제재내용 공개안

1. 금융회사명 : ㈜한국씨티은행

2. 제재조치일 : 2020. 7. 21.

3. 제재조치내용

제재대상	제재내용
기관	- 경영유의사항 10건 - 개선사항 12건

※ 경영유의 및 개선사항은 금융회사의 주의 또는 자율적 개선을 요구하는 행정지도적 성격의 조치임

4. 제재대상사실

가. 경영유의사항

(1) 이사회에 경영계획 보고 미흡 등

① 이사회에 경영계획 보고 미흡

은행은 국내회계기준에 따른 연간 경영계획을 이사회의 승인을 거쳐 수립한 후 분기별로 경영계획 대비 실적을 점검하여 이사회에 보고하고 있으며, 씨티그룹 본사에 보고하는 미국회계기준에 따른 경영계획 및 실적은 경영진이 참석하는 경영위원회 및 임원회의에서 매월 점검하고 있으나

2018년 상반기중 씨티그룹의 수익배분 방식 변경 등으로 미국회계기준에 따른 경영계획상 수익목표가 xx백만달러 상향 조정되었음에도 이를 이사회에 보고하지 않은 사실이 있으므로

앞으로 미국회계기준에 따른 경영계획상 중요한 변경이 발생하는 경우 이사회에 보고하여 국내회계기준에 따른 경영계획 변경에 반영할지 여부 등을 논의할 필요가 있음

② 경영위원회 및 임원회의 운영 불철저

내규 「경영위원회규정」 및 「임원회의규정」에 따르면 경영위원회 및 임원회의는 은행의 경영에 관한 사항을 심의하는 기구이나

은행장이 한국에 소재한 씨티그룹 계열사를 대표*한다는 이유로 경영위원회 및 임원회의에서 관계회사인 씨티그룹글로벌마켓증권㈜의 경영계획 및 경영실적을 포함하여 관리하고 있으므로

* 은행장은 씨티 한국 대표자(Citi Country Officer)로서 한국에 소재한 계열사 간 의사소통 및 상호 협력을 위한 조정위원회(CCC, Country Coordination Committee)의 의장을 맡고 있음

앞으로 경영위원회 및 임원회의에서는 씨티그룹글로벌마켓증권㈜의 경영계획 및 경영실적을 제외하고 은행의 경영에 관한 사항만을 심의하도록 할 필요가 있음

(2) 대주주 등과의 이해상충 행위에 대한 감독 강화

「금융회사의 지배구조에 관한 법률」 제15조에 의하면 이사회는 대주주·임원 등과 회사 간의 이해상충 행위 감독에 관한 사항을 심의·의결하여야 하는데도

은행은 대주주·임원 등과 회사 간의 이해상충 행위 감독과 관련한 이사회의 심의·의결 범위를 명확하게 정하지 아니하여 연도별로 심의·의결 범위를 상이하게 운영한 사실이 있으므로

앞으로 대주주·임원 등과 회사 간의 이해상충 행위 감독에 관한 범위를 명확하게 규정하는 등 이해상충 행위 감독 체계를 적정하게 구축·운영할 필요가 있음

(3) 업무문서의 한글화 필요

「은행업감독업무시행세칙」 제98조에 따르면 은행은 은행의 업무와 관련된 서류 및 내규 등 제반 문서를 원칙적으로 한글로 표기하여야 하며 한글요약표 등으로 대체하는 경우에도 감독·검사업무에 지장을 초래하지 않도록 하여야 하는데도

은행은 실무위원회의 의안자료 및 의사록뿐만 아니라 여신심사보고서, 임직원 성과평가자료 등 다수의 업무자료를 영어로만 작성·보관하고 있으므로

앞으로 은행에서 영어 등 외국어로 생산하는 문서에 대하여 한글을 병행하여 표기하거나 한글요약표를 첨부하는 등 감독·검사업무에 지장을 초래하지 않도록 유의할 필요가 있음

(4) xx부의 본부부서 검사업무 강화

내규「조직규정」및「감사본부장직무규정」등에 따르면 xx부는 각 부점에 대한 일반검사 업무를 담당하도록 되어 있고, 일반검사는 재무·준법·업무·경영 등 기능별로 검사를 실시하는 종합검사와 특정부문에 대한 부문검사로 구분되어 있으나

xx부는 본부부서에 대해서는 부문검사만을 수행하고 종합검사는 씨티그룹 감사부(IA : Internal Audit)의 검사로 대체*하고 있어 은행의 자체적인 검사 기능이 저하될 우려가 있으므로

* 검사부는 본부부서에 대해서 2017년에는 결산 검사, 내부자본적정성 검사 등 감독규정에 근거한 검사만 수행하였으며 2018년에는 장기간(3년) 검사를 받지 않은 본부부서에 대한 감사계획을 마련하였으나 대주주 검사가 결정됨에 따라 검사 미실시

대주주(씨티그룹) 검사와 별도로 xx부가 자체적으로 감사계획을 수립·이행하는 등 본부부서에 대한 검사 기능을 강화할 필요가 있음

(5) 계열사와의 채권·채무 정산 불철저

은행은 고객과의 파생상품, 수출입금융 거래 등에서 발생하는 영업수익을 씨티그룹 계열사 간에 상호 정산하는 수익배분 모델에 2016.1월부터 참여하고 있으나

동 수익배분 모델을 통해 은행과 계열사 간의 채권과 채무를 정산하는 방식과 정산주기를 정하지 않아 계열사 관련 채권 및 채무*가 최장 x년 x개월간 정산되지 못하는 문제점이 있었으므로

* 2018년말 기준 순채권은 xx백만달러 수준(채권 xx백만달러, 채무 xx백만달러)

앞으로 계열사와의 채권·채무가 장기간 미정산되지 않도록 관련 채권·채무를 주기적으로 정산하는 등 업무 처리에 유의하시기 바람

(6) 효율적 차세대시스템 구축을 위한 대책 강화 필요

2022년 가동을 목표로 차세대추진TF 조직을 구성하여 차세대시스템 구축 프로젝트(1단계) 사업을 추진하고 있으나

차세대시스템 구축 프로젝트에 대한 타당성 검토 및 비용 대비 효과분석 결과 등을 전산운영위원회에 이메일 등으로만 보고하고 전자결재시스템(스마트씨티)에는 공식적으로 등록하고 있지 않아 업무실효성이 저하될 소지가 있고

차세대시스템 구축을 위한 별도 계약 없이 기존 수탁사(Citi Group)와 맺고 있는 계약(ICSA*-주계약 및 ADR**-세부계약)만으로 차세대시스템 구축 사업을 추진하고 있어 사업추진 결과물에 대한 귀속관계 및 이행 시 사고·장애에 대비한 비상대응계획 등을 처리하기 미흡하므로

* ICSA(Intra Citi Service Agreement) : 씨티그룹 계열사간 업무위수탁 계약서
** ADR(Additional Documentation Requirements) : 위탁대상 서비스에 대한 상세 업무 기술서

차세대시스템 구축사업 추진 시, 프로젝트 운영위원회(Steering Committee) 회의록 등 사업추진 관련 중요자료 등을 전자결재시스템(스마트씨티)에 등록·관리하는 등 품질관리 활동을 합리적으로 추진하는 한편

사업 추진 결과물에 대한 귀속관계 및 비상사태에 대비할 수 있도록 계약관계를 명확히 하는 등 차세대시스템 구축을 위한 대책을 강화하시기 바람

(7) IT자체감사업무 독립성 강화

은행 IT업무는 전산본부와 고객보호본부가 분장하여 각각 수행하고 있고 전산본부는 자체감사자를 지정하여 본부 수행업무에 대한 자체감사를 실시토록 하고 있는데

xx본부는 위험통제팀장(Risk & Control Head) 및 xx부장(Technology Planning & Control Head)이 자체감사자에 대한 보고통제 및 업무성과 평가를 하고 있고 xx본부는 자체감사자를 지정·운영하고 있지 않아 IT보안업무 등에 대한 자체감사체계가 미흡하므로

xx본부 및 xx본부 자체감사자에 대해서는 보고통제 및 업무성과평가를 xx본부장(CIO) 및 xxx본부장(CISO)이 직접 수행하고, IT업무에 대한 자체감사가 누락되지 않도록 xx본부는 자체감사자를 지정·운영하는 등 자체감사체계를 강화할 필요가 있음

(8) 외화 유동성커버리지비율 모니터링 관리 미흡

「은행업감독업무시행세칙」<별표 3-6> 58. 및 76.에 의하면 은행은 외화 유동성커버리지비율(LCR)을 산정하여 관리하여야 하는데도

2017~2018년 중 일별 외화 유동성커버리지비율(LCR)이 「은행업감독규정」상 경영지도비율을 93회 하회(전체 영업일수의 19%)하고 하회된 상태가 조치 미흡 등으로 최장 7일까지 지속되는 사례가 발생하는 등 외화 유동성 지표 관리에 미흡한 점이 있었으며

2017~2018년 중 중요 통화인 미국달러(USD) 기준 월별 유동성커버리지비율이 2017년 4·6·7월을 제외하고는 모두 경영지도비율을 하회하는 등 중요 통화별 유동성 관리가 제대로 이루어지지 않은 사실이 있으므로

앞으로 외화 유동성커버리지비율 등 외화 유동성리스크에 대한 관리·통제를 강화하시기 바람

(9) 리스크관리위원회 운영 미흡

① 리스크관리 조직에 대한 업무분장 개선 필요

리스크관리위원회는 위험관리를 전담하는 조직의 구조 및 업무 분장 등을 포함하는 위험관리기준을 마련하여야 하나

위험가중자산 산출 업무에 대한 담당부서가 내규화되어 있지 않고 xx부가 장외파생상품 등에 대한 위험가중자산을 산출하고 있으므로

앞으로는 리스크관리 업무 분장을 내규에 명확히 반영하는 한편 익스포져의 생성에 책임이 있는 부서로부터 독립되고 리스크관리 업무에 전문성이 있는 부서가 리스크관리 업무를 담당토록 할 필요가 있음

② 리스크관리위원회 역할 강화

리스크관리위원회는 은행의 리스크관리에 대한 최종적인 의사결정기구임에도 리스크관리 조직 구조 및 업무분장, BIS자기자본비율 관리에 관한 사항 등 리스크관리와 관련된 주요 사항이 동 위원회에서 논의되지 않은 사례*가 있으므로

* 위험가중자산 산출기준 변경(2018.3월), 장외파생상품 상계(2018.9월) 및 조기청산(2018.12월), 시장리스크팀을 리스크기획부에 통합하는 조직개편(2018.9월) 등

앞으로는 리스크관리와 관련된 주요 사항이 리스크관리위원회에서 빠짐없이 논의될 수 있도록 관련 절차를 보완할 필요가 있음

(10) 비트레이딩 거래 분리 강화

「은행업감독업무시행세칙」<별표 3-2> 3.에 의하면 은행은 시장리스크 산출 대상 포지션(트레이딩 포지션)을 별도의 부서에서 관리하여야 하고 조직구조상 트레이딩과 비트레이딩 부서를 완전히 분리하기 어려운 경우에는 최소한 데스크나 딜러에 의한 분리는 이루어져야 하며

내규 「트레이딩정책규정」 제11조 등에서도 xx부 내에 트레이딩과 비트레이딩 거래 담당딜러를 나누어 운영하게 되어 있는데도

2016.12.17.~2018.12.31. 기간중 비트레이딩 포지션 담당자가 트레이딩 계정을 운영(파생상품거래 xx조원)하거나 트레이딩 포지션 담당자가 비트레이딩 계정을 운영(채권 xx조원)하는 사례가 발생하는 등 트레이딩과 비트레이딩 포지션 구분관리에 미흡한 점이 있으므로 관련 조직 개편이나 인력 조정 등을 통해 명확한 구분 관리가 이루어질 수 있도록 운영을 강화하시기 바람

나. 개선사항

(1) 대손충당금 관련 리스크 측정요소 추정 방법 불합리

2018.1월부터 한국채택국제회계기준(K-IFRS) 제1109호가 시행됨에 따라 대손충당금 적립 기준이 발생손실 모형에서 기대신용손실 모형으로 변경되었으므로 리스크 측정요소(PD·LGD·CCF)도 변경된 기준에 따라 합리적이고 일관성 있게 추정하여야 하나

기업여신의 경우 씨티그룹의 추정치를 그대로 적용하고 가계여신의 경우 관대한 가정*으로 추정하는 등 리스크 측정요소 추정의 근거가 미흡하여 대손충당금이 부정확하게 산출될 우려가 있으므로

* (예) 세그먼트 간 추정기간 상이, 선형함수를 이용한 Lifetime PD 과소추정, 담보와 무관하게 상품별로 LGD 추정, 장기간 회수관찰기간 설정으로 LGD 과소추정 등

앞으로는 리스크 측정요소의 추정 방법을 변경된 대손충당금 적립 기준에 맞게 합리적으로 개선하고 이를 충실히 문서화하시기 바람

(2) 위기상황 분석시 독립적인 적합성 검증 불합리

「은행업감독규정」 제30조 제5항, 「은행업감독업무시행세칙」 제29조의3 등에 따르면 은행은 위기상황분석이 적정하게 수행되고 있음을 확인하기 위하여 독립적이면서 전문성을 갖춘 별도의 부서에서 위기상황 분석에 대한 적합성 검증을 최소 연 1회 이상 실시하여야 하나

은행은 통합 위기상황분석의 경우 독립적인 적합성 검증 조직이 아닌 위기상황 분석 실시 부서의 직원으로 구성된 임시조직에서 적합성 검증을 실시하고 있으며 유동성 위기상황분석의 경우 명시적이고 체계적인 적합성 검증이 수행되지 않고 있으므로

앞으로는 위기상황분석에 대한 독립적인 적합성 검증 조직을 마련·운영하는 한편 위기상황분석 검증 범위 및 방법론, 리스크관리위원회 보고 기준·절차 등을 내규에 반영하여 운영하시기 바람

(3) 배당가능이익 산정 업무 불합리

「상법시행령」 개정(2014.2월)에 따라 파생상품 거래의 미실현손익 상계 등 배당가능이익 산정방식이 변경되었으므로 은행은 이를 반영하여 합리적이고 일관성 있는 배당가능이익 산정 절차를 마련·운영하여야 하는데도

xxxx년도 결산배당시 당기순이익 대비 배당규모가 작다는 이유로 배당가능이익을 미산정하고 xxxx년도 중간배당시에는 별도의 원칙 없이 배당가능이익을 변경하여 이사회에 수정 보고하는 등 문제점이 있었으므로

앞으로 은행의 배당가능이익이 「상법」에 부합하게 산정될 수 있도록 배당가능이익 산정·보고·검증 등에 대한 내부통제 기준*을 마련·정비하는 등 업무절차를 개선하시기 바람

* ① 「상법」상 배당가능이익 산정시 파생상품 거래의 미실현손익 상계 기준·방식 (예: 위험회피 회계 거래, 백투백 거래(100%) 등 위험회피 효과 입증이 명확한 거래에 한하여 미실현손익 상계), ② 미실현손익 상계 대상 파생상품 거래의 위험회피 효과(연계성) 관련 입증 방식 등 포함

(4) 여신협의회 의사록 작성·관리 불합리

내규 「한국씨티은행리스크관리정책및절차에관한세칙」 제4절에 따르면 은행은 여신협의회 개최 일시·장소·참석자·회의 내용 등을 기재한 의사록을 작성하여야 하나

작성자에 따라 회의 내용에 대한 기술 방식이 상이하고 참석자별 발언 내용이 명확히 기재되지 않고 있으므로

앞으로는 여신협의회 의사록 작성 시 각 안건별 회의 내용이 통일된 방식으로 작성되고 발언 내용 등 주요 사항이 충실히 기재될 수 있도록 관련 절차를 개선하시기 바람

(5) 임직원 변동성과급 불합리

① 성과평가지표 및 보상기준의 수립시점 변경 필요

보수위원회가 임원 및 금융투자업무 담당자에 대한 성과평가지표 및 보상기준을 2017.6.2. 및 2018.5.29.에 의결함에 따라 연초부터 약 5개월간 성과평가지표 및 보상기준이 없는 문제점이 있으므로

앞으로는 임원 및 금융투자업무 담당자에 대한 성과평가지표 및 보상기준을 매년도 1분기 내에 확정하여 운영하시기 바람

② 성과급 지급 체계 불합리

은행은 임원 및 금융투자업무 담당 직원에 대한 성과급 지급 체계를 운영하고 있으나

금융투자업무 담당 직원의 경우 종합점수 수준별로 성과급지급률 범위*를 폭넓게 정하고 있어 은행장이 보수위원회에 성과급지급률을 제안하는 과정에서 종합점수와 무관하게 성과급 규모가 정해지는 사례가 발생하고 있으며

* (예) 금융투자업무 담당 직원의 성과급지급률 범위 - 기본급의 0%(하한)~XXX%(상한)
⇒ 종합점수가 낮은 직원에게 종합점수가 높은 직원 대비 높은 성과급 지급 가능

임원의 경우 은행장의 제안에 따라 전체 임원의 약 XX%*에 대해 사전에 설정한 성과급지급률 범위를 초과하는 성과급을 예외적으로 지급하는 등 문제점이 나타나고 있으므로

* 2017년도의 경우 임원 총 XX명 중 X명, 2018년도는 임원 총 XX명 중 X명에 대해 사전에 설정한 성과급지급률 범위를 초과하여 성과급 지급

앞으로는 금융투자업무 담당 직원의 종합점수 수준별 성과급지급률 범위를 축소하는 한편 불가피한 경우가 아니라면 임원에 대한 성과급 지급과 관련한 예외사항을 인정하지 않는 등 성과급 지급 체계의 투명성 및 합리성을 제고하시기 바람

③ 금융투자업무 담당자의 성과급 지급 범위 불합리

은행은 외환파생상품 영업담당부서는 부장(2급 등) 이상을, 트레이딩부서는 부부장(3급 등) 이상을 보수위원회 심의·의결 대상에 포함하고 있으나

xx부서 부부장의 경우 개인성과급이 기본급의 xxx%에 달하며 금번 검사에서 거래한도를 초과하여 외환파생상품을 취급하는 사례가 다수 적발되는 등 개인 성과급을 위해 과도한 위험을 추구할 우려가 있으므로

xx부서의 경우 부부장도 보수위원회의 심의·의결 대상에 포함되도록 내규에 반영하시기 바람

④ 금융투자업무 담당자의 성과지표 불합리

은행은 금융투자업무 담당자의 성과지표로 리스크를 전혀 감안하지 않은 지표*를 사용하고 있으므로 앞으로는 리스크를 반영한 성과지표를 사용하도록 개선하시기 바라며

* 목표 대비 개인 수익 공헌, 전년 대비 개인 수익 성장도, 목표 대비 팀 수익 공헌도

xx 부서장의 경우 목표 대비 팀 수익 공헌도가 전부 100점으로 산정되고 있어 변별력이 없으므로 본부 목표 대비 부서 수익 공헌도 비율을 사용하는 등 변별력을 확보하시기 바람

⑤ 성과급 유보기준 불합리

내규「성과보상운영규정」제7조 및 씨티그룹의 보상지침*에 따르면 은행이 임직원에 대하여 직무배제를 하거나 규제기관 등이 임직원의 위규 행위를 조사하는 경우에는 이연보상을 유보하여야 하는데도

* CAP(Capital Accumulation Program) 및 DCAP(Deferred Cash Award Plan)

은행이 자체적으로 임직원을 직무배제하는 경우에만 성과급을 유보하고 있고 규제기관 등이 조사하는 경우에는 구체적인 기준이 없어 이연보상을 유보한 사례가 없으므로

앞으로는 규제기관의 조치내용 사전통지 등으로 일정 수준 이상의 징계가 예상되는 경우에는 해당 임직원에게 부여된 이연보상을 유보할 수 있도록 세부 기준을 마련하시기 바람

⑥ 성과급 감액기준 불합리

내규「성과보상운영규정」제9조에 따르면 임원 및 금융투자업무 담당자가 면직처분을 받는 경우 모든 미확정 이연보상이 취소되도록 하고 있으나 면직을 제외한 징계에 관한 기준은 마련되어 있지 않아 불합리하므로

앞으로는 면직 외의 중징계 처분에 대한 성과급 감액기준을 마련·운영하시기 바람

⑦ xx부서 소속 직원에 대한 변동성과급제도 불합리

은행은 본점직원*을 대상으로 씨티그룹의 변동성과급제도(DIRA)**를 운영하고 있으나 은행장이 xx본부 및 씨티그룹 xx부 소속 임직원의 성과급까지 정하고 있어 검사 업무의 독립성을 침해할 우려가 있으므로

* 지급대상(모수)은 ①xx그룹 소속 전직원, ②xx부서는 부장급 이상 전직원과 부부장이하의 일부직원(선택적), ③전문직계약직원 전원이며 실제 지급대상은 2017년은 XXX명, 2018년은 XXX명이었음

** DIRA : Discretionary Incentive and Retention Awards

앞으로는 xx부서 소속 직원에 대해서는 감사위원회가 변동성과급을 정하도록 개선하시기 바람

(6) 전자메일 보관 정보처리의 업무위탁 관리 미흡

「금융기관의업무위탁등에관한규정」 제3조의2 및 [별표 3]에 의하면 금융회사가 업무위수탁을 추진하는 경우에는 감독당국의 자료접근권을 보장하여야 하며 은행은 전자메일 보관 정보처리의 업무위탁(2015.8월)*시 감독기관 등의 요구가 있을 경우 신속하게 전자메일을 제공하도록 계약한 바 있는데도

* 은행은 2015.8월 씨티그룹 테크놀로지와 전자메일 보관 정보처리 업무위탁을 계약하고 그 내용을 금융감독원에 사후보고(2015.10.5.)

금융감독원이 전자메일을 요구한 날로부터 9영업일* 후에 전자메일을 제공한 사실이 있으므로

* 정보처리 업무위탁 보고에 의하면 5영업일 내에 제공하도록 되어 있음

앞으로는 업무위탁한 정보처리 절차가 원활하게 이루어질 수 있도록 관련 부서 간 업무 분장 및 정보제공 절차 등을 명확히 마련·운영하시기 바람

(7) IT위탁업무에 대한 감사활동 미흡

xx부는 xx그룹 및 xx그룹이 수행하는 IT업무에 대해 감사활동을 수행하고 있으나

xx본부 및 xx본부가 직접 수행하지 않고 씨티은행 그룹사(Global) 또는 씨티은행 지역본부(Region) 등 외부에 위탁하여 수행 중인 업무에 대해서는 감사를 실시하고 있지 않고 있으므로

xx본부 및 xx본부가 그룹사(Global) 또는 씨티은행 지역본부(Region) 등 외부에 위탁·수행하고 있는 업무 중 IT리스크가 높은 업무를 선별하여 감사를 실시하는 등 IT부문에 대한 감사활동을 개선하시기 바람

(8) IT사업 추진관리 불합리

내규「공급업체 선정 및 계약체결 방법서」에 따라 IT사업 추진 시 계약관련 업무를 수행하고 있으나

검사대상 기간 중 외주용역 및 컨설팅 사업(xxx건) 중 전년도에 예산을 미리 확보하지 않고 추진한 사업*이 xx%(xx건)로 사업관리가 일부 미흡하게 수행된 사례가 있으며

* 개인대출심사시스템의 인터넷/모바일 신용대출 등

통합유지보수 계약 시, 한국마이크로시스템과는 작업주문서에 용역비(xx억원)와 개발비(xx억원)를 구분하여 명시하고 있으나, KCC의 작업주문서에는 용역비(xx억원)만 명시하고 개발비 한도를 정하지 아니하여 이를 근거로 별도 수의계약(x건)을 체결하고 있으므로

IT사업 추진 시, 요구사항 관리 등을 철저히 수행하여 예산 미확보사업이 무분별하게 추진되지 않도록 하는 한편, 통합유지보수 업체의 수행업무 범위를 계약과정에서 명확하게 마련하는 등 IT사업 추진 관련 절차 등을 개선하시기 바람

(9) 전산자료 소산 및 복구대책 미흡

비상상황 시 정보시스템의 연속성 확보 및 신속한 장애복구 등을 위하여 백업자료를 주전산센터(인천시 소재)에 일단위로 백업하고 있으나

주전산센터와 소산장소가 동일하여 전산센터의 지진, 화재 등 대규모 재해에 대비하기에는 미흡하고

검사대상 기간 중 소산자료를 활용한 복구훈련은 실시하지 않아 소산자료에 대한 정합성이 검증되지 않았으며

소산자료의 저장매체별 보관자료의 세부목록(업무명, 파일명 등) 및 복구방법(서버 환경, 파일시스템 생성 및 복구 매뉴얼 등)을 보관하고 있지 않아 재해발생 시 자료복구에 차질이 발생할 우려가 있으므로

전산센터의 지진, 화재 등 재해로 인하여 데이터 및 프로그램의 사용이 불가능할 경우에도 복구가 가능하도록 소산자료를 전산센터로부터 원격지에 위치한 장소의 내화금고에 보관토록 개선하고

소산자료 및 저장자료의 세부목록, 복구방법 등이 포함된 복구매뉴얼 등을 원격 소산센터의 내화금고에 보관하고, 정기적으로 소산자료를 활용한 복구훈련을 실시하는 등 소산 및 복구대책을 개선하시기 바람

(10) 암호화키 관리 통제대책 불합리

내규「암호화키 관리 방법서」를 수립하여 암호화키의 생성·주입·운용·폐기와 관련된 사항을 정하고, 암호화키 원본은 봉인하여 금고에 별도 보관토록 정하고 있으나

검사착수일 현재(2019.5.7.) 암호화키의 세부명세서(Inventory)를 수기로 관리함에 따라, 암호화키 명세서(xxx개)와 실제 시스템상의 암호화키(xxx개) 및 금고에 보관된 원본 암호화키 등이 상호 일치하지 않고 있으므로

실제 시스템상의 암호화키와 암호화키 세부명세서(Inventory)를 주기적으로 대사하여 관리하는 등 암호화키 관리통제 절차 및 시스템 등을 개선하시기 바람

(11) 정보보호시스템 원격관리 통제절차 불합리

정보처리시스템 및 정보통신망의 해킹 등 전자적 침해행위를 방지하기 위하여 침입차단시스템(방화벽) 및 침입탐지시스템(IDS) 등 정보보호시스템을 설치·운영하고 있으나,

은행에서 운영 중인 방화벽(xx대) 및 로그관리 분석서버(xx대)의 경우 그룹사(Citi Group)의 일관된 보안정책을 적용하기 위하여 그룹사 담당조직의 원격접속*을 과다하게 허용(xxx명)하고 있으며,

* 그룹사 담당자가 전용회선을 사용하여 원격으로 정보보호시스템에 접속하여 관리

동 정보보호시스템을 관리하는 그룹사 담당조직의 단말기 및 통신망이 국외(싱가포르 등)에 위치하고 있어 보안통제 등이 미흡할 우려*가 있으므로,

* 씨티은행은 정보보호시스템 관리를 위해 단말기 외부반출, 인터넷 접속 및 그룹웨어 차단 등 강화된 보호대책이 적용된 중요단말기를 통해 관리 중

정보보호시스템에 대한 그룹사 담당조직의 원격관리를 최소화하고, 그룹사 담당조직이 은행에서 직접 운영하는 중요단말기를 통해서만 정보보호시스템에 접속토록 하는 등 정보보호시스템 공동 관리 절차 및 통제방법 등을 개선하시기 바람

(12) 기술지원 종료 운영체제 사용에 따른 보정작업 불합리

전산장비에 대하여 유지보수 업체를 통해 정기점검을 실시하고 있으며 필요시 보정작업 등을 실시하고 있으나

제조사의 기술지원이 종료된 운영체제를 사용하는 일부 서버(xx대*)의 경우, 보안 취약점에 대한 보정작업이 이루어지지 않을 우려가 있으므로

* AIX 6.1(2017.4.30. 지원종료) xx대 사용 중(운영 xx대, 재해복구 xx대, 테스트 xx대)

기술지원이 종료된 운영체제에 대한 업그레이드 계획을 조속히 마련하여 이행하는 등 관련 정보처리시스템에 대한 보정작업을 개선하시기 바람