 전자금융업무에 대해서만 침해사고 대응훈련을 실시*하여 ㉮, ㉯ 등 일부 전자금융업무는 검사대상기간 중 훈련을 실시한 이력이 없어 서버 해킹, 분산서비스거부(DDoS) 공격 등에 취약할 우려가 있고

* 2019년 ㉰ 검증계, 2020년 ㉱ 검증계, 2021년 ㉰ 검증계, 2022년 ㉲ 개발계

침해사고 시나리오를 매우 낮은 수준의 공격 트래픽(50Mbps)이 재해복구센터 개발·검증 시스템으로 유입되는 것으로 정하고 있어 모의훈련의 효과성을 보장하기 어려우므로*

* 실제 분산서비스거부(DDos) 공격은 주전산센터 운영시스템을 대상으로 10Gbps 수준의 대량 트래픽이 유입되어 전산시스템을 마비

침해사고 대응훈련을 모든 전자금융업무를 대상으로 확대하고, 주전산센터의 운영시스템을 대상으로 상향된 공격 트래픽을 사용하는 등 훈련 시나리오를 보완하여 침해사고 대응훈련의 실효성을 제고하시기 바람