<별표 2의2> <전문개정>

클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가기준(제14조의2 관련)

금융회사 또는 전자금융업자는 아래의 항목에 따라 클라우드서비스 제공자의 건전성 및 안전성을 평가하되, 제14조의2제1항제1호에 따라 비중요업무로 분류된 경우 또는 클라우드서비스 제공자가 국내·외의 클라우드서비스 관련 보안인증 등을 취득하여 유지 중임을 확인한 경우 대체항목에 관한 평가는 생략할 수 있다.

구분		평가항목	항목	적용 대상
1 정보보호 정책 및 법규 준수	1.1 정보보호 정책	1.1.1. 조직 전반에 적용하고 있는 정보보호 정책 및 지침 또는 규정을 수립·시행하고 있는가?	대체	IaaS, PaaS,SaaS
		1.1.2. 정기적으로 정보보호정책의 타당성을 검토, 평가하여 수정, 보완하기위한 절차를 마련하고 이행하고 있는가?	대체	IaaS, PaaS,SaaS
	1.2 정보보호 조직	1.2.1 조직의 정보보호를 위한 전담조직을 구성하여 안전성 확보 및 이용자 보호 등 정보보호 활동을 효과적으로 수행하고 있는가?	대체	IaaS, PaaS,SaaS
		1.2.2 정보보안 및 정보자산과 관련된 모든 인력의 역할과 책임을 정의하고, 이용자의 정보보호 역할과 책임을 명확하게 정의하고 있는가?	대체	IaaS, PaaS,SaaS
	1.3 법 및 정책 준수	1.3.1 이용자가 법령 등 의무준수를 위해 필요한 사항을 지원 및 협조하도록 체계가 마련되어있는가?	필수	IaaS, PaaS,SaaS

구분		평가항목	항목	적용 대상
	1.4 보안감사	1.4.1 접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되고, 비인가 된 접근 및 변조로부터 보호되고 있는가?	필수	IaaS, PaaS,SaaS
2 인적보안	2.1 내부인력 보안	2.1.1 클라우드서비스의 시스템 운영, 개발, 보안 등에 관련된 모든 임직원을 주요 직무자로 지정하여 관리하고 있는가?	대체	IaaS, PaaS,SaaS
		2.1.2 권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무 분리 기준을 수립· 적용하고 있는가?	대체	IaaS, PaaS,SaaS
		2.1.3 조직 내 인력의 인사 변경 발생시 지체없이 해당 사용자의 정보자산 반납, 접근 권한 변경 및 회수가 이루어 지고 있는가?	대체	IaaS, PaaS
	2.2 외부인력 보안	2.2.1 외부인력에 대한 보안요구사항 준수 여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하고 있는가?	대체	IaaS, PaaS
3 위험평가 및 관리	3.1 자산 식별 및 분류	3.1.1 클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하고 있는가?	대체	IaaS, PaaS,SaaS
	3.2 자산 변경관리	3.2.1 시스템 통합, 전환 및 재개발 시 클라우드컴퓨팅서비스 운영에 지장을 초래하지 않도록 통제절차를 마련하여 적용하고 있는가?	대체	IaaS, PaaS,SaaS
	3.3 위험관리	3.3.1 클라우드서비스를 제공하기 위한 핵심자산 및 서비스를 대상으로 주기적으로 취약점 점검을 수행하고, 발견된 위험에 대한 보완조치를 수행하고 있는가?	대체	IaaS, PaaS,SaaS
4	4.1	4.1.1	대체	IaaS,

구분		평가항목	항목	적용 대상
서비스 공급망 관리	공급망 관리정책	공급망과 관련한 보안 요구사항을 정의하는 관리정책을 수립하고 이행하는가?		PaaS,SaaS
	4.2 공급망 변경관리	4.2.1 공급망 상에서 발생하는 모든 기록 및 보고서에 대해 정기적으로 모니터링 및 검토를 수행하는가?	대체	IaaS, PaaS
5 업무연속성 계획 및 재해복구	5.1 장애대응	5.1.1 클라우드서비스가 중단되지 않도록 업무 지속성 확보방안을 수립하고 이행하는가?	대체	IaaS, PaaS,SaaS
		5.1.2 클라우드서비스 중단이나 피해가 발생한 경우 장애보고 절차에 따라 장애상황을 기록하고 이용자에게 현황을 파악할 수 있도록 관련 정보를 제공하는가?	필수	IaaS, PaaS,SaaS
		5.1.3 클라우드서비스 중단이나 피해가 발생하는 경우, 재해복구목표시간 내 서비스의 장애를 처리하고 복구할 수 있는가?	대체	IaaS, PaaS,SaaS
	5.2 서비스 가용성	5.2.1 가상화 서버, 설비 등 정보처리설비의 장애로 인해 서비스가 중단되지 않도록 관련 설비를 이중화하고, 백업 체계를 마련하고 이행하는가?	필수	IaaS, PaaS,SaaS
		5.2.2 주기적으로 서비스 연속성(가용성) 확보를 위한 점검을 수행하고 있는가?	대체	IaaS, PaaS
6. 침해사고 대응 및 관리	6.1 침해사고 대응 절차 및 체계	6.1.1 해킹 등 전자적 침해행위로 인한 피해 발생 시 대응을 위한 침해사고 대응절차를 수립하고 이행하는가?	대체	IaaS, PaaS,SaaS
		6.1.2 침해사고 발생 시 신속한 대응이 가능하도록 주기적으로 침해사고 대응절차에 기반한 훈련을 실시하고 있는가?	대체	IaaS, PaaS,SaaS
		6.1.3 금융권 통합 보안관제수행을 위한 지원 체계가 마련되어 있는가?	필수	IaaS, PaaS
	6.2 침해사고 대응	6.2.1 침해사고 발생 시 침해사고 대응절차에 따라 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황등을 신속하게	필수	IaaS, PaaS,SaaS

구분		평가항목	항목	적용 대상
		알리고 있는가?		
7 사용자 인증 및 접근통제	7.1 접근통제 정책	7.1.1 비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하고 이행하는가?	대체	IaaS, PaaS,SaaS
	7.2 접근권한 관리	7.2.1 클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 검토하고 있는가?	대체	IaaS, PaaS,SaaS
		7.2.2 이용자의 정보처리시스템과 관련된 단말기 및 전산자료에 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련하고 적용하고 있는가?	필수	IaaS, PaaS,SaaS
	7.3 사용자 식별 및 인증	7.3.1 이용자가 클라우드서비스 이용 시 추가 인증수단을 요청하는 경우 이를 제공하고 있는가?	대체	IaaS, PaaS,SaaS
		7.3.2 이용자의 안전한 클라우드서비스 이용을 위해 계정 및 패스워드 등의 관리절차 마련하고 안내하고 있는가?	대체	IaaS, PaaS,SaaS
8. 가상화 및 인프라 보안	8.1 가상화 보안	8.1.1 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하고 있는가?	대체	IaaS, PaaS,SaaS
		8.1.2 이용자가 클라우드서비스 이용 중 가상자원*을 삭제할 경우 삭제대상과 관련된 모든 자원이 복구되지 않는 방법으로 삭제되는가? *가상머신(이미지, 백업, 스냅샷 등), 가상스토리지, 가상소프트웨어, 가상환경 설정정보 등	필수	IaaS, PaaS,SaaS
		8.1.3 가상자원에 대한 무결성을 보장하고 가상자원 손상 시 이용자에게 안내하고	필수	IaaS, PaaS,SaaS

구분		평가항목	항목	적용 대상
		있는가?		
		8.1.4 하이퍼바이저 등 물리적/논리적 가상화 서버(기능) 및 인터페이스에 대한 보안관리 및 접근통제를 수행하고 있는가?	대체	IaaS, PaaS
		8.1.5 가상자원 관리 시스템*과 가상 소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 관리적, 물리적, 기술적 보호대책을 수립하고 이행하는가? * 가상자원을 제공하기 위한 웹사이트(클라우드 포탈, 클라우드 콘솔, API등)	필수	IaaS, PaaS,SaaS
	8.2 가상환경 보호	8.2.1 이용자의 가상환경 보호를 위한 악성코드 방지대책을 수립하고 이행하는가?	대체	IaaS, PaaS,SaaS
	8.3 인프라 보안	8.3.1 클라우드서비스와 관련된 내외부 네트워크를 보호하기 위한 정보보호시스템을 설치하고 운영하고 있는가?	대체	IaaS, PaaS,SaaS
		8.3.2 업무, 서비스 등을 고려한 영역 간 네트워크를 분리하여 운영하고 있는가?	대체	IaaS, PaaS,SaaS
		8.3.3 이용자의 가상환경 보호 및 네트워크 분리를 위해 필요한 기능을 제공하는가?	필수	IaaS, PaaS
9 개발 및 운영 보안	9.1 시스템 분석 및 설계	9.1.1 보안감사증적(로그)의 정확성을 보장하기 위해 표준시각으로 동기화하고 있는가?	대체	IaaS, PaaS,SaaS
	9.2 구현 및 시험	9.2.1 테스트 시 이용자 정보 사용을 금지(부하테스트 등의 불가피한 경우 이용자 정보 변환 사용 및 테스트 종료 즉시 삭제)하고 있는가?	대체	IaaS, PaaS,SaaS
10 암호화 및 데이터 보호	10.1 데이터 보호	10.1.1 데이터 분류기준에 따라 데이터를 분류하고 관리하고 있는가?	대체	IaaS, PaaS,SaaS
		10.1.2	대체	IaaS,

구분		평가항목	항목	적용 대상
		이용자의 데이터 소유권을 명확하게 확립하고 있는가?		PaaS,SaaS
		10.1.3 입•출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 보장하고 있는가?	대체	IaaS, PaaS,SaaS
		10.1.4 데이터에 대한 접근제어, 위•변조 방지 등 데이터 처리에 대한 보호기능을 이용자에게 제공하고 있는가?	대체	IaaS, PaaS,SaaS
		10.1.5 이용자의 데이터가 처리되는 위치를 추적하기 위한 방안을 제공하고 있는가?	대체	IaaS, PaaS,SaaS
		10.1.6 이용자의 클라우드서비스 이용계약 종료 시 이용자의 모든 가상자원은 복구가 불가능하도록 삭제하고 있는가?	필수	IaaS, PaaS,SaaS
	10.2 암호화	10.2.1 이용자 데이터 처리 시 암호화를 적용하여 보호하고 있는가?	대체	IaaS, PaaS,SaaS
		10.2.2 암호키의 안전한 관리 절차를 수립하고 안전하게 보관하고 있는가?	대체	IaaS, PaaS,SaaS
11 물리적 보안	11.1 물리적 보호구역	11.1.1 전산실 내 주요시설에 출입통제, 감시제어를 위한 설비가 마련되어 있는가?	필수	IaaS, PaaS
		11.1.2 고유식별정보 또는 개인신용정보를 처리하는 경우 전산실 내 무선통신망 사용을 제한(통제) 하고 있는가?	필수	IaaS, PaaS,SaaS
		11.1.3 사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하고 있는가?	대체	IaaS, PaaS
	11.2 정보처리 시설 및	11.2.1 고유식별정보 및 개인신용정보를 처리하는 모든 정보처리시스템을 국내에 설치하고	필수	IaaS, PaaS,SaaS

구분		평가항목	항목	적용 대상
	장비보호	있는가?		
		11.2.2 각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재 감지기, 소화 설비, 누수 감지기, 항온 항습기, 무정전 전원장치(UPS), 이중 전원선 등의 설비를 갖추고 있는가?	필수	IaaS, PaaS
		11.2.3 정보처리시설 내 이용자 정보(자료)가 저장된 장비를 폐기하는 경우 복구가 불가능하도록 처리하고 있는가?	대체	IaaS, PaaS