경영유의사항 등 공개안

1. 금융기관명 : DGB캐피탈(주)

2. 조치일 : 2019. 11. 15.

3. 조치내용

대상	내용
기 관	개선사항 10건

4. 조치대상사실

가. 개선사항

(1) IT감사 업무 불합리

① 검사팀은 내규 「감사 직무규정」에 따라 감사 계획을 수립하고, IT부문에 대한 종합감사 및 특별감사, 임원 전결사항에 대한 일상감사를 실시하도록 규정하고 있으나,

검사대상기간 중 IT부문 일상감사 대상에 해당되는 2017년 IT부문 사업계획 및 2018년 IT부문 사업계획 등에 대해 일상감사를 실시하지 않은 사례가 확인되므로

일상감사 사항에 대해서는 「감사 직무규정」 및 「일상감사지침」을 준수하도록 임직원에게 안내하고, 일상감사 대상인 경우 결재선에 검사팀을 포함하여 일상감사가 누락되는 사례가 발생하지 않도록 운영할 필요

② 내규 「감사규정」에 의하면 경영, 업무, 재무, 준법, IT 분야에 공통적으로 적용되는 검사계획 및 실시, 검사결과 보고 및 조치, 검사결과 조치기준 및 방법, 검사결과 사후관리 등의 내용을 명시하고 있으나,

「감사규정」에 IT감사 범위 등에 대한 기준을 마련하지 않았고, IT감사역의 책임과 역할, 업무절차 등을 포함한 매뉴얼 등을 마련하지 않고 있으므로

IT부문 감사 수행주기, 감사범위 등을 내규에 반영하고, IT감사역의 책임과 역할, 업무절차 등을 포함하는 IT감사 매뉴얼 등을 마련하여 일관된 IT감사를 운영할 필요

(2) IT감사 사후관리 불합리

① 내규 「검사규정」에 의하면 '검사결과 지적사항정리보고서' 제출 시 미정리 사항에 대해 미정리 사유와 정리대책을 구체적으로 기술하도록 되어 있고, 미정리 사항이 있을 경우 정리될 때까지 매분기 검사팀에 이행현황을 보고하도록 되어 있으나,

2015년 IT부문 감사 지적사항에 대한 검사결과지적사항정리보고서에 미정리로 보고한 이후 정리가 완료될 때까지 분기별로 이행현황을 보고하지 않았고, 2017년 IT부문 감사 지적사항 중 'OOOO OO OO OO OO'과 관련하여 정리보고시 미정리로 보고하였으나, 완료보고 전까지 이행현황을 분기별로 보고하지 않는 사례가 발생하고 있으므로

검사결과 지적사항에 대한 조치기한을 준수하도록 임직원에게 안내하고, '검사결과 지적사항정리보고서'는 OOOO로 관리하는 한편, 미정리 사항에 대해서는 해당부서에서 매분기 이행현황을 보고하는 방안을 마련하는 등 IT검사 사후 관리업무를 개선하여 운영할 필요

② 내규 「검사규정」 제OO조(지적사항 정리 및 보고)에 권고사항의 경우 검사서가 상반기에 발송된 경우 당해연도 9월 15일까지, 하반기에 발송된 경우 익년도 3월 15일까지 정리하도록 규정하고 있으나,

검사서 발송날짜에 따라 정리기간이 최대 8.5개월, 최소 2.5개월로 상이하게 운영되고 있어 정리기간의 형평성에 대한 문제가 발생하므로

지적사항에 대한 정리 또는 조치기간이 합리적으로 적용될 수 있도록 「검사규정」을 개정하여 운영할 필요

(3) 비상계획 관리 불합리

① 업무지속성 확보를 위해 자체적으로 시스템별 전산자료, 운영체제, 프로그램 등을 백업하고, 중요자료를 소산 보관하고 있으며, 비상대책으로 위기대응매뉴얼을 2018. 2월에 마련하고 있으나,

정보처리시스템 사용 불능시 대체장비 확보방안이 마련되어 있지 않고, 유관기관 연락처가 유선 전화번호 위주로 관리되고 있어 업무시간 종료 후 비상사태가 발생할 경우 연락이 두절될 가능성이 있으므로

정보처리시스템 사용 불능시 대체장비를 확보할 수 있는 방안을 위기대응매뉴얼에 반영하고, 유관기관 담당자의 연락처를 현행화하는 등 비상대응체계를 개선하여 운영할 필요

② 2017년~2018년 기간 중 실시한 재해복구 훈련은 IT 및 현업부서 직원이 함께 참여하고 있으나,

OOO 시스템 장애를 가정한 비상상황에서 OOO 데이터베이스 백업자료를 활용하여 데이터를 복구하고 복구된 데이터의 물리적 정합성만 확인하는 수준으로 진행하여 다양한 비상상황에 대비한 대응체계가 미흡하므로

네트워크 회선 장애, 하드웨어 고장, 전력공급 중단 등 다양한 비상상황을 고려하여 훈련의 실효성을 확보할 수 있도록 관련 절차를 개선하여 운영할 필요

(4) 서버 성능 모니터링 · 관리 불합리

① 서버에 대한 장애 예방 및 성능 관리를 위하여 성능관리솔루션을 도입하고 CPU, 메모리 및 응답시간 등 시스템의 상태를 실시간 모니터링하고 있으나,

실시간 모니터링을 주전산시스템 OOOOOO서버만 포함하고 OOO시스템 및 OOOOOO 서버 등에 대해서는 성능 모니터링 대상에 포함하지 않고 있어, 전체적인 서버 성능에 대한 이상 징후를 인지하지 못해 사전 예방조치를 적시에 시행하지 못할 우려가 있으므로

OOO시스템 및 OOOOOO 서버 등 연계 서버를 성능 모니터링 대상에 포함하는 등 서버 성능관리를 개선하여 운영할 필요

② 주요 서버에 대한 디스크 용량 등 서버 하드웨어 장치의 운영 상태를 매일 점검하여 관리하고 있으나,

서버를 최적화된 상태로 운영하기 위한 기간별 사용량 추이 분석 결과 등을 체계적으로 관리하지 아니하여 용량 확보가 필요한 시점을 적시에 판단하기 어려울 우려가 있으므로

주요 서버에 대한 기간별 사용량 분석 등을 정기적으로 실시하여 시스템 용량 증설이 적시에 이루어지도록 서버 성능 모니터링 · 관리를 개선하여 운영할 필요

(5) 전산자료 백업·소산관리 불합리

내규「전산규정」제O장 백업 및 복구관리에 따라 주요 전산자료, 프로그램, 환경설정파일 등을 정기적으로 백업하고 원격지에 소산하고 있으나,

OOO 시스템 및 OOO 시스템의 경우 정기 백업대상에 포함하지 않았고, OOO OO 데이터는 소산 대상에서 제외하고 있어 장애·재해 발생 시 데이터 복구에 문제가 발생할 우려가 있으므로

백업정책에 누락된 OOO 시스템 및 OOO 시스템에 대해 주기적으로 백업을 실시하고, OOO 시스템의 OO파일은 소산 대상에 포함하는 등 전산자료 백업·소산관리를 개선하여 운영할 필요

(6) IT사업 추진 시 감리 활동 불합리

내규「정보시스템 감리지침」에 감리 실시기준, 감리 실시시기, 감리 절차 및 방법 등 정보시스템 감리 운용절차를 규정하고 있으나,

동 내규에는 감리법인을 통한 외부감리 수행절차 이외의 회사 내부직원이 수행 가능한 구체적인 내부감리 수행절차를 마련하지 않아 내부감리 수행시 시스템 구축 단계별로 확인하여야 할 점검항목을 시스템 구축이 완료된 이후인 안정화 기간에 점검·확인하여 감리 수행의 실효성을 확보하기 어렵고,

내부감리에서 발견된 미흡사항에 대한 보완조치 이행여부를 확인할 수 있는 'OOOO OOOOO'를 작성·관리하지 않는 등 내부감리 수행 관리가 미흡하므로

내부감리에 대한 수행절차 및 방법 등을 내규에 반영하고 내부감리 수행 시 시스템 구축 단계별로 감리를 실시하며, 감리 수행 결과 미흡사항에 대한 보완조치 이행여부를 확인하여 기록·관리하는 등 감리 활동 체계를 개선하여 운영할 필요

(7) 정보보안 모니터링 불합리

① 정보보안 모니터링을 위하여 OOOOOO시스템에 보안관제 업무를 위탁하여 OOO인터넷망과 OOO인터넷망을 24시간 365일 상시 모니터링을 하고 있고, 내부망 PC 및 중요단말기의 악성코드 감염방지를 위해 백신프로그램을 설치·운영하고 있으나,

백신관리서버를 통한 단말기 내 백신프로그램 정상 동작 여부, 패턴 업데이트 여부 등의 운영현황 모니터링 및 악성코드 감염이력 등에 대한 중앙관리가 미흡하므로

정보보호 모니터링이 누락되고 있는 내부망 단말기에 설치된 백신프로그램에 대해 OOOOOO시스템에 보안관제를 추가로 위탁 처리하는 등 보안관제 절차를 개선하여 운영할 필요

② OOO, OOO 및 OOOO 서버에는 서버용 백신프로그램을 설치·운영하고 있으나,

동 백신프로그램 정상작동, 악성코드 감염여부 확인 등을 수행하는 관리서버가 없이 운영하고 있어, 보안운영자가 수동으로 패턴 업데이트 및 백신 정상 동작여부, 악성코드 감염이력을 확인해야 하는 등 악성코드 감염사고 발생 시 이에 대한 즉각적인 대응에 어려움이 예상되므로

서버에 단독 설치된 백신프로그램을 통합관리하기 위한 관리 서버를 마련하고, 백신프로그램 동작 여부, 악성코드 탐지 여부, 패턴 업데이트 여부 등에 대해 통합 관리가 가능하도록 설정하고, 악성코드 탐지시 자동으로 관리자에게 알림을 주는 등 자체적인 보안 관제 절차를 개선할 필요

③ 전자금융거래 등 대고객 서비스를 제공하고 있는 홈페이지의 경우 OOOOOO 시스템에서 정보보호시스템의 운영 및 모니터링을 수행하고 있으나,

OOOOOO시스템은 홈페이지 정보보안 모니터링 내역에 대한 보고를 누락하고 있어 홈페이지에 대한 외부 공격 등 사고 영향을 적시에 인지하여 대응하기 어려우므로

OOO인터넷망에 대한 보안관제 이력을 보고받아 점검하는 등 자체적인 정보보안 모니터링 관리를 개선하여 운영할 필요

(8) 정보보호 내규 관리 불합리

① 내규 「정보보안규정」 제OO조제O항 및 「정보보안업무지침」 제OO조 및 제OO조에 따르면 전자금융사고 발생시 금융감독원에 사고 보고, OOOO 유출 시 고객에 알림, 침해사고 대응훈련 실시와 관련된 내용 등을 규정하고 있으나,

침해사고 발생 시 각 담당자의 역할 정의, 침해사고의 예방 및 탐지 업무 절차, 침해사고 발생 이후의 후속조치 방안, 재발방지 대책 등 정보보호 침해사고 발생에 따른 효과적인 대응 절차가 내규에 마련되어 있지 않으므로

내규에 침해사고 발생시 담당자의 역할 정의, 침해사고의 예방 및 탐지 업무 절차, 침해사고 발생 시 후속 조치, 재발방지 대책 마련 등의 침해사고 대응 절차를 마련하는 등 관련 내규를 보완하여 운영할 필요

② 내규 「정보보안규정」 제OO조제O항 및 「정보보안업무지침」 제OO조제O항에 따르면 신규 전자금융업무 수행 및 전자금융거래 표준 제정 시 자체 보안성 심의를 실시하도록 하고, 정보처리시스템 업무 담당자가 정보처리시스템의 통합, 전환 및 재개발시 수립하는 변경계획에 업무 흐름 및 보안대책 등을 문서화하여 자체보안성 심의를 의뢰하도록 규정하고 있으나,

신규 전자금융업무 수행 이외의 인증절차 추가·삭제·변경 등 보안상 중요한 변경이 있는 경우에도 자체보안성심의를 진행해야 한다는 내용 및 자체 보안성심의 진행 이후 금융감독원에 보고해야 한다는 내용이 내규에 누락되어 있으므로

전자금융거래의 인증절차 추가·삭제·변경 등 보안에 중요한 영향을 미치는 사항에 대해서도 자체 보안성심의를 진행하도록 하고, 자체 보안성심의 결과를 금융감독원에 보고하도록 관련 내규를 보완하여 운영할 필요

③ 내규 「정보보안업무지침」을 마련하여 외부주문에 대한 관리적·물리적·기술적 보안관리 사항을 명시하고, 외부주문 계약업체, 외부 개발자를 관리하는 부서장 및 계약담당자, 외부 개발자에 대한 책임을 명시하고 있으나,

외부주문 등의 입찰·계약·수행·완료 등 각 단계별로 따라야 하는 보안관리방안에 대한 사항 및 외주 인력에 대한 정기적인 현장점검 실시, 금융거래정보를 위탁 취급하는 외부주문에 대한 금융감독원 보고 등 법규에 명시된 내용이 누락되어 있으므로

외부주문에 대한 입찰·계약·수행·완료 등 각 단계별로 따라야 하는 보안관리방안에 대한 사항, 외주 인력에 대한 정기적인 현장점검 실시 및 금융거래정보를 위탁 취급하는 외부주문에 대한 금융감독원 보고 등 관련 법규 준수사항을 추가하도록 관련 내규를 보완하여 운영할 필요

(9) 정보유출 방지대책 불합리

사용자 단말기에 저장된 중요 전산자료의 외부 유출을 방지하기 위하여 데이터유출 방지솔루션을 구축·적용하여 이동식저장매체 등 비인가 매체의 단말기 접속을 차단하고, 내부망 PC에서 파일을 이동식 저장매체에 저장하여 외부에 반출하는 경우 이동식저장매체 사용에 대해 책임자 사전 승인을 받고 있으나

저장매체에 저장된 파일에 대한 OOOO 포함 여부가 기록되지 않고, 대량의 OOOO가 저장되는 경우 책임자 승인 등 추가적인 통제를 실시하지 않는 등 OOOO 유출방지 통제가 미흡하므로

내부망 PC에서 OOOO가 포함된 자료를 이동식 저장매체를 통해 외부로 반출하는 경우 반출된 파일에 OOOO 포함여부를 기록으로 남기고, OOOO 유출 차단기준을 마련하여 기준을 초과한 OOOO를 유출하는 경우 이에 대한 승인을 받는 등 OOOO 유출방지 대책을 개선하여 운영할 필요

(10) 외주직원 보안 점검 및 전산장비 반·출입 통제 불합리

외주직원의 경우 노트북 및 PC 등의 자산 반·출입시 「자산반출입 관리대장」을 기입하고, 중요 점검사항에 대한「외부주문 일일 점검표」를 작성하며, 프로젝트 종료 시 「OOOOOO OOO」 및 「OOO OOO OO OOO」를 기록하여 전산장비 내 자료 삭제에 대한 증빙을 기록·관리하고 있으나,

보안 중요사항에 대한 「외부주문 일일 점검표」 작성 시 외주직원 당사자의 자필 서명 이외에 해당업무 책임자(PM) 및 소속 팀장의 결재가 없고, 외주직원에 대한 운영업무의 적정성 및 보안 준수여부에 대해 주기적인 현장점검을 실시하지 않고 있으며,

「자산반출입 관리대장」에 제품 일련번호 등을 기재하지 않아 반출되는 장비에 대해 반입장비와의 일치 여부를 확인하기 어렵고, 「OOOOOO OOO」 및 「OOO OOO OO OOO」를 확인한 결과 외주직원이 반·출입한 장비에 대해 디스크 포맷과 관련한 일부 점검사항의 기재가 누락되어 있어 외주직원 철수 시 내부 자료에 대한 삭제 여부를 보증하기 어려우므로

「외부주문 일일 점검표」는 외주직원 당사자의 자필서명과 해당업무 책임자(PM) 및 소속 팀장의 결재를 받고, 외주직원에 대한 주기적인 현장점검을 실시하는 한편,

「자산반출입 관리대장」에 전산장비 반·출입 시 제품 일련번호 등을 기재하고, 전산장비 포맷 확인 등을 명확하게 확인할 수 있는 증빙을 마련하는 등 외부직원 보안점검 및 전산장비 반·출입 관리 업무를 개선하여 운영할 필요