경영유의사항 등 공개안

1. 금융기관명 : 하나캐피탈㈜

2. 제재조치일 : 2023. 5. 18.

3. 제재조치내용

제재대상	제재내용
기 관	경영유의 7건, 개선 20건

4. 조치대상사실

가. 경영유의사항

(1) 이사회 내 소위원회 운영의 부적정

내규「임원후보추천위원회 규정」제6조 제3항에 따르면 위원회 결의에 관하여 본인이 후보로 추천되는 등 위원회의 결의에 관하여 특별한 이해관계가 있는 자는 의결권을 행사하지 못하며, 당해 위원은 재적위원의 의결권의 수에 산입하지 아니하도록 규정하고 있음에도 불구하고, 회사는 2021.3.5. 임원추천위원회에서 甲 후보로 현 甲을 추천하면서 이해관계자인 甲의 의결권을 포함하여 의결하였으며,

내규「평가보상위원회 규정」제4조 및 제7조에 의하면 평가보상위원회는 매년 보상체계에 대한 정기적인 연차보상평가를 경영진으로부터 독립적으로 실시하여야 하고, 위원회의 결의에 관해 특별한 이해관계가 있는 자는 의결권을 행사하지 못하며 당해 위원은 재적위원의 의결권의 수에 산입하지 아니하도록 규정하고 있음에도 불구하고, 경영진인 甲이 위원으로서 연차보상평가에 참여하고 甲 본인을 포함한 임원의 보수를 결정하는데 의결권을 행사하는 등 불합리하게 운영되고 있으므로

앞으로 임원후보추천위원회 및 평가보상위원회가 관련규정에 따라 적정하게 운영될 수 있도록 의결권 행사 등에 유의하시기 바람

<관련규정>
1. 내규 「임원후보추천위원회 규정」제6조 제3항
2. 내규 「평가보상위원회 규정」제4조 및 제7조

(2) 사업추진 시 타당성 검토 강화

내규 「ICT 전략위원회 운영세칙」에 따라 정보처리시스템 및 전자금융거래와 관련된 사업의 타당성 검토 및 비용대비 효과분석, 1억원 이상의 IT관련 시스템 도입 및 구축 사업 건별 타당성 검토 등을 위해 ICT전략위원회를 구성·운영하며 매년 IT사업예산을 심의·의결하고 있으나,

사업추진부서가 예산을 과다책정*하거나 IT부서의 시스템 자체 구축, 사업 이월 등의 사유로 예산이 집행되지 않는 사례**가 빈번함에도 ICT전략위원회의 IT사업예산 심의시 미추진·착수지연 사업 및 잔여예산에 대한 원인분석 없이 예산편성을 승인하고 있고

* 2019년 3건, 2020년 2건, 2021년 3건의 계획사업은 사업종료 후 예산집행률이 60% 미만
** 2019년 계획사업 27개 중 7개, 2020년 계획사업 30개 중 7개, 2021년 계획사업 36개 중 15개

2021년 IT예산심의를 위한 ICT전략위원회 시(2020.11.20.) 사업별 추진현황관리, 미집행 예산에 대한 원인분석 필요성이 제기되었으나 이에 대한 별도의 대책을 마련하지 않는 등 예산 수립·집행이 부실하게 관리되고 있으므로

사업 계획 수립시 당해 연도 미추진 사업에 대해서는 관련 부서가 원인 분석 후 ICT전략위원회에 보고토록하며 ICT전략위원회에서는 익년도 사업계획 심의시 사업 추진의 당위성, 사업일정 등을 포함하여 심의하도록 하는 절차를 마련하는 등 사업예산 수립과 관련된 타당성 검토를 강화할 필요가 있음

(3) 부동산 PF 대출 리스크관리 강화

2022.9월말 현재 PF대출 잔액은 ☆억원이며, 일반브릿지론과 건축 관련 시설자금 대출*을 포함한 익스포져는 ☆억원으로 부동산 시장 침체가 현실화된 상황 등을 감안하여 아래와 같이 리스크 관리를 강화할 필요가 있음

* 준공 이후 시설물 대상 담보대출로 상환 예정이거나 차주사가 임차 등 운영 예정으로, PF와 준공리스크 측면에서 성격이 유사

① 부동산 PF 대출 사업성 평가기준 미흡

여신금융협회의 「여신금융회사의 부동산PF 리스크관리 모범규준」 제9조 제2항, 제3항 및 <별표1>에 의하면 여신전문금융회사는 부동산 PF 대출 사업장별 사업성을 평가하고 이를 반영하여 부동산 PF 대출 관련 자산에 대한 건전성을 분류하여야 함에도,

내규 「PF대출업무 취급 세칙」에 부동산 PF 대출의 사업성 평가 및 건전성 분류를 위한 세부적인 기준 등이 미흡*하게 규정되어 있고, 사업성 평가의 근거 내용 대부분이 여신승인 당시 검토된 내용 수준에 불과하여 평가 시점의 사업성을 제대로 반영하지 못하고 있으므로

* 사업성 평가 및 건전성 분류에 대한 세부기준 마련 없이 「여신금융회사의 부동산PF 리스크관리 모범규준」과 동일한 수준

토지매입, 인허가, 만기 연장, 분양률, 착공 여부, 공사중단 여부, 준공 여부, 공정률, 연체 여부 등을 반영한 세부 기준을 마련하여 운영하는 등 사업성 평가 기준을 합리적으로 개선하는 방안을 마련하시기 바람

<관련규정>
1. 여신금융협회 「여신금융회사의 부동산PF 리스크관리 모범규준」 제9조 및 <별표1>
2. 내규 「PF대출업무 취급 세칙」

② 일반 브릿지론 리스크관리 강화

분양 경기 침체가 본격화되어 기존 PF 사업장의 분양률이 저조한 상황에서 분양물량 적체에 대한 부담으로, PF 브릿지 사업장뿐만 아니라 일반 브릿지* 사업장의 사업진행 역시 어려워지고 있는 상황**이나,

* 2022.9월말 기준 일반 브릿지론은 총 ☆건(☆억원) 수준임

** 만기 연장(예정 포함) : ☆건, 건축인허가 지연 : ☆건

PF 브릿지론은 본PF대출과 동일하게 여신금융협회의 「여신금융회사의 부동산PF 리스크관리 모범규준」 제9조 및 <별표1>에 의하여 사업장별 사업성을 평가하고 이를 반영하여 부동산 PF 대출 관련 자산에 대한 건전성을 분류하고 있는 반면, 일반브릿지론에 대해서는 위와 같이 사업성 평가 및 건전성 분류를 실시하고 있지 않으므로

일반 브릿지론에 대해서도 PF 브릿지론과 동일한 절차에 따라 사업성 평가를 하는 등 리스크관리를 강화하시기 바람

③ 건축 관련 시설자금대출에 대한 리스크관리 강화

회사는 건축 관련 시설자금대출(☆건, ☆억원)의 경우 대출금 상환 재원이 분양수익금이 아니라 완공된 건물 등에 대한 담보대출 등이라는 이유로 PF로 분류하고 있지 아니하여 사업성 평가 및 건전성 분류를 실시하고 있지 않으나

※ PF대출은 여신금융협회의「여신금융회사의 부동산PF 리스크관리 모범규준」제9조 및 <별표1>에 의하여 사업성을 평가하고 부동산 PF 대출 관련 자산에 대한 건전성을 분류하고 있음

동 대출은 본 PF와 준공 리스크 측면에서 동일한 위험을 보유하고 있는 한편, 공사비 상승 등에 따른 건설사 준공 리스크가 현재화된 상황*이므로,

* 2022.9월말 기준 예정 공정율 대비 실제 공정율 차이가 10% 이상인 사업장은 ☆개(☆억원)이고, 30% 이상인 사업장은 ☆개(☆억원)

건축 관련 시설자금대출에 대해 본 PF의 준공리스크 관련 사업성 평가 기준 등을 준용하여 리스크 관리를 강화하시기 바람

(4) 개인신용대출 대손충당금 관련 미래지향승수 조정 유의

내규「리스크관리 시행세칙」제44조에 따라 리스크관리위원회의 결의를 받아 2021년부터 집합평가 부도율(Probability of Default, 'PD')에 코로나19장기화, 경제성장률 등 미래경기전망을 반영한 미래지향승수를 적용하여 대손충당금을 산정하는 과정에서,

경제성장률의 하락 및 물가상승 등 스테그플레이션 상황 및 지속적인 통화긴축 정책으로 경기 전망이 악화되고 있고, 회사의 가계신용대출 1개월 이상 연체비율이 상승 중이며, 1개월 이상 연체액 대비 대손충당금 비율도 ☆%로 캐피탈사 평균**(☆%)대비 낮은 수치를 보이고 있음에도,

** 2022.6월말 기준 가계신용대출 잔액이 1천억원 이상인 14개 非카드사

2022년 미래경기전망을 예측하여 미래지향승수를 조정하는 과정에서 하나금융경영연구소에서 제시한 시나리오별 부도율 추정결과를 자체적인 합리적 조정절차 없이 단순 적용함에 따라 2021년 대비 긍정적인 예측 조정계수*를 사용하여 대손충당금 산정을 위한 부도율(PD)이 낮아지는 등 변경 기준이 불합리하므로

* 하나금융연구소는 2022년 코로나 종식을 예상하고 2021년 대비 긍정적으로 경기 전망하였으나, 2021년 1차 승수 ☆(최종승수 ☆), 2022년 1차 승수 ☆(최종승수 ☆)로 최종승수는 낮아짐

하나금융경제연구소의 거시경제 전망 등을 참고로 하여 자체적으로 합리적인 미래지향승수를 산출한 후 대손충당금 적립에 반영할 필요가 있음

<관련규정>

1. 내규「리스크관리시행세칙」제44조(대손충당금 적립기준)

(5) 개인사업자담보대출 리스크관리 강화

① 「개인사업자대출 여신심사 가이드라인」 제13조 및 제16조에 따라 회사는 개인사업자대출 포트폴리오 관리업종(이하 '관리업종')을 선정하여 업종별 대출 현황을 모니터링하고, 한도 근접 시에는 원인을 파악하여 해당 업종에 대한 여신취급기준을 강화하는 등 적절한 조치를 취해야 함에도

관리업종(부동산업, 도소매업, 숙박 및 음식점업) 여신의 한도 초과가 예상됨에도 적절한 조치를 취하지 않고, 한도 초과 발생 후 사후적으로 한도를 증액시키는 등 관리업종 한도 관리가 미흡*하므로

* 2022.8.25. 리스크관리위원회에서 관리업종 한도 설정 기준을 변경함

앞으로 해당 업종의 대출 취급 추이, 전망, 리스크 수준 및 여신 집중도 등을 종합적으로 분석한 후 준수 가능한 범위 내에서 한도를 설정하고 관리할 필요가 있음

② 「개인사업자대출 여신심사 가이드라인」 제17조에 따라 1억원 초과 신규 개인사업자 대출 취급시 소득대비대출비율(이하 'LTI')을 산출하여 여신심사 시 활용하고, LTI 구간별로 대출 추이 및 건전성 등을 모니터링하여야 하는데도,

2021.9월*부터 검사착수일(2022.11.7.) 현재 고비율의 LTI 대출 건이 다수 존재함에도 LTI를 심사지표로 활용하고 있지 않으며, LTI 관련 모니터링 업무도 수행하지 않고 있으므로

* 2021.9월부터 개인사업자 담보대출을 취급하기 시작

앞으로는 LTI를 여신심사 및 모니터링 등에 활용할 수 있도록 내부 심사 지침을 마련할 필요가 있음

(6) 기업대출 관련 관리 철저

① 2022.9월말 현재 회사의 총자산 15.5조원 중 기업대출(☆조원)이 차지하는 비중이 높은 편(☆%)임에도 기업 대출을 심사 및 사후 관리하는 인력이 부족*하고, 급격한 자산 성장에 걸맞는 전산시스템을 구축하고 상시 유지 보수하여야 함에도 각 영업부서가 귀속자산을 자체 관리하는 등 관리가 소홀**하므로

* 22.9월말 현재 자체 심사인력 ☆명(팀장 ☆명, 계약직 ☆명)

** 기업대출 계정과목이 세분화되어 있지 않아 상세항목의 데이터 추출이 불가하여 금융감독원 검사 시 요청 자료 작성을 수작업에 의존

정해진 일정이 아닌 시기에 이자 및 대출이 실행될 경우 기존 스케줄과 일정이 다르게

생성되어 채권별 수작업이 필요

담보대출의 경우, 담보등록을 시스템에 하지 않았음에도 대출이 실행

기업 대출 심사에 대한 전담 인력을 확충하고, 지원·관리 전담부서를 설치하는 등 관련 전산시스템을 대폭 정비할 필요

② 부동산 경기 침체가 가시화되는 상황에서 부동산 관련 업종 대출에 편중*되어 있어 부실의 현재화 우려가 있으므로, 부동산 관련 업종에 대출이 집중되지 않도록 관리할 필요가 있음

* 2022.9월말 기준 : PF익스포저 ☆조원(PF ☆조원, 시설대출 등 ☆조원) 등 부동산 관련 여신성자산이 총 ☆조원으로 기업 대출(☆조원)의 ☆% 수준

(7) 유동성리스크 관리체계 운영 강화

① 경영진의 유동성리스크 관리절차 미흡

내규「유동성리스크 관리 세칙」제6조 제4항에 따라 경영진은 자금조달비용의 급격한 상승 등 유동성에 중대한 문제가 발생하거나 발생할 것으로 예상되는 경우 즉시 이사회 등에 보고하여야 하나,

자금 및 리스크 담당 임원이 참여하는 회의체 등이 마련되어 있지 않아 내규를 이행하기 위한 구체적인 업무절차가 운영되고 있지 않으므로, 향후 경영진이 유동성리스크를 효율적으로 관리할 수 있도록 유동성리스크 관리 절차를 마련하시기 바람

② 비상대책위원회 운영의 합리성 제고

내규「리스크관리 시행세칙」제68조 제2호 및 제73조에 따라 회사에 발생할 수 있는 위기상황에 대한 조치사항을 마련하기 위해 리스크관리담당임원 및 자금담당부서장 등을 비상대책위원으로 선정하여 비상대책위원회를 운영하고 있으나,

회사채 실행 등에 대한 의사결정 권한이 있는 자금담당임원이 비상대책위원에 해당하지 않아 비상대책위원회가 마련한 위기상황대책이 적시에 실행되지 않을 우려가 있으므로

유동성리스크 관리를 위한 위기상황대책 마련 시 자금담당임원이 비상대책위원으로 참여할 수 있도록 비상대책위원회 운영절차를 개선하시기 바람

< 관련규정 >

1. 내규「유동성리스크 관리 세칙」제6조 제4항
2. 내규「리스크관리 시행세칙」제68조 제2호 및 제73조 제1항, 제2항
3. 내규「직무 전결 규정」<별표1>

나. 개선사항

(1) 자산건전성 분류 업무 개선

「여신전문금융업감독규정」제9조 제5항 및 별표1 자산건전성 분류기준에 따르면 3년연속 결손발생 및 완전 자본잠식 차주에 대한 여신은 자산건전성 분류시 '요주의'로 분류하여야 하고 시가법 및 지분법 평가대상이 아닌 유가증권은 원칙적으로 매월 1회 자산건전성을 분류하여야 함에도

전산시스템을 이용하여 전체 자산에 대해 일괄적으로 자산건전성 분류를 실시하면서 3년연속 결손발생 및 완전 자본잠식 차주를 '정상'으로 분류하고 일부 유가증권에 대한 분류를 누락하는 등 자산건전성 분류 업무를 미흡하게 운영하였으므로,

앞으로「여신전문금융업감독규정」에 맞게 자산건전성 분류가 이루어질 수 있도록 관련 내규를 개정하고 자산건전성 분류 전산시스템을 변경하는 등 관련 업무를 개선하시기 바람

< 관련규정 >

1.「여신전문금융업감독규정」제9조 제5항
2. 내규「리스크관리시행세칙」제45조 제2항 및 별표 3-2

(2) 자동차리스 중도해지비용 산정체계 개선

회사는 2019.10.14. 자동차리스 약관 개정에 따라 관련 내규「업무기준」을 함께 개정하면서 운용리스 중도해지시 고객에게 부과하는 중도해지손해배상금의 산정방식을 리스 잔여기간에 따라 안분하여 차등 인하하는 방식으로 변경*하였으나

* 중도해지손해배상금 = (변경전) (미경과리스료+추정잔가) × 40%
→ (변경후) 미회수원금 ×{80% ×(잔여기간월수/리스기간 전체월수)}

중도해지손해배상금률이 잔여기간에 따라 종전의 40%에서 최고 80%*까지 인상됨에 따라 평균요율이 크게 상승(3.1%p↑)하고 조기 중도해지 고객의 부담이 과도하게 증가** 하는 등 부적정하게 운영되고 있으므로

* 2019.9.23. 85%로 인상하였다가 2021.9.27.부터 80%로 인하

** (사례) 리스차량의 원금(비용 포함) 1억원, 계약기간 60개월인 경우 12개월 경과 후 반납 시 중도해지비용이 종전 최고 46백만원에서 변경 후 최고 58백만원으로 증가

자동차리스 약관 개선 취지를 감안하여 최고요율을 합리적으로 산출하는 등 리스 이용자의 권익 보호를 강화하는 방향으로 중도해지비용 산정체계를 개선하시기 바람

<관련규정>
1. 내규 자동차 운용리스 약정서

(3) 금리인하요구권 운영 기준 개선

회사는 「금리인하요구권 업무매뉴얼」의 '상품별 금리인하 수용기준'상 신용도(개인신용평점) 상승 등에 따른 금리인하 대상 및 인하 폭 등을 결정하고 있으나, 개인대출 등의 금리인하 수용을 위한 최소 신용평점 상승 요구기준 및 인하구간 폭이 높게 설정* 되어 있고, 2022년 3분기 개인차주에 대해 금리 인하를 수용한 57건을 점검한 결과 일부 오류(3건**)가 발견되었는 바,

* ex) 소비자신용대출의 경우 대출당시 NICE평점 ☆점 이상시; 평점 ☆점이상 상승 시 ☆%p, ☆점 이상 상승시 ☆%p & 대출당시 NICE평점 ☆이상 ☆점이하시; 평점 ☆점 이상 상승시 ☆%p, ☆점 이상 상승시 ☆%p 등

** 1건 : 2022.9월말 기준 금리 인하 과소적용(10월 시정)
2건 : 금리인하 대상이 아님에도 고객의 민원성 요구에 따라 금리 인하

개인신용평점에 따른 금리인하 수용기준을 합리적으로 조정 및 보완하고, 금리인하 프로세스 및 결과에 대한 자체 점검을 강화할 필요가 있음

(4) 대출모집인의 다단계 모집행위 점검 절차 마련

내규 「모집인운영세칙」 제11조에 따르면 불법·부당대출 모집행위가 발생하지 않도록 모집인에 대해 관리·감독을 철저히 하여야 함에도,

회사는 다단계 대출 모집 행위를 점검하기 위한 기준 및 절차 등을 마련해놓고 있지 않으므로, 이를 점검하기 위한 세부적인 점검 기준 및 절차를 마련하는 등 관련 내부통제를 강화할 필요가 있음

<관련규정>

1. 내규「모집인운영세칙」제11조

(5) IT계약 업무 운영 미흡

내규「IT자원 도입운영 세칙」및「계약 규정」에서 수의계약방식으로 진행할 수 있는 불가피한 경우를 규정하고 있으며 수의계약을 체결하는 경우 품의문에 수의계약 사유에 해당하는 조항을 명확히 표시하도록 하고 있으나,

2019년~2022년 중 체결된 정보시스템 구축 및 도입 계약 184건 중 수의계약으로 체결된 61건(33.2%)의 계약은 품의문에 수의계약 사유에 해당하는 조항을 명시하지 않고 계약을 체결하거나 수의계약의 타당성을 객관적으로 입증할 검토 내역 없이 계약을 체결하는 등 수의계약 업무 운영이 미흡하므로,

수의계약시 수의계약 사유에 대한 증빙내역을 품의문서에 첨부하고 일상감사시 해당내역을 확인하는 등 절차를 마련하여 수의계약의 타당성을 제고하시기 바람

< 관련규정 >

1. 내규「IT자원 도입운영 세칙」제7조 제2항
2. 내규「계약 규정」제9조 제4항

(6) IT감사 사후관리 미흡

① 내규「감사규정」에 따라 피감사부서장 또는 관련부서장이 감사결과 통보된 지적사항에 대하여 필요한 조치를 취하여야 하며, 그 결과를 정해진 기일 내에 감사총괄에게 보고하고 감사인은 조치결과보고서를 검토한 결과 그 이행 내용이 적정하지 않다고 판단되거나 정당한 사유 없이 그 조치를 이행하지 않은 경우에는 별도의 조치를 취할 수 있으나,

감사인은 2021년 IT 정기 감사 지적사항 13건 중 3건*에 대하여 해당부서가 제출한 조치이행계획만으로 완결 처리하고 이행결과를 관리하지 않아 실제 해당부서는 지적사항을 조치이행 계획대로 이행하지 않았으며,

* IT 기획담당 인력 부재, 프로그램 소스 취약점 점검 미흡, 프로그램 변경 내용 기록관리 미비(2022.4.13. 조치완료 보고)

감사실의 감사인력 8명 중 IT업무를 수행하거나 IT 관련 자격증을 보유한 감사인력이 없어 외부 전문기관이 수행*한 2021년 IT 정기 감사 지적사항에 대한 해당 부서의 이행결과 적정성을 판단하기 어려워, 실제 미조치된 8건(조치이행계획만 제출한 3건 포함)을 조치완료된 것으로 판단하는 등 감사실의 감사 사후관리수행이 미흡하므로,

* 회사는 내규「감사규정」에 따라 "2021년 IT 정기 감사" 수행을 A에 의뢰

미정리 사항에 대해서는 해당부서에서 매분기 이행현황을 보고하도록 하는 절차를 마련하여 매뉴얼에 반영하고 감사부서 내 IT전문 감사인력을 보강하는 등 IT감사 사후관리업무를 강화하시기 바람

② 내규「IT자체감사 운영 세칙」에 따라 IT 자체감사에서 지적된 사항에 대해 피감사 부서 또는 해당 업무담당자가 시정조치계획을 수립하고 시정조치계획에는 위반의 근본원인을 제거할 수 있는 조치사항과 이행 일정이 포함되어야 하나,

IT자체감사인의 시정조치계획 수립 요구 및 해당 부서의 이행 계획에 대한 회신이 공문 행위 없이 이루어져 2019년~2022년 중 수행한 자체감사 지적사항 48건에 대한 시정조치 요구 및 조치계획 확인이 불가하며 IT자체감사인은 자체감사 지적사항에 대한 조치계획 수행내역을 입증할 문서를 관리하고 있지 않는 등 IT자체감사의 사후관리가 미흡하므로,

IT자체감사인의 감사 결과에 대한 내용을 공문행위를 통해 관리하고 장기적으로 감사 지적 사항을 사후관리 하는 시스템을 개발하여 감사기능 강화 및 감사 효율성을 제고하시기 바람

< 관련규정 >

1. 내규「감사규정」제5장 제19조
2. 내규「IT자체감사 운영 세칙」제13조 제1항 내지 제3항

(7) IT부서 자체감사 업무 및 운영 미흡

① 내규「IT자체감사 운영 세칙」에 따라 IT자체감사 계획을 수립하고, 정기감사를 연 1회 이상 실시하여야 하며 IT경영, IT운영, IT개발, 정보보호 등을 IT자체감사의 점검사항으로 지정하고 있으나,

2019년~2022년 기간 중 IT자체감사는 연간 감사계획을 수립하지 않았으며 정기감사의 경우 IT부서 자체감사의 범위를 정보보호부분에 국한하여 수행하였으므로

향후 IT자체감사 계획 수립을 누락하지 않고 정보보호 부문 외의 업무(IT경영, IT운영, IT개발)를 정기 감사대상에 포함하여 IT전반에 대해 감사를 수행하시기 바람

② 내규「IT경영관리 세칙」에 따라 IT인력의 자질향상을 위하여 직무특성을 고려한 IT교육 계획을 수립하여 운영하고 있으나,

IT자체감사가 근무기간(2019.4.7.～현재) 동안 법정의무교육 외에 IT자체감사의 역량을 키우기 위한 교육프로그램에 참여한 이력이 없어 IT자체감사 역량 부족이 우려되므로

정기적인 정보보호 교육 및 외부 감사 관련 교육 수강을 통해 IT자체감사인의 역량을 강화하시기 바람

③ 내규「IT자체감사 운영 세칙」에 따라 IT자체감사 부서는 IT자체감사를 객관적으로 수행하기 위하여 감사대상 영역에 해당되는 업무를 수행하지 않도록 직무를 분리하고 정보기술 총괄 임원이 정보기술 및 정보보호 업무와 독립된 IT자체감사 부서를 지정하고 운영하도록 하는 등 피감사부서로부터 독립적으로 운영하는 것을 원칙으로 하고 있으나,

검사착수일(2022.11.21.) 현재 자체감사자의 업무성과 평가절차에 감사대상 업무를 수행하는 ICT운영팀장이 포함되어 있어 IT자체감사업무의 독립성이 우려되므로

IT자체감사인의 독립성을 유지하기 위해 ICT본부장이 IT자체감사인의 업무평가를 수행하도록 평가절차를 개선하시기 바람

< 관련규정 >
1. 내규「IT자체감사 운영 세칙」제5조 제1항 제1호, 제8조 제1호
2. 내규「IT경영관리 세칙」제9조 제2항

(8) IT아웃소싱 서비스 관리 소홀

회사는 2016년 이후 B와 IT아웃소싱 계약을 체결하여 정보처리 시스템의 운영과 유지관리를 맡기고 있으면서,

계약체결시 업무별 월간 서비스시간과 연간 서비스단가를 통해 연간 서비스금액을 산출하나, 계약 기간 중 외부주문 인력의 업무별 실적을 검토하여 용역수행의 적정성을 평가한 사실이 없어 회사가 IT아웃소싱 업무를 체계적으로 관리하지 못할 우려가 있으므로*,

* ㉮서비스의 거래규모는 2020년 ☆억원에서 2022.9월 ☆억원으로 크게 줄었으나, ㉮서비스의 월간서비스시간은 2020년부터 2022년까지 67시간으로 동일

연간 유지보수 인력의 업무별 소요시간을 측정하여 월간 서비스 시간의 적정성을 확인하고 IT아웃소싱 계약 만료 전, B로부터 수행업무와 서비스 품질수준(SLA) 적정성 여부 보고 절차를 마련하는 등 IT아웃소싱 업무 관리를 개선하시기 바람

(9) 비상대응훈련 계획 수립 미흡

내규 「IT서비스연속성 관리 세칙」에 따라 업무 중단 방지 및 신속한 복구를 위하여 연 1회 이상 비상대응훈련을 실시하고 있으며 「IT업무연속성 및 비상대응 매뉴얼」에서 비상 상황 시나리오를 4가지 유형*으로 정의하고 있으나,

* ① 주전산센터 사용이 불가능하나 인력 피해가 없는 상황
  ② 주전산센터 사용이 불가능하고 인력 피해도 발생
  ③ 재해발생으로 주전산센터와 연결된 전력 및 통신회선 단절 등 센터 전환이 필요한 경우
  ④ 주전산센터 사용이 가능하나 인력 손실로 인해 비상대응 체계가 가동되어야 하는 경우

검사대상기간 중 수행한 3회의 비상대응훈련 모두 '주전산센터 사용이 불가능하나 인력 피해가 없는 상황'을 가정하여 수행하였고 인력피해 및 대외기관의 업무 중단 상황 등을 가정한 비상대응훈련을 수행한 적이 없어 실제 비상상황 발생시 서비스 연속성 유지에 어려움이 예상되므로,

비상대응 모의훈련 계획 수립시 기존에 수행하지 않은 다양한 상황을 가정하고 수행하여 비상대응 모의훈련의 실효성을 제고하시기 바람

< 관련규정 >

1. 내규「IT서비스연속성 관리 세칙」제15조 제1항

(10) 일괄작업(BATCH) 통제 미흡

일괄작업 자동화 시스템을 도입하여 운영하고 있으며 스케줄 등록이 필요한 정기 배치작업에 대해서는 전자문서를 통해 작업 요청 및 책임자 승인을 득한 후 스케줄에 따라 시스템이 자동 수행토록 하는 등 정상적으로 통제하고 있으나,

비정기 수시 배치작업은 작업 요청 및 책임자 승인을 전자문서가 아닌 '비정기 배치작업 기록 대장'에 수기로 관리*하고 있어, 책임자 사전 승인없이 비정기 배치작업이 수행될 우려가 있으므로

* 검사대상기간(2019.1.1.~2022.11.8.) 중 총 319건의 비정기 배치작업을 기록·관리

비정기 수시 배치작업도 일괄작업 자동화 시스템을 통해 작업 요청 및 책임자 승인이 진행될 수 있도록 개선하시기 바람

(11) 소스코드 취약점 점검 미흡

2021.4월 형상관리시스템과 연동하여 실제 운영서버에 소스코드를 배포하기 전에 취약점 점검을 수행할 목적으로 소스코드 취약점 점검 시스템을 도입하였으나,

동 시스템의 도입 목적과는 다르게 프로그램 배포 전 소스코드 취약점 점검 수행을 강제화*하지 않아, 홈페이지 프로그램 소스가 보안 취약점이 제거되지 않은 채 실제 운영서버에 적용되어 보안 위협에 노출될 우려가 있으므로

* (예시) 심각(Critical)한 취약점 발견시 운영서버 적용 불가

기존 프로그램의 소스코드 취약점 점검 및 조치계획을 수립하여 이를 추진한 후 프로그램 배포 전 소스코드 취약점 점검 수행을 강제화할 필요가 있음

< 관련규정 >

1. 내규「IT 개발관리 세칙」제10조 제2항

(12) 정보변경 업무 처리 불합리

장애 또는 오류 등에 의한 전산원장 변경과 별도로 전산원장 내 단순 정보변경 업무를 처리하고 있으나,

동 업무 처리와 관련된 내규 또는 매뉴얼 없이 통합단말시스템을 활용하는 단순 정보변경 업무를 오너쉽이 있는 현업부서가 아닌 IT부서가 처리*함으로써 착오 처리시 책임 소재 등의 문제가 발생할 우려가 있으므로

* 검사대상기간(2019.1.1.~2022.11.8.) 중 총 2,012건을 요청받아 처리

통합단말시스템을 활용하는 단순 정보변경 업무는 현업부서가 책임자 승인 절차를 거쳐 처리하도록 현업부서에 이관할 필요가 있음

(13) 유해사이트 차단시스템 보안정책 미흡

① 내규 「임직원 보안관리 세칙」에 따라 불건전 사이트, 비업무 사이트 및 정보유출 위험사이트 등에 대한 접속을 금지하고 있고 해당 사이트에 대한 접근은 유해사이트 차단시스템에서 보안정책을 수립하여 통제하고 있으나,

일부 임직원이 특정 외부사이트에 대해서 업무상 예외적으로 접속을 필요로 하거나 한시적으로 접속을 요청하는 경우 보안정책 예외적용 절차가 마련되어 있지 아니하여 예외정책 적용*에 대한 적정성 확인 등이 미흡할 우려가 있으므로

* 2019.1.1.~2022.10.26. 기간 중 예외접속 신청 21건

임직원 인터넷 사용에 대한 보안정책 예외적용 절차를 마련하여 예외정책에 대한 안전성을 확보하시기 바람

② 정보보호시스템 담당자는 「정보보호시스템 운영보안 방안」에 따라 유해사이트 차단시스템의 보안정책을 정기적으로 점검하고 장기간 미사용 정책 등 불필요한 예외정책을 삭제 또는 변경하고 있으나

장기간 미사용 중임에도 불구하고 인터넷 전용PC에서 상용메일 및 주식(HTS) 거래 프로그램을 허용하는 예외정책이 일부 존재하는 등 보안정책 관리 소홀로 인한 내부정보 유출사고 발생이 우려되므로

예외정책에 대한 적정성을 전면 재검토하여 임직원 인터넷 사용에 대한 보안정책을 강화하시기 바람

< 관련규정 >
1. 내규 「임직원 보안관리 세칙」 제13조
2. 내규 「정보보호시스템 운영보안 방안」 제9조

(14) IT장애 관리 미흡

내규 「IT장애 관리 방안」에 따라 IT장애 발생시 장애 등급을 판정하고 장애 등급별 해결 목표시간 내 장애 복구를 진행하고 있으나,

① 장애 등급 산정을 위한 체크리스트 상 장애대상 정보시스템 항목에 인터넷 VDI 등 총 9개의 정보시스템을 누락함으로써 누락된 정보시스템에 대한 자의적 평가*가 가능하도록 운영하고 있고

* 2020.3.22. '통합운영 SAN 스위치 비정상 재기동 증상'이 발생한 인터넷VDI시스템 장애는 장애대상 정보시스템 항목 등급점수가 누락되어 있어 자의적으로 30점 부여 (10~90점 범위)

② 「IT장애 관리 방안」에는 IT장애 보고 기한을 명시하지 않아 최대 39일 경과 후 보고한 사례*가 존재하는 등 장애 조치 및 보고가 지연될 우려가 있으며, 민원 및 시스템 개발·변경 요청건 중 4건**은 IT장애로 판단되나 IT장애 관리가 누락되었으므로

* 2020.5.4. 대표 홈페이지 접속 장애 발생의 건
** 2019.1.8. 채무불이행 오류 등록의 건

장애등급 산정 체크리스트 상 누락된 정보시스템 항목을 추가하고 장애 보고기한을 IT아웃소싱 SLA* 평가항목에 편입하는 등 관련 절차를 개선하여 IT장애 관리를 강화하시기 바람

* 서비스수준협약(Service Level Agreement) : 제공될 정보 서비스 및 조건들에 대한 협약서

< 관련규정 >
1. 내규 「IT장애 관리 방안」 제9조

(15) 프로그램 변경관리 운영 불합리

2021.4월 노후화된 형상관리시스템을 새로운 형상관리시스템으로 재구축하여 운영하고 있으나,

① 현업부서가 프로그램 개발·변경 요청시 동 시스템을 이용하지 않고 기존 방식대로 공문으로 요청하고, 이를 IT부서가 형상관리시스템에 대신 등록하고 있어 공문번호가 누락되거나 착오 입력된 사례가 총 121건 발생하였고

② 프로그램 개발·변경은 업무 오너쉽이 있는 현업부서가 요청하는 것이 타당하나, 일부 프로그램 개발·변경건*의 경우 IT부서가 시스템 개선 명목으로 자체 처리하고 있으며

* 2021.4.30.~2022.11.21. 기간 내 총 1,806건 중 333건(요청서 기준, 18.4%)

이 경우 현업부서의 인수테스트가 생략된 채 개발자 테스트만 수행되고 있어 테스트 미흡에 따른 IT장애 발생 등이 우려되며

③ 일부 프로그램 개발·변경건*의 경우 요청일로부터 3개월이 경과하였음에도 종결처리되지 않는 등 프로그램 개발·변경 업무가 지연되고 있으므로

* 2021.4.30.~2022.11.21. 기간 내 총 1,806건 중 131건(요청서 기준, 7.3%)

현업부서가 형상관리시스템을 활용토록 하고, IT부서 자체 변경은 최소화하는 등 형상관리시스템 운영을 개선하시기 바람

< 관련규정 >
1. 내규「IT 개발관리 세칙」제3장

(16) 통합단말시스템 권한관리 미흡

통합단말시스템을 활용하여 업무처리를 수행하고 있으며 동 시스템의 전체 화면(총 1,813개)에 대한 조회 또는 저장 등의 권한은 사용자 그룹(248개)별로 각각 부여되어 있으나,

① 소속된 직원이 없는 개발자 그룹에 총 880개(48.5%) 화면에 대한 저장 권한이 부여되어 있고,

② 업무처리 부서가 아닌 DT리빌드TFT 그룹*에 총 953개(52.6%) 화면에 대한 저장 권한 등 과도한 권한이 부여되어 있으므로

* 차세대 TF팀 소속으로 실제 업무처리가 아닌 현행 시스템 분석 목적으로 권한 부여

불필요한 사용자 그룹을 삭제하고, 사용자 그룹별 부여 권한의 적정성을 재검토하여 저장 권한 회수 등 사용자 그룹별 권한 조정하시기 바람

< 관련규정 >

1. 내규「어플리케이션 보안관리 세칙」제7조

(17) 정보보호 관련 직무·보안통제 소홀

① ICT본부에 정보보호팀을 편성하고「IT 경영관리 세칙」에 따라 IT기획, 정보보호 업무 및 데이터베이스 시스템 운영 등 상호견제 기능을 갖출 수 있도록 직무를 분리하고 IT기획담당자와 정보보호담당자를 구분하여 운용 중에 있으나,

IT기획업무를 담당하는 직원이 1명에 불과*하여 동 담당자가 퇴사 등 인사변동시 정보보호담당자가 IT기획 업무를 겸업하는 등의 상호견제 기능을 상실할 가능성이 있으므로,

* 정보보호 업무의 경우 2명(정,부)이 담당

IT기획업무 담당 인력을 정·부로 지정하여 운영하는 등 정보보호 업무와 직무가 분리되도록 개선하시기 바람

②「정보시스템 운영보안 세칙」에 따라 정보보호시스템 운영 담당자는 보안정책 예외사항*을 한시적으로 적용 받는 대상자가 있을 경우 예외 허용 기간 만료일에 해당 정책을 회수하여야 하나

* USB 등 매체제어 읽기/쓰기, DRM 복호화 권한, 망간 자료전송 반출입 정책 등

2019.1.1.~2022.10.21. 기간 중 USB 읽기 허용 등 보안정책 예외요청 총 322건*을 정보보호시스템에 적용하면서 예외 허용 기간 만료일에 자동으로 회수되도록 운영하지 아니하고 담당자가 수작업을 통해 매월 한 번씩 일괄 회수하고 있어, 허용 기간을

초과한 일부 예외정책으로 인하여 내부 중요 정보가 업무목적 외 용도로 회사의 보안통제를 적용받지 않고 유출될 우려가 있으므로

* USB 등 매체통제 39건, DRM 권한통제 70건, 망간 자료전송 통제 213건

자동화 솔루션 등을 도입·구축하여 보안정책 예외사항이 적시에 회수될 수 있도록 보안통제를 강화하시기 바람

< 관련규정 >
1. 내규 「IT 경영관리 세칙」 제8조
2. 내규 「정보시스템 운영보안 세칙」 제17조

(18) 단말기 보정(PATCH) 관리절차 미흡

「정보시스템 운영보안 세칙」에 따라 정보시스템 운영 주관부서는 주기적으로 패치 정보를 수집하고, 긴급하고 중요한 보정 사항에 대하여 안정성 확보 및 영향도 분석 후 패치 적용을 수행하고 있으나

패치 대상 정보시스템* 중 단말기에 대해서만 보안 패치 작업** 관련 의사결정 기록을 별도로 남기고 있지 않아 중요한 패치 사항에 대하여 안정성 확보 및 사전 영향도 분석 등 충분한 검토가 이루어졌는지를 확인할 수 없는 등 관리업무가 미흡하여 단말기 패치 작업의 실패에 대비한 복구 대책 등이 소홀해질 우려가 있으므로

* 단말, 서버, 네트워크, 데이터베이스, 정보보호시스템
** 업무용 단말기 741대에 Windows 10 2022년 9월 업데이트 적용

단말기 보안 패치시 영향도 분석 등 안정성 확보에 필요한 작업 계획서를 마련하여 책임자 승인을 거친 후 단말기 보정작업을 진행하도록 관련 절차를 개선하시기 바람

< 관련규정 >
1. 내규 「정보시스템 운영보안 세칙」 제8조

(19) 암호화 키 관리 미흡

「어플리케이션 보안관리 세칙」 제10조에 따라 암호화 프로그램 담당자를 지정

하고 담당자 이외의 이용을 통제하고 있으며, 암호화 프로그램 적용과 키 생성 및 배포는 「정보시스템 암호화 관리 방안」에서 정한 바에 따라 “암호화 키 관리대장”에 등재하여 안전하게 관리하고 있으나,

① 암호화 키에 대한 무결성 확보를 위하여 암호화 키 복사본을 생성한 뒤 물리적으로 분리된 내화금고에 보관하는 과정에서 암호화 키 변조를 방지하기 위한 적절한 수단*이 마련되어 있지 아니하여 저장 중인 암호화 키에 대한 무결성 보장이 곤란하므로

* 무결성 검사(HASH, MAC, CRC, 패리티 등), 키 관리 시스템(KMS) 도입·구축 등

암호화 키 복사본 생성시 저장 중인 암호화 키의 해쉬값(HASH)을 추출하여 키 복사본과 해쉬값을 함께 백업하는 등 무결성 보장 절차를 마련하여 개선하시기 바람

② 자체 모바일 앱 등록·배포시 필요한 전자서명 키의 경우 물리적으로 분리된 내화금고에 보관하지 않고 변조 방지를 위한 별도의 무결성 보장 조치 마련 없이, “암호화 키 관리대장”에서 누락된 상태로 형상관리시스템에 소스코드와 함께 업로드하여 보관하는 등 이용 중인 암호화 키 관리 소홀로 인한 부당사용 및 유출의 우려가 있으므로

“암호화 키 관리대장”에 전자서명 키를 등록하여 물리적으로 분리된 내화금고에 안전하게 보관하고 앱 등록·배포시 전자서명 키가 외부로 유출되지 않도록 기술적·관리적 대책을 마련하여 관리하시기 바람

< 관련규정 >
1. 내규 「어플리케이션 보안관리 세칙」 제10조
2. 매뉴얼 「정보시스템 암호화 관리 방안」 제12조

(20) 모바일 앱 IT보안사고 예방활동 미흡

정보시스템 운영 주관부서는 「정보시스템 운영보안 세칙」에 따라 정보시스템에 대한 모니터링 및 로그 분석 작업을 지속적으로 수행하고 있으며, 정보보호주관부서는 「보안사고 대응 관리 세칙」에서 정한 바에 따라 그룹통합보안관제센터와 연계하여 보안사고가 발생하지 않도록 침해 징후에 대한 모니터링을 수행하고 있으나

2020.10월, 모바일 앱 보안솔루션 재구축 사업* 당시 모바일 앱이 설치된 이용자의 단말기에서 발생한 이상징후(루팅, 원격제어 등)에 대한 탐지로그를 수집하는 기능을

누락하여 침해사고 모니터링 및 로그 분석 작업의 수행이 불가능함에 따라 IT보안사고 등을 미연에 방지하지 못할 우려가 있으므로

* 모바일 앱 구동시 루팅 등 단말기 해킹 방지를 위한 보안솔루션 도입

모바일 앱 보안솔루션의 로그 생성 기능 개선하고 탐지된 로그는 그룹통합보안관제 업무와 연계하는 등 침해징후에 대한 차단 방안을 마련하여 보안사고가 발생하지 않도록 사전 예방활동을 강화하시기 바람

< 관련규정 >

1. 내규「정보시스템 운영보안 세칙」제9조
2. 내규「보안사고 대응 관리 세칙」제4조 및 제9조