경영유의사항 등 공개안

1. 금융기관명 : 상호저축은행중앙회

2. 조치일 : 2018. 12. 12.

3. 조치내용

대상	내용
기 관	경영유의사항 2건, 개선사항 5건

4. 조치대상사실

가. 경영유의사항

(1) 재해복구시스템 성능·용량 산정기준 강화

재해복구시스템의 성능 및 용량을 차세대시스템 구축 컨설팅 회사(OOOO)에서 권고한 운영서버(O대) 대비 OO%수준으로 산정하고 있으나

재해복구센터에 구축 중인 OOOO 재해복구(DR) 서버(OO, OO)의 CPU, 메모리 등 장비의 성능 커버리지 비율이 주전산센터 OOOO 운영서버의 실제 사용량에 비해 크게 부족하여 現수준으로는 재해복구센터로 전환시 적절한 수준의 성능을 보장하기 어려울 것으로 예상되므로

복구대상 업무에 대한 실제 가동률(최대 처리용량 등) 및 보정사항 등을 상세히 분석하여 재해복구시스템의 최소 성능기준을 재해복구 대상 업무가 현저하게 지연되지 않는 수준으로 설정·보완하는 등 재해복구시스템의 성능·용량에 대한 산정기준을 실효성 있게 운영할 필요

(2) 취약점 분석·평가 관리 강화

전자금융기반시설 취약점 분석·평가를 연 1회 실시하고 결과보고 및 보완조치 이행계획을 단기(1년 이내) 및 중장기(1년 이상) 조치 건으로 구분하여 최고경영자에게 보고하고 있으나,

2015년~2017년 발견된 일부 취약점의 경우 기술적인 제약 또는 차세대시스템과 연관성이 없음에도 장애발생 우려의 이유로 차세대시스템 구축 이후의 중장기 조치계획으로 수립하여 취약점이 최장 2년 이상 장기간 잔존함으로써 전년도 대비

취약점 재발견 비율은 2016년 OO%(OO건), 2017년 OO%(OO건)에 이르고, 최종 잔여 취약점 대비 조치 완료율이 2016년에는 OO%(OO건), 2017년에는 O%(O건)에 불과하여 조치 완료율이 저조하며,

매년 이행계획의 시행 결과에 대한 최고경영자 보고 시에는 단기조치(조치율 100%) 건을 대상으로 하고, 중장기조치 건에 대해서는 보고하지 아니하여 최고경영자가 잔존 취약점의 제거 또는 위험 수용 등 보안리스크에 대한 합리적인 의사결정을 함에 있어 어려움이 예상되므로

보안리스크를 고려하여 취약점에 대한 보완조치가 지연 없이 이행될 수 있도록 관리 방안을 마련하고, 단기 및 중장기 조치계획에 대한 이행 결과를 최고경영자에게 모두 보고하는 한편, 취약점을 제거 또는 이에 상응하는 조치가 불가한 경우 최고경영자 승인을 득하여 관리하는 등 취약점 분석·평가 관리를 강화할 필요

나. 개선사항

(1) 시스템 개선 요구사항 관리 불합리

차세대시스템 오픈 이후 시스템 안전성 확보를 위해 개별 저축은행에서 발생하는 개선 요구사항 등을 전달받아 IT부서에서 처리하고 있으나,

개선 요구사항에 대하여 조치내역을 상세하게 기록·관리하지 아니하여 조치 결과의 적정 여부를 판단하기 어렵고, 진행 중인 개선 요구 건에 대해서는 향후 조치 일정, 조치 계획 등의 내용을 작성하지 아니하여 즉각적인 개선이 필요한 사항에 대한 조치 지연이 발생할 우려가 있으므로

저축은행의 개선 요구사항 등을 철저하게 분석하여 즉각적인 개선이 필요한 사항은 지체 없이 조치하고 조치내역 등을 상세하기 기록·관리하는 한편, 조치 결과에 대한 적정 여부를 확인하는 등 개선 요구사항 관리 방식을 개선할 필요

(2) 테스트데이터 변환·사용 절차 불합리

차세대시스템을 오픈 전에 테스트데이터 변환 솔루션(OOOOO)을 이용하여 주요 이용자 정보를 테스트데이터로 변환하고, OOO OO OO로 이관하였으나,

오픈 이후 동 솔루션의 라이센스 문제로 인하여 OOO OO시스템에 테스트데이터 변환·사용을 위한 작업 등록 및 결제, 사용목적 종료 후 즉시 삭제 등의 정책이 반영되지 않아 테스트 시 이용자 정보 변환 및 삭제 절차가 누락될 우려가 있으므로

테스트데이터 변환 솔루션을 OOO 관련 OO에 연동·적용하고 사용목적 종료 후 즉시 삭제하는 등 테스트데이터 변환·사용 통제 절차를 개선할 필요

(3) 손익계정 잔액대사 절차 불합리

정기예금, 일반자금대출 등 전산화된 업무와 관련된 정기예금잔액, 일반대출금 잔액 등 전산원장 파일의 합계액과 대차대조표 계정잔액의 일치여부를 매일 대사하고, 일치하지 않을 경우 그 원인을 파악하여 수정하는 등 전산원장 파일의 합계액과 대차대조표 계정잔액의 정합성을 유지하고 있으나,

OOOOOO, OOOOOOOO 등 전산원장 OOOO의 OOO과 OOOOOO의 일치여부를 대사하는 기능이 없어 프로그램 오류, 전산장애 및 원장수정 등으로 인한 OOOO OOO과 OOOOOO의 불일치가 발생 하였으므로,

계정계 시스템의 OOOOOO OOO과 OOOOO OO OO에 대한 상호 일치여부를 주기적으로 대사하여 프로그램 오류 등으로 인한 전산원장 합계액과 회계잔액의 불일치가 발생하지 않도록 업무를 개선할 필요

(4) 중요단말기 지정·관리 방식 불합리

주요 시스템 모니터링 및 원격접속용 PC 등을 중요단말기로 지정·관리하고 있으나, OO 및 OO 등 OOOOOOO에 OO 접속하는 IT본부 직원의 PC에 대해서는 중요단말기로 지정·관리하지 않고,

중요단말기와 일반 업무용 단말기 OO간 OO OOOO 및 OO OOO 등이 가능한 OO OOOO에서 운영하고 있어 중요단말기가 일반 업무용 단말기를 통해 악성코드에 감염되거나 동 단말기에서 처리된 자료가 유출될 우려가 있으므로

중요단말기 대상을 재검토하여 OO 및 OO 등에 OO OO하는 OOO 등을 중요단말기로 지정하는 한편, OOOO을 OO하여 접근을 통제하는 등 중요단말기 지정·관리 방식을 개선·운영할 필요

(5) 기술지원 종료 OOOO 관리 불합리

일부 정보처리시스템(O대)은 제조사로부터 기술지원이 종료되어 보안패치 및 서비스 업그레이드 등의 지원을 받지 못하는 OOOO(OO)를 사용하고 있어 시스템 오류 및 장애발생 시 신속한 대응이 어렵고, 신규 취약점을 악용한 해킹, 악성코드 감염 등이 발생할 우려가 있으므로

기술지원이 종료된 OOOO를 업그레이드 하거나 제조사와 기술지원 연장 계약을 체결하는 등 OOOO 장애 발생을 미연에 방지하기 위한 구체적인 대응 계획을 마련·운영할 필요