경영유의사항 등 공개안

1. 금융기관명 : KB캐피탈(주)

2. 조치일 : 2019. 7. 17.

3. 조치내용

대상	내용
기 관	경영유의사항 2건, 개선사항 8건

4. 조치대상사실

가. 경영유의사항

(1) IT관련 내규 관리체계 개편을 통한 내부통제 강화

① 정보보호본부는 정보처리시스템 및 정보보호 관련 규정 O개, 지침 OO개 등 총 OO개의 내규를 마련하여 IT 및 정보보호 업무에 관련된 사항을 규정하고 있으나,

정보시스템 관리·운영에 필요한 「정보시스템 운영지침」, 「프로그램 개발지침」, 「네트워크 운영지침」 등 필수 정보처리시스템 운영지침을 마련하지 않았고, IT관련 내규가 정보보호 업무에 편중(OO.O%)되어 있으므로

정보시스템 운영, 프로그램 개발 등에 필요한 IT관련 지침을 제정하고, 정보보호부에 편중되어 있는 지침은 통합하는 등 IT관련 내규 관리체계를 IT조직규모에 맞게 개편하여 내부통제를 강화할 필요

② IT관련 내규 이외에 업무 매뉴얼, 가이드 및 지침서 등을 부서별로 제·개정하고 있으나,

일부 업무매뉴얼은 제품의 기능을 설명하는 수준으로 작성되어 업무담당자가 업무에 활용하기 어렵고, 최근 도입한 OOO시스템(OO-OO)의 「OOO 관리 사용자매뉴얼」, 「OOO&O 운영매뉴얼」 등은 회사의 운영 환경이 반영되지 않은 상태로 관리되고 있으므로

IT부서에서 제정 및 관리하고 있는 업무매뉴얼, 가이드 및 지침서 등은 회사의 운영 현황에 적합하게 작성하고, IT환경 변화를 지속적으로 반영하여 현행화할 필요

③ 회사에서 관리하는 IT관련 내규를 포털(OO-OOOOOOO)에 게시하여 전 직원이 열람·참고할 수 있도록 운영하고, OOOO시스템의 '지식관리> Knowledge' 메뉴에도 내규를 게시하고 있으나,

OOOO시스템에 게시된 IT관련 내규에는 최근 제·개정된 내용이 누락되어 있는 등 포털에 게시된 내규와 상이하므로

내규를 관리하는 준법지원부와 협의하여 내규 게시를 일원화하거나 게시된 내규가 다르지 않도록 통일하는 등 내규 관리를 강화할 필요

(2) IT사업계획 수립 및 운용관리 강화

정보보호위원회는 연간 IT사업 계획 및 예산을 심의·의결하고, '투자심사위원회'는 신규 투자사업(O억원 이상)에 대해 타당성 검토 결과를 심의·의결하여 IT사업을 추진하고 있으나,

신규 IT사업 추진 시 사업의 필요성, 추진방안 및 일정 등 사전에 충분한 타당성 검토를 실시하기 위한 담당부서, 검토시기 및 방법 등 세부적인 업무절차를 마련하지 않아 OOOO년~OOOO년 기간 중 추진한 IT사업이 수차례 지연 또는 추진되지 않아 연간 IT사업 예산 대비 집행률이 저조하고,

OOOO년에는 IT사업에 대한 타당성 검토 결과를 투자심사위원회에 상정한 이력이 없고 연초 수립한 주요 IT사업이 추진되지 않는 등 IT사업에 대한 타당성 검토 및 사업 추진 관리가 미흡하며,

IT전략계획 수립 및 이행상태를 감시하여야 할 'IT운영위원회'를 구성·운영하지 않고, '투자심사위원회'를 통해 회사 전체에서 추진하는 주요 사업의 타당성만 심의하고 있어 전사 차원의 IT사업계획 수립 및 추진과정에 대한 감시가 미흡하므로

IT사업 추진 시 사전 타당성 검토에 대한 세부 절차를 마련하여 타당성 검토 관리를 강화하고, 「IT운영위원회 운영지침」을 마련하여 IT사업계획 및 추진상황에 대한 심의·의결을 위한 'IT운영위원회'를 구성·운영하는 등 IT사업계획 수립 및 운용관리를 강화할 필요

나. 개선사항

(1) IT감사 업무 불합리

① 감사부는 내규「감사업무규정」에 따라 부문감사와 종합감사를 실시하여 IT부문의 안정성과 건전성을 평가하도록 규정하고 있으나,

검사대상기간 중 IT부서에 대한 종합감사 실시이력은 O회에 불과하고, 감사부 내 IT감사 담당자가 다른 감사업무를 겸임하고 있어 전산원장 통제, 프로그램 통제 및 일괄작업 통제 등 IT부서의 특정업무에 대한 부문감사를 실시할 여력이 없으며, IT부서 내에 자체감사 담당자가 지정되지 않아 자체감사를 실시한 사례가 없으므로

IT부문에 대한 주기적인 감사가 이루어질 수 있도록 IT감사계획을 수립·실시하고, IT자체감사에 대한 객관적인 평가기준 마련 및 IT자체 감사역 지정 등을 통해 실효성 있는 자체감사를 실시할 필요

② 내규「감사업무지침」에 의하면 감사운영, 감사결과의 보고 및 처리, 감사결과 조치와 사후관리 등 재무, 준법, 업무, 경영, IT 분야에 공통적으로 적용되는 내용을 명시하고 있으나,

IT감사 범위에 대한 기준을 마련하지 않았고, IT감사역의 책임과 역할 및 업무절차 등을 포함한 매뉴얼(업무편람) 등을 마련하지 않고 있으므로

IT부문 감사 수행주기, 감사범위 등을 내규에 반영하고, IT감사역의 책임과 역할, 업무절차 등을 포함하는 IT감사 매뉴얼(업무편람) 마련 등을 통해 일관된 감사체계를 운영할 필요

(2) IT업무 위탁관리 불합리

① 정보보호본부는 침해대응 모니터링 및 관제센터 운영·관리 등의 업무를 위탁하면서 외주인력에 대한 신원보증서 징구 및 외주업체에 대한 재무건전성 평가 등은 수행하고 있으나,

외부주문 서비스의 수준관리 및 비용지불의 합리성을 제고하기 위한 서비스수준약정서(SLA) 계약 체결 없이 운영하고 있으므로

IT업무 위탁계약 체결 시 서비스수준약정서(SLA)을 작성하여 품질관리 및 비용 지급의 적정성 등을 평가하여 관리할 필요

② OO에는 전산센터(OOOO 소재) 내 IT운영관제 업무를 본사(OOO 소재) IT직원이 원격으로 관리하고 있으나,

OO 및 OO에는 운영관제가 이루어지지 않아 장애 등 비상상황 발생 시 신속한 대응에 어려움이 예상되므로

OO 및 OO 운영업무에 대한 전담자를 지정·운영하는 등 OO, OO에 발생하는 비상상황에 대비한 실시간 대응체계를 마련할 필요

(3) 비상계획 불합리

① 업무지속성 확보를 위해 자체적으로 시스템별 전산자료, 운영체제 및 프로그램 등을 백업하고, 중요자료를 소산 보관하고 있으나,

IT부문 비상계획서에 시스템 도입(OOO시스템 포함) 이후 인프라 구축 현황, 금융거래 자료 복원 및 전산서비스 개시절차 등을 포함하지 않아 미흡하므로

비상사태 발생 시 업무지속성 확보를 위해 IT부문 비상계획서를 재정비하는 등 비상대응체계를 개선할 필요

② OOOO년~OOOO년 기간 중 실시한 재해복구 훈련은 IT부서 직원이 백업 자료를 활용하여 OOO 데이터를 복구하고 복구된 데이터의 물리적 정합성만 확인하는 수준으로 진행하여 다양한 비상상황에 대비한 대응체계가 미흡하므로

현업부서 직원이 참여할 수 있는 훈련 시나리오를 마련하여 복구된 데이터를 통해 운용 가능성을 확인하는 등 훈련 범위를 확대하고, 다양한 비상상황을 고려하여 훈련의 실효성을 확보할 필요

(4) 프로그램 변경통제 불합리

① OOO 등 주요 프로그램은 OOO시스템 구축을 통해 신규 도입한 형상관리시스템(OOOOO)과 IT서비스관리시스템(ITSM)을 통해 프로그램 변경·이관 및 승인·작업이력 등을 일괄 관리하고 있으나,

OOO의 OOOO 및 OOO 프로그램의 경우 이관, 승인 등 관리기능이 부족한 SVN(Subversion) 방식의 소스코드 버전관리시스템을 운영하고 IT서비스관리시스템(ITSM)과 연동하지 아니하여 체계적인 프로그램 변경관리가 어려우므로

OOO의 OOOO 및 OOO 프로그램에 대해서도 형상관리시스템을 적용하여 프로그램 변경·이관 통제 절차를 강화할 필요

② 프로그램 변경 시 IT서비스관리시스템(ITSM)을 통해 개발자 테스트 및 현업검수 확인을 거쳐 책임자 승인 후 운영시스템에 반영하고 있으나,

테스트 결과에 대해서 테스트 실시 유무 기록 이외의 '테스트결과서' 등 테스트 실시 관련 내용을 상세하게 기록·관리하지 아니하여 테스트 적정성에 대한 객관적인 확인이 어려우므로

프로그램 변경 시 IT서비스관리시스템(ITSM)에 '테스트결과서' 등 테스트 수행결과를 기록·관리하여 테스트 적정성을 확인할 수 있도록 통제절차를 개선할 필요

(5) 미사용 전산장비 관리 불합리

내규「전산규정」에 의하면 노후화되어 재활용이 불가능한 전산장비는 내부에 기록된 데이터 등을 재생할 수 없는 형태로 파기한 후 폐기절차에 따라 폐기하도록 규정하고 있으나,

사용이 종료된 전산장비(서버 OO대)를 내부 네트워크에 연결된 상태로 운영장비와 분리하지 않고 동일한 랙(RACK)에 방치하여 상대적으로 보안관리가 소홀한 미사용 전산장비에 의한 운영시스템에 악성코드 감염 등의 우려가 있으며,

전산센터 내에 보관하고 있는 폐기대상이나 아직 폐기하지 못한 하드디스크 및 백업 테이프를 시건장치 등이 미흡한 일반 캐비넷에 보관하고 있어 도난·분실에 의한 내부정보의 외부 유출 우려가 있으므로

미사용 전산장비는 운영장비와 분리하여 별도로 관리하고 폐기절차에 따라 전산장비 및 저장매체를 폐기하는 등 미사용 전산장비 관리절차를 개선할 필요

(6) 백업장비 가용성 관리 불합리

백업장비(OOO, OOO)를 통해 주요 전산자료를 정기적으로 백업하여 전산센터(OOOO 소재)에 보관하고 본사(OOO 소재)에 소산하고 있으나,

OOO시스템 오픈(OOOO.O.OO.) 이후 현재(OOOO.O.OO.)까지 백업장비(OOO)의 호환성 문제, 용량 부족 등의 원인으로 인해 OOOO시스템 등 일부 백업 실패가 지속적으로 발생하고 있어 비상상황 발생에 대비한 시스템 복원용 백업자료 확보가 미흡하므로

백업 대상자료 대비 백업장비 용량을 재검토하여 용량 증설 등 가용성 확보방안을 마련하고, 백업장비와 시스템 간 호환성 문제로 인한 백업 오류 문제를 해결하는 등 백업장비 운영을 개선할 필요

(7) 이상징후 모니터링 등 정보보호 관리 불합리

해킹 방지를 위하여 OOOO, OOOO시스템, OOOO시스템 및 OOOOOOO시스템 등을 도입하고 KB그룹사 보안관제센터(OOOOO㈜ 도급)에서 보안관제 모니터링을 실시하며, 개인정보처리시스템 로그 및 보안솔루션 로그를 수집하여 내부 임직원에 대한 개인정보 유출 및 오남용 등을 모니터링하기 위한 정보보호 모니터링 솔루션을 도입하였으나,

OO OO 등 단편적인 보안 로그 분석 이외에 추가적인 정밀 로그 분석(이벤트 분석 등)을 실시하지 않았고, 정보보호 모니터링 솔루션에 개인정보처리시스템 로그를 연동하지 않고 시나리오 기반의 모니터링 규칙을 적용하지 않아 개인정보 유출 및 해킹 등에 따른 이상징후 탐지가 어려우므로

정보보호 모니터링 솔루션에 개인정보처리시스템 로그를 연동하여 정밀 로그 분석을 실시하고, 이미 연동된 정보보호 장비에 대해 시나리오 기반 탐지 규칙을 생성하여 이상징후를 탐지하는 등 모니터링을 강화할 필요

(8) 개인신용정보 조회 모니터링 불합리

업무시스템의 개인신용정보 과다조회 모니터링을 위하여 개인신용정보에 대한 출력 승인 및 다운로드 이력, 개인신용정보 초과접근시도 통제 등록 등을 확인할 수 있는 기능을 개발·운영하고 있으나,

개인신용정보 과다조회 탐지 규칙에 오류가 발견되는 등 모니터링 관리가 미흡하므로

업무시스템 과다조회 모니터링에 대한 탐지규칙을 정비하여 탐지율을 제고하는 등 개인신용정보 조회 모니터링을 개선할 필요