BNP PARIBAS

MS365 클라우드서비스 이용에 따른 안전성 확보 조치

BNP 파리바은행 서울지점은 전자금융감독규정 제 14 조의 2 (클라우드컴퓨팅서비스 이용절차 등) 및 금융회사의 정보처리 업무 위탁에 관한 규정 제 5 조에 따라 MS365 클라우드 서비스로 위탁 처리되는 정보의 보호를 위한 안전성 확보 조치가 아래와 같이 확보되었음을 공시합니다.

전자금융감독규정 별표 2-2 에 따라, '기본 보호조치'와 '금융분문 추가 보호조치'로 구분함.

1. 기본 보호조치

   규정에 의거하여 국내·외에서 아래의 보안 인증을 획득하여 유지하고 있는 클라우드 서비스 제공자의 경우 '기본 보호조치' 항목들에 대한 평가를 생략가능하며, Microsoft 는 아래 열거된 국내외 인증을 모두 취득하였고 금융보안원의 평가절차를 거쳤음을 확인합니다.

분류	인증제도	평가 생략 근거
국내	CSAP	- 과학기술정보통신부에서 관장, KISA 에서 평가 및 인증 부여 - 국내 주요 클라우드서비스 제공자들이 인증 획득 - 약 120 개 평가 항목을 구성
해외	FedRAMP (High) (미국)	- 연방정부 (FedRAMP Program Management Office)에서 관장 - 최대 약 400 개 평가 항목으로 구성
	CSA STAR (Gold) (글로벌)	- 약 400 개 클라우드서비스 제공자가 동참하여 CSA 에서 관장 (* CSA: Cloud Service Alliance – 최대 약 300 개 평가 항목으로 구성)
	MTCS (Level3) (싱가포르)	- 정보통신미디어 개발청 IMDA (Info-communication Media Development Authority) 에서 관장 및 인증 부여

2. 금융부문 추가 보호조치

금융부문 추가 보호조치 항목	세부 항목	조치사항 확보
1 사고 보고 및 분석 수행 절차 확보	사고보고 및 분석을 위해 사고조사 지원, 훈련 지원 등 금융위원회, 금융감독원, 침해사고 대응기관의 협조 요청에 대응할 수 있도록 체계가 마련되어 있는가?	확보완료
	전산장애, 전자적 침해행위 등 발생 시 금융회사 및 침해사고 대응기관에 즉시 알리고 적절히 대처할 수 있는 방안이 마련되어 있는가?	
2 금융권 통합보안관제 수행 체계 지원	금융권 통합 보안관제수행을 위한 관리적· 물리적· 기술적 지원 체계가 마련되어 있는가?	확보완료
3 취약점 분석·평가 수행 체계 지원	관계 법규에 따라 금융회사가 취약점 분석·평가를 수행할 수 있도록 지원 체계가 마련되어 있는가?	확보완료
	전자금융기반시설의 취약점 분석·평가 전문기관의 취약점 분석·평가 업무 수행을 위해 전산실 및 정보처리시스템에 대한 접근을 허용 (필요시 물리적 접근 포함)하도록 절차가 마련되어 있는가?	
	금융회사의 취약점 분석·평가 결과에 따라 취약점의 제거 또는 이에 상응하는 조치를 수행하는 절차가 마련되어 있는가?	
4 합동비상대응훈련 지원	금융회사가 수립한 비상대책에 따른 비상대응훈련 및 재해복구전환 훈련 실시에 대해 협조 및 지원 하도록 체계가 마련되어 있는가?	확보완료
	필요한 경우 금융위원회가 실시하는 금융분야 합동비상대응훈련에 참여하고 지원하도록 체계가 마련되어 있는가?	
5 건물·전원·전산실 금융회사 수준 구축 (* 금융회사 시스템을 운영하는 클라우드 서비스 제공자의 데이터센터는 금융회사 전산실로 볼 수 있어 관련 규정 준수 필요)	화재, 침수, 진동 등 외부요인으로부터 적절한 보호대책이 마련되어 있는가?	확보완료
	전산실내 주요시설에 출입통제, 감시제어를 위한 설비가 마련되어 있는가?	
	전력공급중단에 대비하여 적절한 대책이 마련되어 있는가? (자가발전설비, 전력선 이중화, UPS 등)	
	전산실내 적정한 온도 및 습도 유지를 위한 설비가 마련되어 있는가?	
	(고유식별정보 및 개인신용정보 처리 시) · 해당 정보를 처리하는 모든 정보처리시스템을 국내에 설치할 수 있는가? · 무선통신망이 미설치되어 있는가?	해당사항없음
6 전산자료 보호	사용자계정과 비밀번호를 개인별로 부여하고, 관리하기 위한 기능을 제공하는가?	확보완료
	전산자료를 정기적으로 백업하고 검증할 수 있도록 지원 체계가 마련 되어 있는가?	확보완료

	정보처리시스템 관리자의 주요 업무 관련 행위를 책임자 또는 금융 회사가 이중확인 및 모니터링 할 수 있는 기능을 제공하는가?	확보완료
	정보처리시스템의 가동 기록을 1 년 이상 보존하고 있는가?	
	정보처리시스템 접속 기록(일시, 접속자, 접근확인), 전산자료 접근 기록(일시, 사용자, 자료내용), 전산자료 처리 내용 기록(사용자 로그인, 액세스 로그 등)이 접속 성공 여부와 상관없이 자동으로 기록·유지에 협조 및 지원하도록 체계가 마련되어 있는가?	
	금융회사의 정보처리시스템과 관련된 단말기 및 전산자료에 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제 장치를 마련·운용하는가?	확보완료
7 이중화 및 백업체계 구축	(주요 전산장비의 경우) 금융회사가 이중화 또는 예비장치를 확보 할 수 있도록 협조 및 지원 체계가 마련되어 있는가?	확보완료
	금융회사가 각 업무별로 지정한 복구목표시간을 준수할 수 있도록 협조 및 지원 체계가 마련되어 있는가?	확보완료
	장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단 되지 않도록 상황별 대응절차, 재해복구계획, 비상대응조직의 구성 및 운용, 모의훈련, 비상연락체계, 파업 시 비상지원인력, 업무 매뉴얼 등을 포함한 업무지속성 확보방안을 수립·준수하고 주기적으로 점검하는가?	확보완료
8 해킹 등 방지대책	시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업을 실시하고 있는가?	확보완료
	내부 업무용시스템 설치 시 인터넷 등 외부통신망과 분리·차단 및 접속을 금지(물리적 또는 논리적) 할 수 있도록 기능을 제공하고 지원하도록 체계가 마련되어 있는가?	확보완료
	패치 수행 등을 위해 중앙에서 파일을 배포할 경우 무결성 검증을 수행하는가?	확보완료
	클라우드서비스 제공자 내에서 클라우드 시스템 관리를 목적으로 클라우드 시스템에 직접 접속하는 단말기에 대해서는 인터넷 등 외부 통신망으로부터 분리(물리적 또는 논리적) 하는가?	확보완료
	금융회사가 클라우드서비스 이용 정보처리시스템 및 정보통신망에 대해 정보보호시스템을 설치·운영할 수 있도록 지원 체계가 마련되어 있는가?	확보완료

	해킹 등 전자적 침해행위로 인한 사고를 방지하기 위해 적절한 정보보호시스템을 설치하여 안전하게(이력보관, 접근통제 등) 운영하고 있는가?	확보완료
9 기타	금융회사가 재무건전성 평가 등 주요 경영활동에 대해 상시 모니터링을 실시할 수 있도록 지원 체계가 마련되어 있는가?	확보완료
	금융회사가 서비스 품질수준을 평가할 수 있도록 지원 체계가 마련 대한 기준) 되어 있는가?	
	금융회사의 정보처리업무 위탁과 관련한 계약서, 계약서 부속자료 및 그 밖의 전자금융업무와 관련한 자료 등을 금융감독원의 요구를 수용하도록 체계가 마련되어 있는가?	왁보완료
	금융회사가 개인(신용)정보 관련 규제 등 기타 금융관련 법령을 준수하는데 필요한 사항을 지원 및 협조하도록 체계가 마련되어 있는가?	