# 경영유의사항 등 공개안

1. 금융기관명 : 비씨카드㈜

2. 조치일 : 2025. 11. 11.

3. 조치내용

| 제재대상 | 조치내용 |
|---|---|
| 기 관 | 경영유의사항 2건, 개선사항 2건 |

4. 조치대상사실

가. 경영유의사항

(1) 제3자 서비스 관리체계 강화 필요

회사는 핵심업무에 대한 역량 집중, 기타 업무의 효율적 운영 등을 위하여 다수의 외부 전문업체와 제휴 및 정보처리위탁 계약을 맺고 있으며, 이를 관리하기 위해 구매정보시스템에 제휴 및 정보처리위탁 계약을 등록하여 관리하고 있고 관련 전자금융거래 서비스의 주기적(반기) 현황 관리, 제3자 서비스 단일 장애지점의 식별 및 리스크 제거를 위한 제3자 서비스 이중화를 지속적으로 고려하고 있다.

하지만 제3자 서비스와 관련한 총괄 관리부서 및 관리 체계가 존재하지 않고 제3자 서비스에 대한 업무 영향도 관리 기준이 수립되어 있지 않다. 이로 인해 제3자 서비스 전체 현황 및 관련 전자금융거래 서비스의 최신화, 제3자 서비스 장애 발생시 업무 영향도 등이 체계적으로 관리되지 않고 있다.

<조치할 사항>

따라서 회사는 제3자 서비스 총괄 관리부서 지정 및 업무 영향도 관리 기준 등 관리 체계를 마련하여 단일 장애지점을 식별·관리하는 등 제3자 서비스 관리를 강화하여 운영하시기 바랍니다.

### (2) 클라우드서비스 인프라 관리체계 강화 필요

회사는 페이북 서비스 등에 대해 클라우드서비스를 이용하고 있으며, 클라우드서비스의 원활한 운영을 위해 일부 인프라 및 보안 운영 업무를 외부주문 업체(A, 이하 'MSP')에 위탁하여 운영하고 있다.

하지만 클라우드서비스 인프라 및 보안 운영 업무를 MSP에서 수행하고 있는데도, 이에 대한 내부감사 절차 등은 마련·운영하고 있지 않다.

그리고 회사에서 관리하는 자체 인프라(On-Premise)에 대해서는 운영 현황 분석 보고서를 분기별로 작성·보고하고 있으나, MSP에 위탁관리하고 있는 클라우드서비스에 대해서는 동 운영현황 보고서를 작성·보고하지 않는 등 IT 거버넌스 관리 수준 및 운영인력의 적정성 등에서 차이가 발생하고 있다.

또한, 회사 자체 인프라에 대한 재해복구시스템 전환 복구 매뉴얼(B본부 관리)과 클라우드서비스 인프라에 대한 재해복구시스템 전환 복구 매뉴얼(C팀 관리)을 통합하여 관리하지 않고 각각 운영하고 있어 재해 발생 시 클라우드서비스 시스템을 포함한 전사 차원의 재해복구시스템 전환이 원활하지 않을 우려가 있다.

<조치할 사항>

따라서 회사는 클라우드서비스에 대한 인력 규모의 적정성 검토, 관리절차 및 내부통제 방안, 인프라 관리 기준을 개선·운영하고, '재해복구시스템 전환 복구 매뉴얼' 등에 클라우드서비스 시스템에 대한 재해복구 절차 등을 통합하여 운영하는 등 클라우드서비스 관리에 대한 전반적인 거버넌스 체계를 갖추어 운영하시기 바랍니다.

## 나. 개선사항

### (1) 외부 연계기관 통신회선 연결 및 대체수단 마련 미흡

회사는 원활한 전자금융서비스 제공을 위해 외부 연계기관의 서비스를 이용하고 있는데, 이를 위해 외부 연계기관과 전용회선 등을 이중화하여 연결하고 있다.

하지만 핵심 업무와 관련된 일부 고객사(D 등) 및 일부 국제카드사(E, F 등)와 회사 재해복구센터 간 전용회선이 연결되어 있지 않아 회사 주전산센터 재해 발생으로 재해복구센터가 가동되는 경우 연계된 외부 서비스를 이용하지 못할 위험이 있다.

그리고, 회사와 회사의 G 법인은 암호화 강도가 약한 알고리즘으로 VPN을 연결하고 있어 보안 위험이 우려된다.

또한, ARS 인증, 계좌점유인증(1원 인증)을 위해 H, I와 서비스 제휴 계약을 맺고 있는데, 동 서비스의 장애 발생에 대비한 대체수단을 마련하지 않아 해당 서비스 장애 시 페이북 머니 계좌 연결 등 관련 전자금융거래 서비스의 이용이 불가하다.

<조치할 사항>

따라서 회사는 핵심 업무에 대해서 외부 연계기관과의 통신회선 연결을 확인하여 회사의 장애 또는 재해 발생 시에도 서비스가 가능하도록 통신회선 연결을 보완·강화하고 암호화 강도가 약한 알고리즘으로 구성된 VPN 연결은 강한 알고리즘으로 개선하시기 바랍니다.

또한, 제3자 서비스의 대체수단 가능여부를 재검토하여 대체수단 혹은 보완수단을 마련하여 제3자 서비스 장애로 인한 전자금융거래 서비스 장애로의 전이를 예방하는 등 운영복원력을 확보하시기 바랍니다.

**(2) 온라인 결제 관련 단일 장애지점 관리 및 재해복구전환훈련 미흡**

회사는 매년 재해복구전환훈련 실시 계획에 따라 업무연속성 확보를 위한 자체 재해복구전환훈련을 월 1회 실시하고, 부가통신사업자(VAN) 연동 재해복구전환훈련은 연 2회, 고객사(카드발급사) 및 부가통신사업자(VAN) 합동 재해복구전환훈련은 연 2회 실시하고 있다.

하지만 회사는 온라인 결제 과정 대부분[1]을 J에 위탁하여 수행하고 있으며, 동사는 대체수단이 존재하지 않는 단일 장애지점으로 장애 등 비상 상황 발생 시 비씨카드 온라인 결제업무가 불가[2]한데도 J에 대한 관리가 미흡[3]하다.

1) PG연동, VAN연동, ISP인증, 추가인증(100만원 이상 고액결제, 상품권·환금성 상품 구매 등)
2) 삼성페이, 네이버페이, 카카오페이 등 타사 간편결제를 통한 결제업무는 가능
3) H에 대한 전산 성능 및 운영 상황과 SLA 점검은 연 1회 수행하고 있고, 위탁업무 장애시 대응을 위한 비상대책 수립이 미흡함

또한, 회사 재해복구전환훈련 시 J 등과 연계한 온라인 결제 업무에 대해서는 재해복구전환훈련을 실시하지 않았다.

<조치할 사항>

따라서 회사는 온라인 결제 관련 단일 장애지점의 서비스 중단을 예방하기 위해 J에 대한 운영현황 점검 등* 관리를 강화하고 상황별 비상대책을 수립하시기 바랍니다.

* 전산 성능, 운영 상황 및 SLA 점검 주기 단축 및 점검내용 강화 등

또한, 페이북 온라인 결제 서비스의 연속성을 보장하기 위해 장애 발생시 비상대책을 보완하고, J와 연계한 재해복구전환훈련을 실시하는 등 제3자 서비스 기관과 연계 모의훈련을 강화하여 운영하시기 바랍니다.