경영유의사항 등 공시

1. 금융회사명 : 한국스탠다드차타드은행

2. 제재조치일 : 2018. 8. 23.

3. 조치내용

제재대상	제재내용
기 관	경영유의 8건, 개선 23건
직 원	-

4. 제재대상사실

가. 경영유의사항

(1) 집행임원리스크위원회와 여신위원회 간 이해상충 방지 강화 등

○ 여신위원회가 집행임원리스크위원회의 하부위원회로 운영되어, 집행임원리스크위원회가 여신신청 및 승인 규정을 포함한 여신위원회 규정을 결의하고 여신위원회의 부의안건을 보고받고 있으므로

앞으로 여신위원회를 집행임원리스크위원회의 수준으로 운영하는 등 집행임원리스크위원회와 여신위원회 간 이해상충 방지를 강화할 필요가 있음

○ 또한 특수여신의 편입 및 해제를 결정하는 특수여신 관련 여신위원회의 구성원이 리스크관리본부 소속 인원으로만 구성되어 있어 여신심사본부의 전문적인 의견이 반영되기 곤란하고, 동 위원회의 위원장이 위원보다 하위직급으로 임명되는 등 그 구성에서 비합리적으로 운영되는 측면이 있으므로

앞으로 특수여신 관련 여신위원회의 전문성 강화를 위해 리스크관리본부 이외의 여신심사본부 등 관련부서 인원을 위원으로 참여시키는 등 동 위원회를 합리적으로 운영하여 책임성·효율성을 강화할 필요가 있음

(2) 주택담보대출 취급시 통제절차 강화

○ 대출승인 전결권자 등에 따라 심사역 전결 대출 및 선임심사역 이상의 전결 대출로 구분되는데 심사역 전결 대출의 경우 전결권자의 주관적 판단으로 운영될 소지가 있는 등 심사역 전결대출의 통제절차가 선임심사역 이상의 전결 대출에 비해 미흡한 점이 있으므로

주택담보대출에 대한 리스크 관리 강화를 위하여 심사역 전결 대출의 경우에도 선임심사역 이상의 전결대출과 동등한 내부통제를 반영하는 등 합리적인 통제 절차를 마련할 필요

(3) 연체 가산금리 산정절차 강화

○ 연체 가산금리의 산정·운용 절차 및 내부통제와 관련된 내부기준이 미흡하여 명확한 비용 분석이 없이 연체 가산금리가 산정되고 있으므로

앞으로 관련 내규에 연체 가산금리 산정기준에 관한 사항 등을 명시하고 연체 가산금리를 심사하는 내부 심사위원회를 설치·운영하는 등 연체 가산금리의 산정 절차를 강화할 필요가 있음

(4) 카드론 자산에 대한 감독목적상 충당금 적립 사후검증 절차 강화

○ 카드론 자산에 대한 「은행업감독규정」 개정사항을 지연 반영하여 감독목적상 대손충당금 및 대손준비금이 과소 적립*된 사실이 있으므로

* 회계처리기준 중요성 관점에서는 미미한 수준으로 BIS비율 영향은 없음

앞으로 이러한 사례가 재발하지 않도록 관련 규정의 개정사항 반영여부 확인 등 감독목적상 충당금 및 대손준비금 산출 시 사후검증 절차를 강화할 필요가 있음

(5) 은행 익스포져에 대한 신용위험가중자산 산출 사후검증절차 강화

○ 은행 익스포져에 대한 신용위험가중자산 산출시 OECD 국가신용도등급이 수시로 변경·공시되고 있음에도 위험가중치 적용시 변경된 내용을 제대로 반영하지 않아 은행 익스포져에 대한 위험가중자산 산출 오류 발생사실*이 있으므로

* 금액이 미미하여 BIS비율에 영향은 없음

오류사항을 수정하여 신용위험가중자산 및 BIS비율을 재산출하고, BIS비율 산출의 정확성 확보를 위해 사후검증 절차를 강화할 필요가 있음

(6) 집행임원리스크위원회 독립성 강화

○ 은행장이 집행임원리스크위원회 위원으로서 리스크관리 정책수립 과정에 참여하고 있어 영업활동에 대한 집행임원리스크위원회의 견제 기능이 약화될 우려가 있으며, 집행임원리스크위원회의 하부위원회인 신용이슈위원회에도 은행장이 위원으로 참여하고 있으나 회의 참석률이 낮아 실효성이 저하되고 있으므로

앞으로 집행임원리스크위원회 및 관련 하부위원회의 구성을 합리적으로 개선하여 리스크관리 협의체 운영의 독립성을 강화할 필요가 있음

(7) 금리리스크(규제목적)에 대한 관리 강화

○ 표준방법(규제목적)으로 산정한 금리 VaR, 금리 EaR를 분기별로 금융감독원장에게 제출하고 관리현황을 위험관리위원회에 보고하고 있으나 위험관리위원회에 제출된 금리리스크 보고서의 금액 및 분석 내용에 오류가 발견되었으므로

금리리스크 산출의 정확성을 제고하기 위한 프로세스를 마련하고 향후 위험관리위원회 보고내용도 충실히 하도록 하는 등 실효성 있는 금리리스크 관리방안을 마련할 필요

(8) IT부문 인프라 투자 및 시스템 성능 강화 필요

○ IT부문 인프라 개선 등이 포함된 중장기 로드맵을 마련하고 정기적으로 주전산기 메인프레임 및 서버 등에 대한 성능 모니터링을 실시하고 있으나 시스템 노후화 및 IT인프라 성능 부족에 따른 CPU 최고치 사용률 증가 등으로 시스템 장애가 발생할 우려가 있음에도 IT인프라에 대한 투자 실적이 없으므로

조속히 장애가 발생한 메인프레임 및 서버에 대한 교체 또는 성능확충 계획을 마련하고, 신기술 도입 관련 인프라 구축 및 IT인프라 성능 강화를 위한 중장기 IT인프라 투자 계획을 수립·시행할 필요가 있음

나. 개선사항

(1) 기업 신용평가 기준 불합리

○ 신용평가모형에 의해 차주의 신용등급이 결정되고 예외적인 경우에 한하여 승인권자의 승인을 받아 신용등급 조정을 허용하고 있으나, 이러한 신용등급의 조정 사유가 구체적으로 내규에 명시되어 있지 않아 평가자의 주관적 판단에 따라 신용등급 조정이 이루어질 수 있으므로

관련 내규에 과거 사례분석 수행 결과를 반영하는 등 신용등급 조정사유를 구체적으로 명시하도록 개선하시기 바람

○ 부실 등 일정 징후를 보이는 문제여신에 대해서는 일정등급 이하를 부여하여야 하나, 문제여신 여부를 판단하는 기준이 명확하지 않아 평가자의 주관적 판단에 따라 운영될 소지가 있으므로

관련 내규에 정상여신이 문제여신으로 분류되거나 문제여신이 정상여신으로 재분류되는 사유를 구체적으로 명시하도록 개선하시기 바람

(2) 보증서담보대출 담보해지 처리절차 미흡

○ 보증서담보대출을 취급한 이후 보증사고 발생하는 경우 대위변제가 완료된 시점에 담보를 해지토록 하고 있으나 담보 해지를 수기로 전산등록하고 해지누락 건에 대해서는 사후에 확인함에 따라 담보 해지가 지연되는 사례가 발생하고 있으므로

대위변제가 완료되는 시점에 보증서 담보가 전산에서 자동 해지될 수 있도록 시스템을 개선하고 동 시스템 개선 전까지 해지누락이 발생되지 않도록 통제절차를 마련하시기 바람

(3) 무역금융 거래 관련 내부통제 미흡

○ 하자가 없이 매입하였다고 내부 처리한 수출환어음 중 사후관리가 미흡한 사례 및 상대방 은행의 하자통보 건이 발생하였던 점 등을 감안하여

수출입어음 매입시 기본적인 서류 점검 관리, 특이한 신용장 조건 모니터링, 사후 하자 사유 및 지연 입금에 대한 지속적인 모니터링, 상대방 수입업체에 대한 조사

등 수출환어음 매입 업무를 보다 신중하게 관리할 수 있도록 관련 내부절차를 개선하시기 바람

(4) 경영자문료 지급 관련 업무처리 절차 불합리

○ 이사회는 SCB 본사에 지급하는 경영자문료 지급과 관련하여 은행장에 포괄적 권한 위임을 하였고 은행은 이에 따라 매년 SCB 본사에 경영자문료를 지급하고 있으나

동 경영자문료의 지급 필요성, 항목별 상세내역의 관리 및 금액산정의 적정성 등을 사전검토하는 내부절차가 미흡하고 매년말 결산 보고 시 해당연도에 반영된 경영자문료의 주요내용 및 지급금액 등을 이사회에 별도 보고하지 않고 있으므로

앞으로 경영자문료 지급에 대한 사전검토를 실시하고 내부 보고절차를 적정하게 운영하는 등 경영자문료 관련 관리체계를 합리적으로 개선하시기 바람

(5) 영업점 성과평가지표(KPI) 불합리

○ 영업점 직원 중 「성과급제 모기지대출 전문 판매직군」은 실적을 높이기 위한 불건전영업 행위가 발생할 소지가 있음에도 성과평가지표(KPI)에서 내부통제 관련 항목 배점 비중이 가장 낮게 설정되어 있으며

「영업점 내부통제 전담 직군」은 성과평가지표(KPI)에 영업점 전체의 신규판매 실적이 영업점장 보다 높게 반영되어 있어 이로 인해 영업점의 내부통제가 약화될 소지가 있는 등 영업점 성과평가지표의 설계가 불합리한 측면이 있으므로

앞으로 영업점의 내부통제 및 리스크 관리가 강화될 수 있도록 관련 성과평가지표(KPI)를 합리적으로 개선하시기 바람

(6) 모바일 플랫폼 관련 업무처리 절차 미흡

○ 은행은 태블릿 PC(모바일 플랫폼)를 이용한 보험모집시 점외 모집을 방지하기 위하여 고객으로부터 영업점 내에서 업무처리가 진행된 사실을 서명받는 등 고객 확인절차를 마련하고는 있으나

영업점 내부통제 관리자가 태블릿 PC를 이용한 점외 모집을 물리적으로 통제할 수 있는 방안 및 실제 점외 모집 여부를 확인하는 절차가 마련되어 있지 않으므로

앞으로 태블릿 PC를 이용한 점외 모집을 예방할 수 있도록 전산적인 통제 장치를 마련하고 영업점 내부통제 담당자가 업무처리의 적정성을 점검·승인하는 등 관련 업무처리 절차를 개선하시기 바람

(7) 방카슈랑스 불완전판매 방지 절차 미흡

○ 고객이 영업점에서 보험계약을 청약하면 전산을 통해 6개월 이내 보장내용 등이 비슷한 보험계약을 중도해지한 사실이 있는지 여부(승환계약 여부)를 확인하고 이러한 사실이 있을 경우에는 보험계약사항 비교확인서를 징구하여 계약의 중요 사항을 비교하여 알리고 본인 의사를 확인하는 절차를 운영하고 있으나,

고객이 은행(영업점)이 아닌 제휴 보험사를 통해 기존 보험계약을 해지한 경우에는 전산을 통해 승환계약 여부를 확인할 수 있는 시스템이 갖춰져 있지 않으므로

앞으로 고객이 제휴 보험사를 통해 기존 보험계약을 해지한 경우에도 전산을 통해 승환여부를 확인할 수 있도록 관련 시스템을 개선하고 이에 대한 점검절차 마련 및 관련 직원에 대한 교육을 실시하는 등 내부통제 체계를 강화하시기 바람

○ 고객이 영업점에서 보험계약을 청약하면 전산을 통해 구속성 대상 여부를 확인하고 이러한 사실이 있을 경우에는 구속성 계약에 해당되는지 여부를 별도로 점검하는 절차를 운영하고 있으나,

차주 또는 차주의 관계인 이외의 명의로 보험계약을 체결하고 이후 계약자 명의를 차주 또는 차주의 관계인 명의로 변경하는 경우에는 전산에서 구속성 대상 여부를 확인할 수 있는 시스템이 갖춰져 있지 않으므로

앞으로 보험계약자를 변경하는 경우에도 전산을 통해 구속성 대상 여부를 확인할 수 있도록 관련 시스템을 개선하고 이에 대한 점검절차 마련 및 관련 직원에 대한 교육을 실시하는 등 내부통제 체계를 강화하시기 바람

(8) 금융거래정보 제공 사실 통지업무 절차 미흡

○ 금융회사 등이 금융거래정보 등을 제공한 경우에는 정보 등을 제공한 날로부터 10일 이내에 해당 사실을 명의인에게 통보하는 절차를 마련하고 있으나

수사기관 등이 영업점에 직접 금융거래정보 제공을 요청할 경우에는 영업점에서 이를 수기로 관리하고 있어 명의인에 대한 통보 지연 및 누락 사례가 발생할 소지가 있으므로

금융거래정보 제공사실이 기한내에 통지될 수 있도록 영업점의 관련 전산시스템을 구축하고 점검절차를 마련하는 등 내부통제 체계를 개선하시기 바람

(9) 약관 제·개정 관리절차 미흡

○ 일반 약관 및 약정서를 제·개정하면서 시행일 이후 약관을 공시하거나 전결권자의 결재를 득하지 않고 시행하는 등 관련 업무취급 절차상 일부 미흡한 점이 있었고 약관 사전심사를 담당하는 부서가 다수임에도 관련 업무를 수기 등으로 관리하고 있어 절차상 누락이 우려되므로

약관 제정·변경 절차 관련 유의사항을 명확히 고지하는 등 준법감시부서의 역할을 강화하고, 타 부서 사전심의여부 및 기한 준수 여부 등을 확인할 수 있는 전산시스템을 구축하는 등 관련 절차를 개선하시기 바람

(10) 영업점 자체점검 관련 내부통제절차 불합리

○ 은행은 영업점 자체점검을 위한 내부통제기준 등을 감사부 등 관련 부서의 사고예방대책 매뉴얼에 일부 반영하여 운영하고 있고, 영업점 자체점검 실시 결과에 대한 준법감시인의 보고의무 및 절차를 정하고 있지 않으므로

앞으로 영업점 자체점검에 대한 사항을 내규로 구체화하고 그 결과를 준법감시인에게 정기적으로 보고하는 절차를 마련하는 등 영업점 자체점검 관련 내부통제절차를 합리적으로 개선하시기 바람

(11) 유동성 위기 대비 비상조달계획 미흡

○ 유동성 위기 발생시 대응방법 및 자금조달 가능 규모 등을 이사회내 위험관리위원회에 제출하여 매년 승인을 받고 있으나,

유동성 위기 발생시 자금조달 가능 규모는 반영되지 않아 유동성 위기에 대응한 은행의 비상조달계획이 미흡하게 수립될 우려가 있으므로 앞으로 이를 반영하시기 바람

(12) 유동성커버리지비율(LCR) 산출 업무 미흡

○ 유동성커버리지비율(이하 'LCR')의 순현금유출액 산정시 향후 30일 이내 지급이 예상되는 배당금을 기타 계약상 현금유출에 반영토록 하고 있고 주주총회 결의 시점을 배당금 지급이 예상되는 시점으로 보고 LCR를 산정하고 있으나,

주주총회 당일 또는 이와 가까운 날에 지급하는 경우에도 주주총회 결의 시점을 배당금 지급이 예상되는 시점으로 판단하는 것은 유동성 리스크 관리 측면에서 불합리하므로

앞으로 안정적인 유동성 리스크 관리를 위하여 이사회 결의 등 배당금 지급이 합리적으로 예상되는 시점부터 배당금 지급에 따른 현금유출금액을 반영하여 일별 LCR를 산출토록 개선하시 바람

○ 또한 배당계획 검토 시 은행의 자본적정성, 수익성에 미치는 영향을 분석하고 있으나 현금배당이 LCR에 미치는 영향에 대한 분석이 이루어지고 있지 않으므로

효율적인 유동성 리스크 관리를 위하여 현금배당으로 인한 현금유출로 인해 LCR에 미치는 효과 분석도 함께 실시하는 것으로 개선하시기 바람

(13) 전자금융기반시설의 취약점 분석·평가 불합리

○ 전자금융기반시설의 취약점 분석·평가를 실시하고 있으나 전체 메인프레임 및 서버 중 채널계 서버에 대해서만 제한적으로 취약점 분석·평가를 실시하였으며, 취약점 분석·평가에서 발견된 취약점이 다시 발견되는 등 사후관리도 미흡한 수준으로

전자금융기반시설의 취약점 분석·평가 대상을 확대하고, 위험도가 높은 취약점을 중점으로 취약점 보완 결과에 대한 자체 점검, 발견된 취약점과 관련된 업무담당자 교육 실시 등 사후관리 체계를 개선하시기 바람

(14) IT부문 감사체계 불합리

○ IT감사 인력이 IT부문 이외에 타부문 감사업무도 수행하고 있어 IT부문에 대한 감사가 원활히 이루어지지 못할 우려가 있으므로 업무분장 재조정, IT전담 감사 인력을 확충 등을 통해 IT부문 내부통제를 강화하고, 위규사항 및 해킹 등 침해사고 발생 시 소관 부서 리스크 평가에 반영하여 감사를 실시하고

IT부문 자체감사 관련 리스크 평가지표 작성 및 평가를 모두 해당 IT부서에서 자체적으로 수행하고 있어 객관성이 결여될 우려가 있으며, 테스트 시 이용자 정보를 변환하지 않는 사례가 적발되었음에도 이후 유사사례 존재 여부에 대해 자체감사를 실시하지 않는 등 자체감사가 다소 미흡하게 운영된 측면이 있으므로

IT부서에서 작성한 리스크 평가지표 및 평가결과의 적정성을 정기적으로 점검하고 내규에서 정한 일상감사 대상 업무에 대한 감사를 빠짐없이 수행하는 한편 주요 장애 및 오류 발생 시 자체감사 수행 후 재발방지대책을 마련하여 감사부에 보고하는 체계를 마련하시기 바람

(15) 기술지원 종료 운영체제 및 장비 사용에 따른 보안통제 미흡

○ 정보처리시스템 일부 서버에 기술지원이 종료된 운영체제가 탑재되어 있으며 일부 네트워크 장비 기술 지원도 종료되어 해킹 및 악성코드 등에 의한 침해 우려가 있으므로

기술지원이 종료된 운영체제 및 네트워크 장비의 구체적인 전환계획을 수립하고 전환이 이루어지기 전까지 강화된 보안대책을 마련하시기 바람

(16) SWIFT 시스템 보안대책 미흡

○ 계정관리시스템을 통해 사용자의 SWIFT 서버 접속을 통제하고 접근이력을 관리하고 있으나 일부 보안대책이 미흡하므로

SWIFT 시스템 접속을 SWIFT 시스템 접속용 단말기를 통해서만 접속이 가능하도록 운영하고, 계정관리시스템 우회 접속을 차단하고 부정 접속 모니터링을 강화하는 등 SWIFT 시스템 보안체계를 개선할 필요가 있으며

SWIFT 전문 생성이 가능한 계정보유자에 대해서는 동 시스템 전용 단말기를 지급하고, SWIFT 전문 조회가 가능한 계정보유자에 대해서는 동 시스템 접속 단말기를 외부 인터넷과 물리적으로 분리하는 등 강화된 단말기 보안대책을 마련하시기 바람

(17) 개발자 단말기 프로그램 통제 소홀

○ 개발용 단말기 악성코드 감염을 방지하기 위한 대책을 마련하고 있으며, 개발자는

프로그램 설치가능 권한(관리자 권한)을 부여받은 경우에 한하여 단말기(업무용, 개발용)에 프로그램 설치가 가능하도록 운영하고 있으나

프로그램 설치권한만을 부여하고 동 프로그램의 설치 필요성 및 사후 점검 등을 실시하지 않아 프로그램 설치과정에서 악성코드가 유입되는 등 전자적 침해사고가 발생할 우려가 있으므로

개발자에게 프로그램 설치가능 권한을 부여하는 대신 개발자 단말기 표준 환경을 마련한 후 개발자(은행 및 외주업체) 단말기를 동 표준 환경으로 일제히 정비하는 한편, 향후 신규 개발자 투입 시에는 동 표준 환경에 따른 프로그램을 설치하는 등 개발자 단말기 프로그램 통제를 강화하시기 바람

(18) 파일 등 전산자료 보호대책 소홀

○ 업무용 단말기에 매체통제 솔루션, 개인정보 탐지 솔루션을 설치하고, 네트워크에 이메일을 통한 자료 유출을 차단하기 위한 솔루션을 설치하는 등 전산자료 보호 체계를 갖추고 있으나

문서 암호화 솔루션(DRM)이 자동으로 업무용 단말기내 모든 문서 파일에 적용되지 않고 사용자가 개별적으로 적용하거나 개인정보 탐지 솔루션으로 고객정보가 탐지되는 경우에만 강제 암호화하도록 설정하고 있어

작성자가 DRM 적용을 고의 또는 과실로 누락하는 경우에는 주요 문서가 외부에 노출되거나 유출될 우려가 있고 외주직원이 단말기 간에 파일을 이동하는 경우, 망간 파일전송 시스템을 통해 직상위자, 현장 대리인 또는 은행직원의 승인을 받도록 통제 절차를 마련하고 있으나

정해진 통제절차를 준수하고 있지 않은 사례가 발견되어 주요 자료의 외부 유출, 개발 서버 등에 허가받지 않은 자료 적재, 개발용 단말기에 악성코드 유입 등의 사고 발생 가능성이 있으므로

단말기에서 문서 파일을 생성·저장하는 즉시 암호화하는 방안을 마련하고, 외주인력이 망간 파일전송 시스템을 통해 단말기 간에 파일을 전송하는 경우에는 반드시 현장 대리인 또는 은행직원의 승인을 받도록 통제 절차를 강화하는 한편

정상적인 승인 절차를 거치지 않은 파일이나 허가받지 않은 파일이 이동되지

않도록 외주관리 책임자가 정기적으로 외주직원의 파일전송 내역을 사후점검하는 절차(내규)를 마련하는 등 강화된 통제절차를 마련하시기 바람

(19) IT부문 비상대책 수립·운용 절차 불합리

○ 재무적 리스크, 평판 리스크 등을 감안한 업무영향 분석을 통해 각 업무중요도에 따라 핵심업무와 일반업무로 구분하여 재해복구시스템을 구축하고 있으나

여신, ATM, 모바일뱅킹 업무는 일반업무로 분류됨으로써 향후 IT인프라 변경 시 동 업무의 재해복구시스템 구축이 누락될 우려가 있으므로

향후 IT인프라 변경 시에도 은행의 주요 업무가 핵심업무 선정에서 누락되지 않도록 업무중요도 및 핵심업무 설정을 일제히 정비하고, IT부문 비상대책 수립·운용 절차를 개선하시기 바람

(20) 테스트 목적의 이용자 정보 변환 사용 통제절차 불합리

○ 프로그램을 테스트하기 위해 운영계의 실제 데이터 사용이 필요한 경우 주요 이용자 정보를 변환하여 사용하고 테스트 종료 후 삭제하도록 정하고 있고,

이를 위해 주요 이용자 정보를 자동 변환하여 테스트 시스템에 적재하는 솔루션을 도입하였으나 사용실적이 전무하고, 도입 이전과 동일하게 개발자가 배치 프로그램을 통해 수동으로 변환한 후 사용하여 개발자의 과실 등에 의해 이용자 정보가 변환되지 않은 상태로 테스트 데이터로 사용될 우려가 있으며

테스트 승인 요청서, 테스트 데이터 변환작업 결과서 등 관련 문서 양식이 솔루션 도입 이후에도 변경되지 않아 변환작업에 대한 적정성 검토 등이 미흡할 우려가 있으므로

앞으로는 기도입한 이용자 정보 자동 변환 솔루션을 통한 테스트 데이터 변환만 허용하는 한편 테스트 관련 양식을 개정하고 동 솔루션에 등록·관리하는 고객정보 보유 테이블 목록의 적정성을 정기적으로 점검하는 절차를 마련하는 등 통제절차를 강화하시기 바람

(21) 정보처리시스템 사용자 계정관리 미흡

○ 계정관리시스템을 통해 사용자별 보유 계정 목록을 관리하고 있으며, 사용자의 계정 및 접근권한 정당성을 사후 점검하고 있으나

사용자가 퇴사 또는 부서이동 시, 본인이 직접 계정 삭제를 신청하여야 하고, 정보보안부에서 미삭제 계정을 정기적으로 관리하지 않는 등 계정 삭제 및 접근권한 관리가 미흡하므로

사용자가 퇴사 또는 부서이동을 한 경우, 운영체제, 데이터베이스 계정이 즉시 삭제 또는 이용 제한될 수 있도록 시스템을 개선하고 각 부서에서 수행하는 관리자접근검토 이외에 정보보안부에서 계정발급 및 권한부여 현황을 주기적으로 사후 점검하는 절차(내규)를 마련하시기 바람

(22) 데이터베이스 운영·통제 미흡

○ 데이터베이스(DB) 접근통제 솔루션을 운영하고 있으며, 접근권한은 승인권자 승인하고 이후 데이터베이스관리자가 각 계정을 그룹으로 세분화하여 부여하고 있으나

일부 그룹의 경우 데이터 조회만 가능하도록 명령어 권한을 부여하여야 함에도 데이터 입력・수정・삭제 권한을 잘못 부여한 사례가 발견되었고,

개발담당 외주직원 일부가 운영시스템 데이터베이스 조회권한을 보유하고 있으며, 데이터 조회 시 일부 테이블에 한정하여 고유식별정보를 마스킹 처리하고 있어 개인신용정보가 노출될 위험이 있으므로

계정그룹별 명령어 권한의 적정성, IT직원 직무별 권한의 적정성을 일제히 점검하여 정비하고, 고유식별정보가 포함된 모든 테이블에 대해 마스킹 처리를 적용하는 등 데이터베이스 운영·통제 체계를 개선하시기 바람

(23) 서버 명령어 통제 미흡

○ 서버 접근 통제를 위해 이중인증 솔루션을 도입하여 비인가자의 접근을 차단하고 있으나 서버 접속 후 명령어를 이용하여 관리자 권한 획득 및 서버간 원격접속 등이 가능하여 권한 없는 자에 의해 서버 내 정보가 유출될 우려가 있으므로

서버 명령어에 대한 통제 방안을 마련하여 부정한 관리자 권한 획득 및 서버간 원격접속 등을 차단할 수 있도록 개선하시기 바람