경영유의사항 등 공개안

1. 금융기관명 : 롯데카드㈜

2. 조치일 : 2024. 8. 2.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 2건, 개선사항 11건

4. 제재대상사실

가. 경영유의사항

(1) IT아웃소싱 운영 관리 강화

2003년 이후 A사와 IT아웃소싱 계약을 체결하여 정보처리시스템의 운영과 유지관리 업무를 위탁하고 있으나,

2017년 변경계약 체결 및 이후 갱신 시 과업의 목적 및 범위, 과업의 내용 등 과업을 원활히 수행하기 위하여 필요한 사항을 규정하는 과업지시서 작성 없이 계약서 제3조(용역의 범위)에 포괄적인 서비스 범위만을 규정함으로써 회사가 IT아웃소싱 업무를 체계적으로 관리하지 못할 우려가 있으며

계약서 제4조에 따라 검사대상기간 중 매년 IT아웃소싱 계약을 자동 연장하고 있으나, 계약종료 예정 시점에 A사로부터 정보처리시스템의 운영 및 유지관리 전반에 대한 결과보고서 등을 제출받아 계약내용에 따른 용역수행의 적정성 등을 평가하고 계약연장 여부를 결정하는 절차가 없어 IT아웃소싱 서비스의 품질수준 저하 등 IT아웃소싱 업무가 부실하게 관리될 우려가 있으므로

계약 연장시 용역수행의 적정성을 평가하는 등 IT아웃소싱 운영 관리를 강화하시기 바람

⑵ IT계약 체결 업무 강화

① 내규 「B규정」에 따라 의사결정권자가 최종 결재하기 전에 프로젝트를 이미 착수한 사례가 총 ○○건(56.5%)이며, 이는 소급계약 형태로 계약체결이 불확실한 상태에서 구축사에게 인력 및 장비 우선 투입의 위험부담을 가중시킬 우려가 있음

② 내규 「C지침」에 따라 IT 운영 품질 유지를 위해 '경쟁입찰'이 원칙이고 필요시 '수의계약' 체결이 가능하도록 운영하고 있긴 하나, 수의계약 체결의 필요성 검토 내역 없이 총 ○○건(86.3%)의 계약을 체결하였음

③ 내규 「C지침」에 예정가격의 작성방법, 결정방법 및 결정기준 등을 구체적으로 마련하지 않은 채 연초에 수립한 IT예산을 예정가격으로 사용하고 있어, 경쟁입찰시 IT예산이 특정 입찰자에게 유출될 경우 공정한 경쟁입찰이 저해될 소지가 있음

④ 또한, 내규 「C지침」에는 입찰보증금, 계약보증금, 하자보수보증금, 지체상금 관련 내용이 마련되어 있지 않으며, 이 중 입찰보증금은 실제 IT계약 업무에 적용* 하지 않고 있어, 낙찰자가 계약 체결을 거절할 경우 입찰보증금을 회수하는 등의 대안이 없으므로 회사가 피해를 볼 우려가 있음

* 계약보증금, 하자보수보증금, 지체상금은 실제 IT계약 업무에 적용

앞으로 소급계약 및 수의계약은 최소화하고, 예정가격 및 입찰보증금·계약보증금·하자보수보증금·지체상금 운영 관련 사항을 내규에 반영하고 이를 준수하는 등 IT계약 체결 업무를 강화하시기 바람

나. 개선사항

⑴ IT아웃소싱 서비스 수준 협약 관리 소홀

IT아웃소싱 서비스 수준 평가를 위해 수탁사와 합의서를 체결하고 총 ○○개의 평가지표를 기준으로 매월 평가하여 인센티브 또는 패널티를 적용하고 있으나,

장애 발생 지수 산정시 제외 대상 장애는 H/W 장비에 대한 장애로 제한되어 있으나, 프로그램 오류, 관리 소홀 등 제외 사유에 해당하지 않는 장애 총 ○○건을 부당하게 제외하여 장애 발생 지수를 평가하는 등 총 ○○개의 평가 지표를 소홀히 관리하였고

장애보고 시점에 장애 원인 불명인 경우와 재발 방지 대책이 중장기 계획인 경우, 사후 진행결과를 확인하지 않은 사례가 있으므로

앞으로, 장애 사후관리가 포함되도록 IT아웃소싱 서비스 수준 협약 내용을 보완하고 평가 지표 측정을 강화하는 등 IT아웃소싱 서비스 수준 협약 관리를 개선하시기 바람

⑵ IT프로젝트 관리 미흡

매년 정보기술부문 계획을 수립하고 동 계획에 따라 검사대상기간 중 총 ○○건의 정보시스템 구축 및 도입 프로젝트를 추진하면서

① IT프로젝트는 현업부서·IT부서·구축사가 각각 프로젝트 매니저(PM)를 지정하여 협업을 통해 프로젝트를 추진하는 것이 일반적인데, IT프로젝트 추진 관련 내규를 마련하지 않은 채 가이드라인에 해당하는 「U가이드」에 따라 현업부서와 구축사 PM만 지정하고 IT부서는 지원업무*만을 수행하였음

* (예시) 테스트 단계 중 단위 및 통합테스트에 참여하지 않은 채 결함 조치 확인 등을 지원

② 계약금액 및 일정 변경이 발생한 계약변경의 경우, IT프로젝트 범위관리 미흡으로 요구사항 증가 및 변경 등이 발생함에 따라 IT예산 및 구축 일정이 증가하여 연간 정보기술부문 계획을 적기에 이행하지 못하였음

③ 또한, IT프로젝트 종료 시 프로젝트를 종합적으로 점검하고 문제점을 개선할 수 있도록 계약종료일 이전에 검수를 완료해야 함에도, 총 ○○건(59.9%)의 IT 프로젝트가 계약종료일 이후에 검수 완료되었음

앞으로, IT프로젝트 운영 관련 내규를 마련하고 IT프로젝트가 계획된 범위 및 일정 내에 추진될 수 있도록 IT프로젝트 관리를 개선하시기 바람

⑶ IT부서 자체감사 업무 미흡

① Q팀은 내규 「D지침」에 따라 IT·정보보호 업무 감사를 수행하고 있으나, IT부서는 자체감사에 대한 별도의 내규를 마련하지 않은 채 업무매뉴얼에 해당하는 「E매뉴얼」에 따라 업무를 수행하고 있음

② Q팀은 「D지침」에 따라 IT전담 감사인을 지정·운영하고 있으나, IT부서 자체감사자는 IT감사 대상 업무인 a·b 및 c 등의 업무를 함께 수행하고 있어 IT감사 업무 독립성이 결여될 소지가 있음

③ IT부서 자체감사는 검사대상기간 중 연간 자체감사 계획을 수립하지 않았으며, 「E매뉴얼」에 따라 매월 IT자체 정기감사를 실시하고는 있으나, 이는 체크리스트에 따라 정보처리시스템 운영현황 중 특이사항 유무를 체크하는 수준으로 IT 전반을 감사하기 위한 정기감사 실적은 없음

앞으로는 IT부서 자체감사 관련 내규를 제정하고, 연간 감사계획을 수립하여 정기적으로 종합감사를 실시하는 등 IT부서 자체감사 체계를 강화하시기 바람

⑷ 프로그램 변경·통제 절차 강화

내규 「F규정」, 「G매뉴얼」, 「H매뉴얼」에 프로그램 개발, 유지보수 및 테스트 등의 절차가 규정되어 있고, 전산개발관리시스템 및 형상관리시스템을 이용하여 프로그램을 변경·통제하고 있으나,

프로그램 변경시 연계 프로그램에 대한 영향도 분석 등의 절차가 누락되어 있고, 개발자가 변경한 프로그램을 직접 운영환경에 적용*할 수 있어, 전산개발관리시스템 및 형상관리시스템의 프로그램 변경·통제 미흡으로 인한 전산사고가 발생할 우려가 있으므로

* 개발자가 변경한 프로그램을 직접 운영환경으로 적용하지 못하도록 내규화하고 있으나, 전산개발관리시스템 및 형상관리시스템에서 강제화되어 있지 않음

프로그램 변경시 연계 프로그램의 영향도 분석 등 주요 사항에 대한 점검이 선행되도록 관련 절차를 개선하고, 개발자가 변경한 프로그램을 직접 운영환경에 적용하지 못하도록 관련 시스템을 개선하는 등 내부통제 절차를 강화하시기 바람

⑸ 일괄작업 운영 관리 미흡

내규 「I매뉴얼」에 일괄작업 관리담당자의 임무 등을 규정하고 일괄작업 모니터링 시스템을 통해 일괄작업을 통제하고 있으나,

검사대상기간 중(2018. 1. 1. ~ 2022. 6. 29.) 프로그램 일괄작업 처리결과 동일한 오류*가 지속적으로 발생하였음에도 발생한 오류에 대한 원인분석, 프로그램 수정 및 스케줄링 조정 등을 수행하지 아니하여 전산장애가 발생할 우려가 있으므로

* 2021년 이후 일괄작업 오류건수 : 6,899건, 10회 이상 반복오류 프로그램 : 95개

앞으로 주기적으로 일괄작업 처리결과를 점검하여 동일한 오류가 지속·반복적으로 발생하는 프로그램에 대해 원인분석을 실시하여 적기에 프로그램을 수정하는 등 일괄작업의 관리를 강화하시기 바람

⑹ 정보처리시스템 감리기준 수립 미흡

내규 「J지침」 제1조 및 제3조 등에서 정보처리시스템의 안전성 및 효율성 확보를 위하여 전자금융업무 및 그 기반이 되는 정보기술부문과 관련된 외부주문 등을 제3자가 감리하도록 정하고 있으나,

감리대상을 정보처리시스템 구축 사업비가 100억원 이상이고, 개발 기간이 12개월 이상인 개발 프로젝트로 기준이 높게 설정되어 있어 중요 정보처리시스템이 감리대상에서 제외되어 정보시스템의 효율성 및 안전성 확보가 미흡할 우려가 있으므로

감리대상이 되는 IT사업비 기준을 하향 조정하고, 대고객 전자금융업무 시스템구축 및 다수의 전자금융업무에 영향을 미치는 IT사업 등을 감리대상에 포함시키는 등 중요 정보처리시스템에 대한 감리가 이루어질 수 있도록 감리대상 기준을 강화하시기 바람

⑺ 전산원장 변경통제 절차 운영 미흡

① 「K매뉴얼」에서 긴급변경 가능 업무를 프로그램 변경, 프로젝트 지원 및 모니터링 등으로 한정하고 있으며 「L지침」에서 전산원장 변경 시 사전에 제3자가 변경의 적정성을 검토하도록 규정하고 있으나,

검사 대상기간 중(2018. 1. 1. ~ 2022. 6. 29.) 데이터베이스 보정 시 사후승인이 허용된 프로그램 긴급변경 절차를 이용한 사례가 있어 전산원장 등 주요 데이터 변경 시 해당 절차가 사용되어 제3자의 확인 없이 전산원장을 변경할 우려가 있으므로

앞으로 데이터베이스 보정 시 전산원장 등 중요 데이터의 변경 절차와 일반 데이터 변경 절차를 구분하여 정의하는 등 프로그램 긴급 변경 절차와 혼용하여 사용하지 않도록 데이터 변경 절차를 세분화하고

데이터베이스 보정 이력을 관리하는 프로그램에서 전산원장 변경 건의 작업 근거를 확인할 수 있도록 시스템을 개선하여 전산원장 변경 근거를 확인하기 용이하게 시스템을 변경하는 등 전산원장 변경 통제를 강화하시기 바람

② 「M매뉴얼」에 따라 전산원장 변경시 정보보호담당자와 O팀이 전산원장 변경 요청의 적정성에 대해 사전에 확인하고 있으나,

P팀이 작성한 전산원장 변경 프로그램 명령어(쿼리)의 적정성을 확인하는

사후 검증 절차가 존재하지 않아 P팀에서 프로그램 명령어를 임의로 변경할 수 있는 가능성이 있으므로

앞으로 전산원장 변경 시 P팀이 작성한 쿼리를 현업 및 IT자체감사인 등 제3자가 확인 후 시스템에 의해 자동 실행될 수 있도록 하여 P팀이 프로그램 명령어를 임의로 변경할 수 있는 가능성을 사전에 차단하는 등 전산원장 변경 절차를 강화하시기 바람

⑻ 모바일 앱카드 부정사용 예방활동 불철저

모바일 앱을 이용한 신용카드 부정결제 및 불법적인 접근을 예방하기 위해 모바일 앱이 설치된 이용자의 단말기에서 발생한 이상징후 탐지내역을 실시간으로 수집하고 있으나,

① 검사착수일(2022. 6. 9.) 현재 내규「R지침」제14조 제5항*에도 불구하고 이상징후 탐지로그를 3일만 보관 후 삭제처리를 하고 있으며 특정 운영체제에서 탐지된 패턴정보가 누락되는 등 이상징후 인지가 불가하여 사전 예방조치를 적시에 시행하지 못할 우려가 있으므로

* 제14조(로그 관리) ⑤ 정보보안 이벤트 관련 로그는 최소 1년 이상 보관

모바일 앱이 설치된 이용자의 단말기에서 수집된 이상징후 탐지로그를 최소 1년 이상 보관하도록 보관주기를 변경하고, 일부 운영체제의 탐지패턴 정보 누락 건에 대한 조치를 보완하여 모바일 앱 부정사용에 대한 사전 예방조치를 개선하시기 바람

② 검사기간 중 이용자 단말기에서 수집한 탐지정보 처리실태를 점검한 결과, 동일한 IP주소에서 다수의 앱설치ID가 반복적으로 탐지되고 있었음에도 이에 대한 이상징후를 분석하거나 이상금융거래탐지시스템(FDS)과 연계하여 부정거래를 차단하는 등의 사전 예방활동에 대한 업무가 상시 운영되고 있지 않아 모바일 앱카드 부정사용 사고 등을 미연에 방지하지 못할 우려가 있으므로

이용자 단말기에서 수집된 이상징후에 부정사용 여부 등을 판단할 수 있는 탐지로그 모니터링 기준을 수립하고, 이용자 단말기 탐지 로그를 분석하여 이상징후 발생 IP를 식별하는 등 동 IP주소를 이상금융거래탐지시스템(FDS) 등과 연계하여 모바일 앱카드의 부정 사용 사고 발생을 예방할 수 있도록 관련 절차를 개선하시기 바람

⑼ 전산자료 유출방지 대책 미흡

검사착수일(2022. 6. 9.) 현재 내규 「S규정」 및 「T지침」에 따라 전산자료 유출방지 대책 등을 수립하여 운용하고 있으나

① 전체 단말기에 대한 부팅 비밀번호 설정을 강제화하고 있지 않아 부팅 USB 등을 이용하여 부팅절차를 우회한 뒤 암호화되어 있지 않은 전산자료가 유출될 우려가 있으므로

부팅 비밀번호 설정을 내규에 반영하고 전체 단말기에 부팅 비밀번호를 설정하여 전산자료에 대한 유출방지 대책을 개선하시기 바람

② 기존에 시스템 접근권한이 부여된 甲이 인사이동 등으로 담당직무가 변동되는 경우 乙이 수작업으로 해당 직원에 대한 시스템 접근권한을 회수하고 있어 정보처리시스템에 대한 접근 통제가 누락될 우려가 있으므로

인사이동 등 직무 변경시 시스템 및 데이터베이스 접속 권한을 자동으로 회수하여 최소한의 권한만 부여되도록 접근제어시스템의 관련 기능을 개선하시기 바람

③ DB접근통제시스템에서 개인별 접속계정을 부여하여 접근권한을 통제하고 있으나 일부 개인(신용)정보처리시스템에서 데이터 조회시 주민번호에 대한 마스킹이 누락되어 있으며, 콜센터 전용 녹취시스템의 경우 별도의 로그인 기능을 제공하고 있지 않음에도 불구하고 구축 당시 초기 로그인 비밀번호가 DB에 그대로 저장되어 있는 등 중요 정보가 노출될 위험이 있으므로

운영 중인 개인(신용)정보처리시스템에 대해 마스킹 누락 여부 및 비밀번호 노출 여부를 전수 점검하여 중요 정보가 유출되지 않도록 보안 통제를 개선하시기 바람

⑽ 취약점 분석·평가 사후 관리 미흡

전자금융기반시설의 취약점 분석·평가를 연 1회(홈페이지는 6개월에 1회) 실시하고 발견된 취약점에 대해서는 이행계획을 수립하여 취약점을 보완 조치하고 있으나,

① 취약점 점검 대상을 선정하는 기준 및 절차 등이 마련되어 있지 않아 취약점 분석·평가 담당자의 주관적 판단에 따라 임의적으로 선정될 우려가 있으므로

전자금융거래에 이용되는 정보처리시스템(서버, 네트워크장비, 정보보호시스템 등) 현황을 정기적으로 현행화하고, 취약점 점검 대상 선정시 해당 시스템이 누락되지 않도록 업무 절차를 개선하시기 바람

② 검사대상 기간 중 홈페이지 취약점 분석·평가를 실시한 결과 ○○○○ 등 중대한 취약점이 홈페이지에서 최초 발견되어 취약점 보완 조치를 완료하였으나, 홈페이지 이외에 다른 채널에도 동일한 취약점이 있는지 여부를 확인하지 않는 등 취약점 분석·평가 사후 관리를 소홀하게 운영하고 있어 보안 위협이 증가할 우려가 있으므로

○○○○ 등 중대한 취약점 발견시, 해당 기능이 구현되어 있는 다른 영역(동일 기능 페이지 등)에도 동일 취약점이 존재하는지 확인하여 조치할 수 있도록 업무 프로세스를 개선하시기 바람

⑾ 망분리 예외사이트 통제 절차 미흡

내부 업무망과 연결과 단말기 등에서 업무상 필수적으로 외부 통신망과 연결하여야 하는 경우 자체위험성 평가를 실시하고 망분리 대체 정보보호

통제를 적용하여 정보보호위원회 심의를 거쳐 망분리 예외 접속을 허용하는 절차를 수립·운용하고 있으나,

현업부서에서 요청한 망분리 적용 예외 사이트의 접속 필요성에 대한 충분한 내용없이 丙이 자체위험성 평가를 실시하고 정보보호위원회에 안건을 부의하는 등 동 위원회에서 이에 대한 필요성을 충분히 인지하지 못하고 동 안건을 의결할 우려가 있으므로

내부 업무망과 연결된 단말기에서 망분리 예외접속 필요시 접속 필요성 등을 충분히 검토 후 정보보호위원회에서 의결하도록 절차를 개선하시기 바람