경영유의사항 등 공개안

1. 금융기관명 : 에스비아이저축은행

2. 조치일 : 2018. 10. 2.

3. 조치내용

대상	내용
기 관	경영유의사항 1건, 개선사항 8건

4. 조치대상사실

가. 경영유의사항

(1) IT사업 계획 수립·운용에 대한 관리 강화

정보보호위원회의 심의·의결을 거쳐 연간 IT사업 계획을 수립 및 추진하고 있으나, IT사업을 추진하기 위한 사업 우선순위 결정, 의사결정 체계 등 세부적인 업무절차를 마련하지 않아 OOOO년~OOOO년 기간중 연간 IT사업 과제에 대한 사업 이행률(평균 OO%)이 저조한 편이며

심의·의결된 IT사업이 지연되거나 추진되지 않더라도 해당 사유, 향후 계획 등을 동 위원회에 보고하는 등 별도 관리하지 않아 중요 IT사업이 적시에 이행되지 못할 우려가 있으므로

사업의 중요성, 성과지표 등을 근거로 IT사업 우선순위를 결정하는 등 IT사업 계획 수립 및 추진에 대한 세부절차를 마련하여 IT사업이 효과적으로 추진될 수 있도록 하고, 계획된 IT사업이 지연되거나 추진되지 않는 경우 지연사유 등을 정보보호위원회에서 심의하는 등 IT사업 계획 수립·운용에 대한 관리를 강화할 필요

나. 개선사항

(1) IT자점감사 업무 불합리

감사부에서는 본점부서 및 영업점에 대한 자점감사 제도를 운영하고 있고 정보시스템실 내 자점감사자가 '전산운영상 이상여부' 등 일일감사 대상항목(총 O개)을 점검하고 있으나, 부서별 업무 특성을 고려하지 않고 일률적으로 감사대상항목을 선정함으로써 자점감사 업무의 실효성이 낮고,

점검결과보고서를 작성하거나 보고하는 절차 없이 이상여부 만을 감사관리시스템에 등록하고 IT부문의 자점감사 제도 시행 이후 현재까지 미흡사항을 지적한 사례가 없는 등 형식적으로 운영하고 있으므로

IT부서별 업무 특성에 적합한 감사대상항목을 선정하여 감사를 실시하고 IT자점감사 점검결과보고서를 작성하여 보고하는 등 IT자점감사 업무를 강화할 필요

(2) IT사업 검수 및 대금 지급 관리 절차 불합리

IT사업 완료 시 사업발의 부서의 계약담당자가 검수확인서를 작성하고 제3자에 의한 확인절차를 운영하고 있고, 대금 지급 시 재무경리 담당자가 전산시스템에 등록된 사업품의서, 세금계산서 등의 제반 증빙자료를 확인하고 있으나,

① 내규「계약규정」에는 제3자 확인절차를 명시하지 않고 계약담당자가 스스로 검수할 수 있도록 규정하고 있어 검수가 공정하게 이루어지지 않을 우려가 있으므로 검수확인서에 대한 제3자 확인절차가 명시되도록 해당 내규를 개정할 필요

② 검수확인서에 대한 기록·관리가 미흡하여 총 OO개 IT사업 중 'OOO OOOO OOOO OO' 등 OO개 사업에 대해서는 검수확인서를 관리하고 있지 않으므로 검수확인서를 IT사업에 대한 필수 산출물 목록에 포함하여 체계적으로 기록·관리할 필요

③ 대금 지급 시 정보시스템 설치·가동 여부를 확인할 수 있는 검수확인서를 필수 검토서류 대상에 포함하지 않아 IT사업에 대한 검수 및 대가 지급에 대한 신뢰성을 보장하기 어려우므로 IT사업에 대한 대금 지급 시 검수확인서를 필수적으로 확인할 필요

(3) 불용 IT전산기기 관리 불합리

내규「출입 및 시설보안관리 지침」에 의하면 하드디스크 등 저장매체를 폐기처분할 때에는 초기화 프로그램을 사용하여 데이터 삭제(이하 '포맷') 후 물리적으로 폐기하고, 전문업체를 통해 전산기기를 폐기하는 경우 실제 이행여부를 확인해야 하며

내규「업무용정보자산보안 관리 지침」에서는 개인PC 및 저장매체 폐기 시 하드디스크를 재사용하지 못하게 디가우징(Degaussing)하도록 규정하고 있으나,

외부업체를 통한 전산기기 폐기 요청 시 장비에 장착된 하드디스크 등 저장매체에 대한 수량을 명시적으로 기록·관리하지 않아 폐기대상 매체의 정확한 수량 파악이 곤란하고

내규「업무용정보자산보안 관리지침」와 달리 개인PC 하드디스크는 천공 작업으로 폐기 처리하면서 사전 포맷 여부 등에 대해서는 관리하고 있지 있으며,

외부업체로부터 불용 하드디스크의 폐기작업 결과보고서를 받고 있으나, 동 보고서에 폐기 담당자, 입회자, 하드디스크의 고유번호 등이 상세하게 기재되지 않아 내부 직원의 현장입회 여부 및 폐기대상 하드디스크의 일치 여부를 사후검증하기 어렵고 최종 처리결과도 정보보호최고책임자에게 보고하지 않고 있으므로

불용 IT전산기기 처리대상 목록을 상세하게 기록하고, 하드디스크 등 저장매체 폐기 시에는 사전 포맷 결과 등을 관리하며, 폐기대상 하드디스크의 고유번호를 확인하여 일치 여부를 검증하는 한편, 폐기 결과보고서에 폐기 담당자, 입회자, 폐기대상 목록 등을 상세히 기록하고 정보보호책임자에게 최종 처리결과를 보고하는 등 불용 IT 정보자산 관리 절차 개선 필요

(4) 백업·소산 등 비상대책 관리 불합리

① 주전산센터의 전산원장 등 주요 전산자료를 백업하고 있으나, OOO OO 데이터 및 OO OOOO 등 OOO OO데이터의 경우 백업 대상에 포함하지 않아 장애·재해 발생 시 고객응대에 필요한 OOOOO 및 OOO OOOO 데이터의 소실로 인해 회사 업무 정상화에 지연이 우려되므로 OOO OO데이터 및 OOOO OO데이터 등을 백업 대상에 포함할 필요

② 주요 백업자료에 대한 소산을 OO 주기로 실시하고 있어 재해발생 시 최장 OOO 동안의 금융데이터의 소실 우려가 있으므로 주요 백업자료의 소산 주기를 단축할 필요

③ 소산용 백업테이프의 경우 OO의 내화금고에 보관하고 내역을 소산관리대장에 수기로 관리하고 있으나, 백업테이프의 반입·반출 이력을 별도 기록·관리하지 않아 관리대장과 소산된 백업테이프의 현황이 불일치하게 되는 경우 추적·관리에 어려움이 예상되므로 소산 백업테이프에 대한 반입·반출 이력을 기록·관리할 필요

④ 매년 재해복구훈련 시 백업자료 복구에 대한 검증을 실시하고 있으나, 소산데이터에 대해서는 복구테스트를 실시하지 않아 비상 상황 발생 시 소산데이터를 이용한 복구 작업이 신속하게 이루어지지 않을 우려가 있으므로 소산데이터를 활용한 복구테스트를 실시할 필요

(5) 일괄작업(batch) 통제 관리 불합리

① 일괄작업(batch)을 관리하기 위하여 일괄작업 모니터링 시스템을 설치하고, 개발담당자가 일괄작업의 등록·변경을 요청할 경우 부서장 승인 후 일괄작업 운영관리자가 요청 작업을 일괄작업 모니터링 시스템에 등록하고 있으나,

작업 요청 근거, 내용 등 상세 내용을 기록하지 않고 요청일자, 작업명, 등록·승인자 이름만 파일에 수기로 관리함으로써 일괄작업 내용에 대한 정당성 여부 및 부서장 승인일시 등 확인이 어려우므로

일괄작업에 대한 등급분류, 전결기준, 긴급 배치작업 등의 세부 절차를 마련하고 프로그램 변경관리에 사용되는 전산요청관리시스템(ITSM) 등 전산시스템을 활용하여 일괄작업 요청·승인 등의 이력을 체계적으로 관리할 필요

② 일괄작업 수행 과정에서 오류가 발생하여 이를 재수행하는 경우, 개발담당자에게 전체 일괄작업에 대한 등록·변경이 가능한 운영자 권한을 부여하고 있어 개발담당자의 조작 실수 등으로 인해 다른 일괄작업에까지 영향을 미칠 우려가 있으므로

오류로 인한 배치작업 권한부여 시 해당 일괄작업에 대한 재수행 권한만 제한적으로 부여하도록 운영할 필요

③ 일괄작업 운영 관리자 업무를 OO OOO 소속 파트장이 겸임하고 있어 OO업무에 대해서는 변경내용의 정당여부에 대한 제3자 확인이 이루어지지 않는 등 통제가 적절하게 이루어지지 않을 우려가 있으므로 이에 대한 보충통제 방안을 마련하는 등 개선 필요

(6) 프로그램 통제 관리 불합리

IT서비스관리시스템(ITSM)을 통해 프로그램 등록·변경 등을 관리하고 개발담당자가 운영시스템으로 프로그램 이관을 요청하는 경우 부서장 승인 후 개발팀 파트장이 이관 작업을 실시하도록 통제절차를 마련하고 있으나,

프로그램 통제 담당자의 역할과 책임, 상황별(일반/긴급) 프로그램 변경·이관에 대한 승인(사전/사후) 등 세부 업무절차를 내규에 반영하지 않았고, 긴급프로그램 변경 시

IT서비스관리시스템(ITSM)에서 결재 단계를 임의 지정할 수 있도록 기능을 구현하여 개발담당자가 프로그램 변경 통제 절차를 우회할 수 있으므로

프로그램 통제 관련 세부 업무절차를 내규에 반영하고 IT서비스관리시스템(ITSM)에서 긴급프로그램 변경 건에 대한 부서장 사후결재 기능을 적용하는 등 프로그램 통제 절차 개선 필요

(7) 데이터베이스 접근통제 관리 불합리

데이터베이스에 대한 접근권한 통제 및 접근이력 등을 관리하기 위해 DB접근통제 솔루션을 설치·운영하고 있으나,

OOO OOOO 등 일부 OO서버에는 동 솔루션을 적용하지 않아 데이테베이스 통제 절차를 우회할 가능성이 있고, 사용자별 명령어 통제 및 접근이력 관리 등이 어려우므로 OO정보가 저장된 OO서버 등에 DB접근통제솔루션을 확대 적용하여 데이터베이스에 대한 접근통제 관리 강화 필요

(8) 서버 운영체제(OS) 관리 불합리

운영 서버 총 OOO대 중 일부 서버에서 제조사로부터 기술지원이 종료되어 보안 패치 및 서비스 업그레이드 등의 지원을 받지 못하는 운영체제(OS)를 사용하고 있어 시스템 오류 및 장애 발생 시 신속한 대응이 어렵고, 신규 취약점을 악용한 해킹 및 악성코드 감염 등이 발생할 우려가 있으므로

기술지원이 종료된 운영체제를 업그레이드 하거나 제조사와 기술지원 연장 계약을 체결하는 등 운영체제 장애발생을 미연에 방지하기 위한 구체적인 대응 계획을 마련·운영할 필요