경영유의사항 등 공개안

1. 금융회사명 : 에이비엘생명보험(주)

2. 조치일 : 2019. 7. 17.

3. 조치내용

대상	내 용
기관	경영유의사항 2건, 개선사항 6건

4. 조치대상사실

가. 경영유의사항

(1) 업무지속성 확보를 위한 재해복구계획 강화 필요

회사는 업무지속성 확보를 위해 재해복구계획서를 마련하고 연 1회 재해복구훈련을 실시하고 있으나,

재해복구시스템 처리용량을 평상시 주전산센터 대비 30%용량으로 운영하고 필요시에는 추가자원을 동적으로 할당할 수 있도록 운영하면서 재해복구매뉴얼에 자원 할당방법 및 상세절차를 마련하지 않았고

재해복구센터에 은행, VAN사 및 ○○○○ 등 대외기관 연결용 통신회선을 설치하지 않아 전산센터 장애시 보험금·제지급금 등 대고객 온라인 지급 처리가 불가능하며

본점건물에 재해발생시 본점직원들의 업무복구를 위한 장비 수급계획을 수립하지 않았고, 재해복구계획에 업무환경복구절차를 마련하지 않아 비상시 신속한 업무복구가 곤란할 수 있으며

재해복구센터에 ○○○○시스템을 설치하지 않아 재해복구시스템에 서버관리자가 접속이 불가능함에도 재해복구 훈련시 훈련결과를 정상으로 처리하는 등 비상시 재해복구센터의 정상업무 가동여부 검증이 미흡하므로

재해복구시스템 구축대상을 재검토하여 통신회선 및 ○○○○시스템 등을 확대 구축하고, 재해복구매뉴얼 및 테스트 시나리오를 보완하여 실효성 있는 재해복구계획을 마련하여 훈련을 실시할 필요가 있음

(2) 외부주문 내부통제 강화 필요

회사는 주전산센터(○○○○○센터) 운영을 외부주문업체(IBM)에 위탁(○○명)하여 운영하면서

서버 및 데이터베이스 관리업무를 수행하는 외주직원의 운영시스템 접근 및 작업이력의 적정성에 대해 정기적인 점검을 수행하지 아니하였고

외부주문업체(IBM)가 수행한 자체보안사항 점검 내역에 대해 증빙자료 검토 등을 통한 적정여부를 점검하지 않고 있으며

내규에 따르면 외주직원에게 최고관리자 권한 및 데이터 변경권한 부여를 금지하고 있음에도 해당 업무를 외주업체가 수행하고 있는 등 외부주문 업무수행사항에 대한 내부통제가 소홀하므로

외주직원의 운영시스템 접근 및 작업내역을 주기적으로 점검하고, 외부주문 업무에 대한 보안사항 점검 시 현장점검 및 증빙자료 검토 등을 통해 「IT정보보호규정 규정」 및 「IT운영정보지침」 상의 외주업체 통제 관련사항이 실효성 있게 준수될 수 있도록 내부통제를 강화하시기 바람

나. 개선사항

(1) 프로그램 변경관리 미흡

회사는 프로그램 등록·변경·폐기 절차의 체계적인 관리를 위해 「IT 어플리케이션 표준개발지침」을 마련하여 프로그램 변경요청사항은 요청관리시스템에 등록하고 변경처리내용은 프로그램 변경관리시스템에 기록하여 관리하고 있으나,

「IT 어플리케이션 표준개발지침」에 오류·장애 등에 따른 프로그램 긴급변경 사항에 대해서는 업무처리 절차를 구체적으로 정하지 아니하여 긴급 변경시 프로그램 변경요청 및 처리사항이 체계적으로 관리되지 않을 우려가 있으며

검사대상기간중 프로그램 변경관리시스템에 등재된 총 5,298건의 프로그램 변경작업 중에서 1,200건의 프로그램 변경작업을 IT실에서 자체적으로 시스템을 변경함에 따라 프로그램 변경요청시스템에 작업요청사항이 등재되어 있지 않는 등 일부 미흡사항이 발견되었으므로,

프로그램 긴급변경 관련사항을 규정에 명문화하여 체계적으로 수행하고, 프로그램 변경 관리를 철저히 수행할 수 있도록 IT부서 자체변경건도 관련 시스템에 포함하여 관리하는 등 프로그램 변경관리를 개선하시기 바람

(2) 전산원장 변경 및 내부통제 업무 불합리

(가) 현업부서의 정상적인 업무 수행을 위해 정기적(매월)으로 데이터베이스관리자가 계리시스템 전산원장에 대해 다수의 변경·삭제·삽입 작업을 수행하면서 일괄작업 또는 프로그램 등 통해 수행하지 아니하고, 데이터베이스 조작명령어(SQL)를 직접 입력하는 방식으로 작업하여 오입력 등 작업실수의 우려가 있으므로,

앞으로 정기적으로 계리시스템의 전산원장 수정작업시 일괄작업 또는 프로그램을 통해 작업할 수 있도록 업무절차를 개선하시기 바람

(나) 전산원장 및 회계원장의 오류발생 여부 등을 검증하면서 두 원장간의 변경사항에 대한 일치여부는 월 1회 준법감시담당자가 총액으로만 확인하고 있어,

보험료 수납액, 준비금 정정 등 개별사항 변경으로 전산원장과 회계원장 중 하나의 원장만 변경사항이 반영될 경우 각 원장의 변동내역에 대한 정합성 검증이 미흡할 우려가 있으므로,

준법감시담당자 등 제3자가 보험업무 일일마감시 계리시스템의 전산원장 및 회계원장에 대한 건별 마감대사를 실시하는 등 전산원장에 대한 내부통제를 개선하시기 바람

(3) 데이터베이스관리자 수행업무 통제 미흡

회사는 데이터베이스(DB) 변경작업 시 변경관리시스템을 통해 책임자의 승인을 거쳐 해당 작업을 수행하고 DB접근제어시스템을 이용하여 DB사용자에 대한 접근통제, 마스킹 해제 및 DB사용자 비밀번호 설정 등의 업무를 수행하고 있으나,

데이터베이스관리자(DBA)가 DB관리 뿐만 아니라 DB접근제어시스템도 운영하는 등 데이터베이스 관리 및 통제 업무가 DBA에게 집중되어 있음에도

회사는 DBA의 작업내역에 대한 적정성 여부를 점검하지 않고 있어 DBA가 무단으로 DB를 변경하거나 정보유출 등의 사고가 발생할 우려가 있으므로

데이터베이스관리자의 작업수행 내역에 대한 책임자 승인 및 적정성 검토를 강화하고, 개인정보 조회·산출 내역에 대해 주기적으로 점검하는 등 데이터베이스관리자가 수행한 업무의 통제를 개선하시기 바람

(4) 침입차단시스템(방화벽) 운영관리 미흡

회사는 정보처리시스템 및 정보통신망의 해킹 등 전자적 침해행위를 방지하기 위하여 총 ○○대의 침입차단시스템(방화벽)를 운영하면서

방화벽 ○○대에 적용된 총 □□의 보안규칙(Rule)중 △△개의 규칙은 현재 사용하지 아니하는 규칙임에도 방치하고 있어 불필요한 규칙으로 인한 서비스 노출이 발생할 우려가 있고

사이버청약센터, 홈페이지 등의 보호를 위해 ○○대의 □□□ 방화벽을 운영하면서 □□□ 대역에서 외부로 향하는 접속을 제한 없이 허용하여 해킹공격 발생시 중요정보 유출 등 침해사고의 위험이 있으므로

불필요한 보안규칙은 삭제하고, 보안규칙의 적정성을 정기적으로 점검하는 한편, 업무상 필요한 서비스번호(port) 등에 대해서만 최소한으로 접속을 허용하는 등 방화벽 운영 관리를 개선하시기 바람

(5) 정보처리시스템 접근통제 미흡

(가) 회사는 어플리케이션 통합인증시스템 ○대, 디도스대응장비 ○대, 통신장비 ○○○대 및 VPN장비 ○○○대를 운영하면서

동 시스템 관리자가 어플리케이션 통합인증시스템, 통신장비 및 VPN장비에 접속하여 관리업무 수행시, 각각 암호화되지 않는 통신을 허용하고 있고, 외부 보안관제업체가 ○○○○장비의 보안이벤트 모니터링시에도 암호화되지 않은 통신을 사용하고 있어

해당시스템 접속시 통신구간에서 계정정보 등이 노출될 우려가 있으므로 안전한 암호알고리즘 및 강도의 암호통신 방법을 적용하시기 바람

(나) 서버장비의 경우 접속시 접근제어시스템을 통해서만 접속하고 접근내역을 기록·관리하고 있으나,

통신장비, 지점의 ○○○장비는 접근제어시스템을 적용하고 있지 않아 접근기록이 누락될 수 있으므로 접근통제 및 접근기록관리 강화를 위해 접근제어시스템을 적용하시기 바람

(6) 전산자료 보안통제 미흡

(가) 회사는 대내·외 업무용 이메일로 ○○○○○○社에서 제공하는 ○○○○○를 이용하면서,

주민등록번호 등 개인정보가 포함된 이메일은 외부 발송시 자동차단하고 있으나, 비밀번호가 지정된 압축파일 등이 첨부된 경우에는 차단하지 아니하여 책임자 승인없이 개인정보 등이 외부에 발송될 우려가 있으므로

비밀번호가 지정된 압축파일 등이 첨부된 이메일의 발송을 차단하고, 불가피하게 외부 발송이 필요한 경우 책임자 승인후에 발송하는 등 이메일 발송통제를 개선하시기 바람

(나) PC 및 서버에 저장된 전자문서의 암호화를 위해 문서보안시스템(DRM)을 운영하면서 ○○○○○, ○○○○, ○○○ 및 ○○○ 등으로 저장시 자동으로 암호화하고 있으나,

저장시 자동으로 DRM이 적용되지 않는 다수의 문서편집 프로그램이 PC에 설치되어 있음에도 복호화된 전자문서가 PC 및 파일서버에 존재하는지에 대해서 점검하고 있지 않으므로

DRM이 적용되는 문서편집 프로그램을 확대하거나 업무상 불필요한 문서편집 프로그램을 제거하는 한편, 복호된 전자문서의 존재여부를 정기적으로 점검하여 암호화 조치하는 등 전산자료에 대한 보안통제를 개선하시기 바람