경영유의사항 등 공개

1. 금융기관명 : 한화생명보험㈜

2. 제재조치일 : 2018. 2. 6.

3. 제재조치내용

제재 대상	제재 내용
기 관	• 경영유의사항 2건
	• 개선사항 7건

4. 제재대상사실

가. 경영유의사항

(1) IT조직·운영관리에 대한 적정성 확보 필요

(가) 회사는 정보처리업무를 외부주문에 의하여 처리함에 있어 자체적으로 통제가 가능하도록 회사 내부에 조직과 인력을 갖추고 통제 기준을 마련하여 안전하게 운영할 수 있도록 노력하여야 하는데도,

콜센터 및 인터넷을 통한 보험계약의 조회 등 대고객 서비스를 제공하는 시스템 등 일부 시스템의 운영 및 데이터베이스 관리자 업무를 외부주문업체를 통해 처리하면서

외부주문 업무를 관리하기 위한 내규인 「IT위탁업무 운영관리 지침」에서 각 업무별로 마련한 업무지침에 따라 처리한다고 규정하는 등 외부주문 업무에 대한 구체적인 통제기준이 없어 외부주문에 의한 업무 처리과정 전체에 대한 회사 IT부서의 체계적인 통제기준 수립·운영이 미흡하므로

외부주문 통제를 위한 자체 조직과 인력을 보강하고, 구체적인 통제 기준 등을 마련하여 운영할 필요

(나) 회사는 외부주문업체가 구축한 집적정보통신시설(IDC)에 주전산센터를 구축·운영하면서

정보처리시스템과 직접 연결된 유지·관리용 단말기가 위치한 주전산센터의 사무공간을 다른 회사 시스템의 담당자와 공동으로 사용하고, 주전산센터에 대한 관리업무를 동 외부주문업체에 일임하면서도 적정한 모니터링을 실시하지 않고 있으므로

주전산센터의 유지·관리용 단말기가 위치한 사무공간을 다른 회사와 분리 및 미승인자 출입통제 체계를 갖추고, 주전산센터에 대한 상시 모니터링이 가능하도록 자체 인력이 상주하는 등 주전산센터의 운영관리를 강화할 필요

(2) IT조직·운영관리에 대한 적정성 확보 필요

(가) 회사는 전산센터 장애에 대비하여 업무지속성을 확보할 수 있도록 재해복구센터를 구축·운영하고, 재해복구센터로 실제 전환하는 훈련을 매년 1회 이상 실시하고 있으나,

내규 「재해복구센터 운영메뉴얼」에 따르면 재해복구센터의 계정계 통합서버는 평상시와 재해발생시 정보처리시스템 성능 구성을 달리하도록 하고 있음에도 전환훈련시 정보처리시스템 성능 구성을 설정하는 작업을 누락하여 전환 훈련의 실효성이 낮고,

검사기준일 현재 진행중인 '노후 IT 하드웨어 교체 및 재해복구 확대구축 사업'에서 주전산센터의 노후장비를 충분한 검토 없이 재해복구센터에서 재활용하도록 하는 등 재해복구센터의 기능상 안전성·신뢰성을 담보하기 어려울 수 있으므로

재해복구센터의 안정적 운영을 위해 재해복구훈련계획을 실효성 있게 재정비하고, 재해복구 관련 노후 장비에 대한 안전성 확보 방안을 마련하는 등 재해복구센터 운영을 강화할 필요

(나) 회사는 대고객업무를 처리하는 콜센터시스템을 주전산센터와 재해복구센터에 구축·운영하고 있으나,

재해복구센터에 구축된 콜센터의 경우 녹취시스템 및 상담지원 전용시스템이 누락되어 비상상황시 적정수준의 콜센터 운영이 어려울 가능성이 크므로

장애 발생시 재해복구센터의 콜센터시스템이 안정적으로 서비스를 제공할 수 있도록 녹취시스템 및 상담지원 전용시스템 등 시스템을 확대 구축할 필요

(다) 회사는 통신망 장애시 신속한 복구를 위하여 주요 대외기관 전용회선을 이중화하여 운영하고 있으나,

모든 대외기간 전용회선이 재해복구센터를 경유하여 주전산센터로 연결되어 있어 재해복구센터와 대외기관간 통신망 장애시 주전산센터와 대외기간과의 통신에도 장애 발생이 우려되므로

이중화된 주요 대외기관 전용회선은 주전산센터로 직접 연결하고, 재해복구센터에는 대외기관 전용회선을 별도로 구축할 필요

나. 개선사항

(1) IT부문 감사업무 운영 미흡

(가) 감사편람에서 IT부문 종합감사를 ○년 주기로 실시하고, 부문감사를 연간 ○○회 실시하도록 규정하고 있으나,

감사부서는 검사대상 기간 중 IT부문에 대한 종합감사를 총 1회 계획·실시하고, 부문감사는 매년 1회만 실시하는 등 IT부문 감사 실적이 저조하며

IT전문 감사인력을 IT부문에 투입하지 않고 타부문 감사에 투입하는 등 IT전문 감사인력에 대한 운영이 다소 미흡하므로

감사부서는 감사편람 규정에 따라 IT부문에 대한 종합·부문 감사 계획을 수립하고, IT전문 감사인력을 IT부문 감사에 우선적으로 활용하는 등 IT감사업무의 적정성을 확보할 필요

(나) 회사는 IT부서 내부통제 및 자체감사를 위하여 IT운영팀에 자체감사자를 배치하고 내규 「IT내부감사지침」에 따라 자체감사를 운영하고 있으나,

자체감사자가 IT자체 감사업무 외에 피감업무인 IT감리 업무를 겸직 수행하고, 자체감사 결과에 대한 중간결재와 자체감사자에 대한 인사고과를 피감부서의 파트장이 실시하는 등 자체감사 업무의 독립성이 결여될 우려가 있으므로

IT자체감사자로 지정된 인력의 겸직 업무를 조정하고, 자체감사 결과보고 프로세스 및 인사고과 체계를 개선할 필요

(2) 정보처리시스템 감리 실시 미흡

회사는 정보처리시스템의 안정성 및 효율성 확보를 위하여 내규 「IT감리지침」을 마련하고, 동 지침에 감리대상 사업, 감리유형·시점 및 감리절차 등을 규정하고 있으나,

차세대 구축계획 수립, 계리시스템 개선 및 망분리 등 주요 IT사업에 대하여 감리를 실시하지 않았고, 동 지침에 외부감리 대상에 관한 구체적인 실시기준을 마련하지 않고 있으므로

동 지침에 외부 감리 수행에 관한 구체적인 실시기준을 반영하고, 동 지침에 따른 감리를 누락하는 일이 없도록 개선할 필요

(3) 테스트 데이터 변환·사용 통제절차 불합리

회사는 내규「데이터베이스 보안지침」에 따라 프로그램 개발 과정에서 이용자 정보가 포함된 데이터를 사용하는 경우 데이터를 변환하여 이용하도록 운영하고 있으나,

테스트데이터에 대한 이용신청(목적·사용자·기간) 및 폐기절차 등에 대한 관리 정책을 운영하지 아니하고, 이용신청이 없음에도 테스트데이터를 정기적으로 변환하는 등 테스트데이터 사용에 대한 통제관리가 미흡하므로

테스트데이터에 대하여 이용목적·기간·범위 등을 신청하여 사용하고, 이용기간이 경과한 테스트데이터는 즉시 삭제하는 등 관리체계를 개선할 필요

(4) 데이터베이스 변경 통제 프로세스 불합리

회사는 데이터베이스 변경 처리시 IT업무 담당자가 DB변경 명령어(SQL)를 작성하면 데이터베이스 관리자가 DB변경결재를 신청하여 상급자 결재 후 처리하고 있으나,

DBA가 명령어를 수동으로 입력할 수 있어 오입력 등 작업실수의 우려가 있고, 상급자의 결재과정에서 DBA가 입력한 명령어의 이상 여부 등 적정성 확인이 어려우므로

DBA가 처리하는 DB변경 명령어가 데이터 변경 처리과정에서 무결성이 유지될 수 있도록 관련 시스템을 개선할 필요

(5) 일괄작업 결과 파일 관리 미흡

회사는 일괄작업 결과 파일에 대한 접근권한을 직원의 담당업무에 따라 부여하는 등의 방법으로 통제하고 있으나,

일괄작업 결과파일의 주기적인 삭제 등 관리가 이루어지지 않아 불필요하게 파일이 장기간 저장되고, 개인정보가 포함된 일부 결과파일에 대해서는 암호화되지 않은 채 관리되고 있어

일괄작업 결과 파일에 대한 보유 필요성에 따른 정기적인 삭제 및 개인정보 포함시 암호화 적용 등 일괄작업 결과 파일에 대한 체계적인 관리를 수행할 필요

(6) ○○○○○○○ 시스템 접근통제 불합리

회사는 ○○○○○ 가 보험계약 등 중요정보를 조회·관리할 수 있는 ○○○○○○○○ 시스템을 인터넷망을 통해 접속하도록 운영하는데도,

PC 및 태블릿PC를 통해 동 시스템 접속시 아이디 및 패스워드를 통한 단일 사용자 인증체계만 운영하고 있어 사용자의 아이디 및 패스워드를 확보한 비인가자도 접속할 수 있으므로

사전에 지정된 단말기에 한하여 접속 허용하거나, 이중인증방식 도입 등을 통해 ○○○○○ ○○ 시스템의 접근통제를 강화할 필요

(7) 비업무 인터넷사이트 접근 통제 미흡

회사는 업무와 무관한 인터넷사이트에 대한 접속차단 및 정보 유출 방지 등을 위해 내규 「네트워크 운영관리 지침」에 비업무 인터넷사이트를 차단하도록 하고 있고 비업무 인터넷사이트 통제 시스템을 운영하여 통제하고 있으나,

인터넷 접속용 단말기에서 일부 웹하드 및 메일 사이트의 접속이 차단되지 않아 정보유출 및 악성코드 감염의 우려가 있으므로

접속이 차단되지 않는 일부 웹하드 및 메일 사이트를 차단할 수 있도록 관련 기능을 개선하고 비업무 인터넷사이트 차단이 누락되지 않도록 주기적으로 모니터링 하는 등 통제를 강화할 필요