금융위원회 고시 제2022-44호

전자금융감독규정 일부개정고시안

전자금융감독규정 일부를 다음과 같이 개정한다.

제8조의2제3항제5호를 제6호로 하고, 같은 항에 제5호를 다음과 같이 신설한다.

5. 제14조의2제1항의 클라우드컴퓨팅서비스의 이용에 관한 사항

제14조의2제1항제1호 중 “자체적으로 수립한”을 “다음 각 목의”로, “이용대상 정보처리시스템”을 “이용업무”로 하고, 같은 호에 각 목을 다음과 같이 신설하며, 같은 항 제2호 및 제3호를 각각 다음과 같이 하고, 같은 조 제2항 중 “제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준”을 “제1항 각 호에 따른 평가결과, 업무연속성 계획 및 안전성 확보조치”로 하며, 같은 조 제3항을 다음과 같이 한다.

가. 규모, 복잡성 등 클라우드컴퓨팅서비스를 통해 처리되는 업무의 특성

나. 클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향

다. 전자적 침해행위 발생시 고객에게 미치는 영향

라. 여러 업무를 같은 클라우드컴퓨팅서비스 제공자에게 위탁하는 경우 해당 클라우드 컴퓨팅서비스 제공자에 대한 종속 위험

마. 클라우드컴퓨팅서비스 이용에 대한 금융회사 또는 전자금융업자의 내부통제 및 법규 준수 역량

바. 그 밖에 금융감독원장이 정하여 고시하는 사항

2. 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가(단, 제

1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 <별표 2의2>의 평가항목 중 필수항목만 평가할 수 있다.)

3. 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획 및 안전성 확보 조치의 수립·시행(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 <별표 2의3> 및 <별표 2의4>의 필수 사항만 수립·시행할 수 있다.)

③ 금융회사 또는 전자금융업자는 제1항제2호의 평가를 직접 수행하거나 제37조의4제1항의 침해사고대응기관이 수행한 평가의 결과를 활용할 수 있다.

제14조의2제4항을 제5항으로 하고, 같은 항(종전의 제4항) 각 호 외의 부분 중 “제3항”을 “제4항”으로 하며, 같은 항 제3호 및 제4호를 각각 제4호 및 제5호로 하고, 같은 항 제2호 중 “자체”를 “업무의”로 하며, 같은 항에 제3호를 다음과 같이 신설하고, 같은 항 제4호(종전의 제3호) 중 “클라우드컴퓨팅서비스 이용 관련”을 “제1항제3호에 따른”으로 하며, 같은 항에 제6호를 다음과 같이 신설한다.

3. 제1항제2호에 따른 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가 결과

6. <별표 2의5>의 계약서 주요 기재사항을 포함한 클라우드컴퓨팅서비스 이용계약서

제14조의2제5항을 제6항으로 하고, 같은 항(종전의 제5항) 중 “제3항”을 “제4항”으로, “제4항”을 “제5항”으로 한다.

제14조의2제6항을 제4항으로 하고, 같은 항(종전의 제6항) 각 호 외의 부분 중 “변경사항이”를 “사유가”로, “7영업일”을 “3개월”로 하며, 같은 항 제1호, 제2호 및 제3호를 각각 제2호, 제3호 및 제4호로 하며, 같은 항에 제1호를 다음과 같

이 신설하고, 같은 항 제2호(종전의 제1호) 중 “등의 사유로 클라우드컴퓨팅서비스 이용계약에”를 “등”으로 하며, 같은 항 제4호(종전의 제3호) 중 “제4항제2호”를 “제1항제2호”로 한다.

1. 클라우드컴퓨팅서비스 이용계약을 신규로 체결하는 경우

제14조의2제7항 중 “제3항 또는 제6항”을 “제4항”으로 한다.

제14조의2제8항 중 “제2항”을 “제1항”으로 하며, “제3항제1호에 따른”을 삭제한다.

제15조제1항제3호 중 “금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)”를 “금지.”로 하고, 같은 호에 단서를 다음과 같이 신설한다.

다만, 다음 각목의 경우에는 그러하지 아니하다

제15조제1항제3호에 각 목을 다음과 같이 신설한다.

가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다)

나. 업무상 불가피한 경우로서 금융감독원장의 확인을 받은 경우

제15조제1항제5호 중 “것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)”을 “것.”으로 하고, 같은 호에 단서를 다음과 같이 신설한다.

다만, 다음 각목의 경우에는 그러하지 아니하다.

제15조제1항제5호에 각 목을 다음과 같이 신설한다.

가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개

발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다)

나. 업무상 불가피한 경우로서 금융감독원장이 인정하는 경우

부 칙

제1조(시행일) 이 규정은 2023년 1월 1일부터 시행한다.

신·구조문대비표

현 행	개 정 안
제8조의2(정보보호위원회 운영) ①·②(생 략) ③ 정보보호위원회는 다음 각 호의 사항을 심의·의결한다. 1. ~ 4.(생 략) <신 설> 5.(생 략) ④·⑤(생 략)	제8조의2(정보보호위원회 운영) ①·②(현행과 같음) ③ ----------. 1. ~ 4.(현행과 같음) 5. 제14조의2제1항의 클라우드컴퓨팅서비스의 이용에 관한 사항 6.(현행 제5호와 같음) ④·⑤(현행과 같음)
제14조의2(클라우드컴퓨팅서비스 이용절차 등) ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다. 1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가 <신 설>	제14조의2(클라우드컴퓨팅서비스 이용절차 등) ① ----------. 1. 다음 각 목의 이용업무---------- 가. 규모, 복잡성 등 클라우드컴퓨팅서비스를 통해 처리되는 업무의 특성 나. 클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중

	단될 경우 미치는 영향 다. 전자적 침해 행위 발생시 고객에게 미치는 영향 라. 여러 업무를 같은 클라우드컴퓨팅서비스 제공자에게 위탁하는 경우 해당 클라우드 컴퓨팅서비스 제공자에 대한 종속 위험 마. 클라우드컴퓨팅서비스 이용에 대한 금융회사 또는 전자금융업자의 내부통제 및 법규 준수 역량 바. 그 밖에 금융감독원장이 정하여 고시하는 사항
2. <별표 2의2>의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가	2. 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 <별표 2의2>의 평가항목 중 필수 항목만 평가할 수 있다.)
3. <별표 2의3>에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수	3. 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획 및 안전성 확보조치의 수립·시행(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 <별표 2의3> 및 <별표 2의4>의 필수 사항만 수립·시행할 수 있다.)

② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.	② ----------제1항 각 호에 따른 평가결과, 업무 연속성 계획 및 안전성 확보조치에 ----------.
③ 금융회사 또는 전자금융업자는 제1항제1호에 따라 다음 각 호의 어느 하나에 해당한다고 평가하는 경우에는 클라우드컴퓨팅서비스를 실제로 이용하려는 날의 7영업일 이전에 금융감독원장이 정하는 양식에 따라 제4항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다. 이 경우 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조 제1항부터 제3항까지의 규정에 따라 보고한 것으로 본다. 1. 고유식별정보 또는 개인신용정보를 처리하는 경우 2. 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 경우	<삭 제>
<신 설>	③ 금융회사 또는 전자금융업자는 제1항제2호의 평가를 직접 수행하거나 제37조의4제1항의 침해사고대응기관이 수행한 평가 결과를 활용할 수 있다.
⑥ 금융회사 또는 전자금융업자는	④ ----------

다음 각 호의 어느 하나에 해당하는 변경사항이 발생한 날로부터 7영업일 이내에 발생 사유, 관련 자료 및 대응계획을 첨부하여 금융감독원장에게 보고하여야 한다.	---------- 사유가 발생한 날로부터 3개월 ---------- ---------- ----------.
<신 설>	1. 클라우드컴퓨팅서비스 이용계약을 신규로 체결하는 경우
1. 클라우드컴퓨팅서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등의 사유로 클라우드컴퓨팅서비스 이용계약에 중대한 변경사항이 발생한 경우	2. ---------- ---------- ---- 등 ---------- ---------- ------
2. (생 략)	3. (현행 제2호와 같음)
3. 제4항제2호 또는 제3호에 관한 중대한 변경사항이 발생한 경우	4. 제1항제2호 ---------- ----------
④ 제3항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.	⑤ 제4항---------- ---------- ----------.
1. (생 략)	1. (현행과 같음)
2. 제1항제1호에 따른 자체 중요도 평가 기준 및 결과	2. ---------- 업무의 중요도 ----------
<신 설>	3. 제1항제2호에 따른 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가 결과
3. 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 안전성 확보 조치에 관한 사항	4. 제1항제3호에 따른 ---------- ---------- ----------

4. (생 략)	5. (현행과 같음)
<신 설>	6. <별표 2의5>의 계약서 주요 기재사항을 포함한 클라우드컴퓨팅서비스 이용계약서
⑤ 클라우드컴퓨팅서비스를 이용하는 금융회사 또는 전자금융업자는 제3항에 따른 보고의무와 관계없이 제4항 각호에 따른 서류를 최신상태로 유지하여야 하며, 금융감독원장의 요청이 있을 경우 이를 지체 없이 제공하여야 한다.	⑥ ---------- ---------- 제4항---------- 제5항 ---------- ---------- ---------- --------.
⑦ 금융감독원장은 제3항 또는 제6항에 따라 제출한 보고 서류가 누락되거나, 중요도 평가 또는 업무연속성계획·안전성 확보조치 등이 충분하지 않다고 판단하는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.	⑦ ---------- 제4항---------- ---------- ---------- ---------- ---------- ---------- ----------.
⑧ 제2항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제	⑧ 제1항---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------

대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.	---------- 고유식별정보 또는 개인신용정보----------. ⑨ (현행과 같음)
⑨ (생 략)	
제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.	제15조(해킹 등 방지대책) ① ----------. 1.·2. (현행과 같음)
1.·2. (생 략)	
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)	3. ----------금지. 다만, 다음 각목의 경우에는 그러하지 아니하다. 가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다)
<신 설>	

<신 설>	나. 업무상 불가피한 경우로서 금융감독원장의 확인을 받은 경우
4. (생 략)	4. (현행과 같음)
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)	5. ----------분리할 것. 다만, 다음 각목의 경우에는 그러하지 아니하다. 가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다) 나. 업무상 불가피한 경우로서 금융감독원장이 인정하는 경우
② ~ ⑥ (생 략)	② ~ ⑥ (현행과 같음)

<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
	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

구분		평가항목	항목	적용 대상
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 서비스 공급망 관리	4.1 공급망 관리정책	4.1.1 공급망과 관련한 보안 요구사항을 정의하는 관리정책을 수립하고 이행하는가?	대체	IaaS, 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

구분		평가항목	항목	적용 대상
		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 알리고 있는가?	필수	IaaS, PaaS, SaaS
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

구분		평가항목	항목	적용 대상
		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 있는가?	필수	IaaS, PaaS, SaaS
		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

구분		평가항목	항목	적용 대상
	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 이용자의 데이터 소유권을 명확하게 확립하고 있는가?	대체	IaaS, 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

구분		평가항목	항목	적용 대상
	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 장비보호	11.2.1 고유식별정보 및 개인신용정보를 처리하는 모든 정보처리시스템을 국내에 설치하고 있는가?	필수	IaaS, PaaS, SaaS
		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

<별표 2의3> <전문개정>

클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획(제14조의2 관련)

금융회사 또는 전자금융업자는 클라우드서비스에 대해 예상치 못한 재해 또는 사고 발생 시 업무 연속성에 미칠 수 있는 영향을 파악하고, 데이터 백업, 재해 복구 및 침해 사고대응 훈련계획, 출구전략 등을 포함한 업무 연속성 계획을 수립하여 이행하여야 한다. 다만, 제14조의2제1항제1호에 따라 중요업무로 분류된 경우 필수 사항과 추가 사항을 모두 준수하여야 하고, 비중요업무로 분류된 경우 필수 사항만을 준수할 수 있다.

1. 데이터 백업 등 장애 대비	필수 사항 (전자금융감독규정상 규율사항)	- 제13조제1항제6호, 제13조제1항제8호내지9호, 제14조제3호내지5호, 제14조제8호, 제15조제2항제6호, 제50조제1항제3호
	추가 사항	- 클라우드서비스와 관련된 중요 설정파일, 가상시스템 이미지 등을 데이터 백업 대상에 포함
2. 이중화 또는 예비장치 확보 등	필수 사항 (전자금융감독규정상 규율사항)	- 제23조제3항, 제23조제7항
	추가 사항	- 클라우드 서비스 제공과 관련된 지리적 특성, 동시 장애 발생 가능성 등을 고려하여 중복 설계 및 구성
3. 훈련 및 사고 관리	필수 사항 (전자금융감독규정상 규율사항)	- 제15조제4항, 제16조제1항제3호, 제16조제2항, 제23조제1항내지6항, 제23조제8항내지10항, 제24조제1항내지4항, 제37조의4제5항
	추가 사항	- 훈련 및 사고관리 계획에 클라우드서비스 제공자의 역할, 책임, 비상연락망 등을 포함
4. 비상대책 수립	필수 사항 (전자금융감독규정상 규율사항)	- 제23조제5항
	추가 사항	- 계약 변경, 파산 등과 같은 중대한 상황 발생에 대비한 공급 대체 방안, 업무 복구 가능성 식별 등 출구전략 수립

<별표 2의4> <신 설>

클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치(제14조의2 관련)

클라우드서비스 관련 보안사고의 예방을 위해 계정관리, 접근통제 등 필수 보안통제가 구현되도록 안전성 확보조치 방안을 수립하여 이행하여야 한다. 다만, 제14조의2제1항제1호에 따라 중요업무로 분류된 경우 필수 사항과 추가 사항을 모두 준수하여야 하고, 비중요업무로 분류된 경우 필수 사항만을 준수할 수 있다.

1.계정관리	필수 사항 (전자금융감독규정상 규율사항)	- 제13조1제1항제1호내지제2호, 제13조제1항제14호, 제13조제2항, 제14조제9호내지제10호, 제17조제1항제2호
	추가 사항	- 클라우드 관리 콘솔에 접근하는 관리자 계정에 대한 이중인증 등 강화된 보안조치 적용
2. 접근통제	필수 사항 (전자금융감독규정상 규율사항)	- 제13조제1항제3호내지제5호, 제13조제1항제12호, 제13조제5항, 제32조제1호, 제32조제2호가목, 제32조제2호다목, 제32조제3호
	추가 사항	- 클라우드시스템 접근 절차를 문서화하고 관리 콘솔 관리자 계정의 경우 별도로 분리된 단말에서만 접근하도록 조치
3. 네트워크 보안	필수 사항 (전자금융감독규정상 규율사항)	- 제15조제1항제3호, 제15조제6항제1호, 제17조제1항제1호, 제18조, 시행세칙 2조의2제1항
	추가 사항	- 시스템간 연계 및 클라우드서비스 내 주요 통신 채널에 대한 암호화 적용
4. 금융회사 등의 내부시스템과 클라우드 시스템 연계	필수 사항 (전자금융감독규정상 규율사항)	- 제12조제1호내지제4호, 제15조제1항제5호, 제34조제1호, 제60조제1항제5호, 시행세칙제2조의2제2항제2호, 시행세칙제2조의2제3항
	추가 사항	- 내부시스템과 클라우드 시스템 간 연계되는 데이터의 식별 및 관리

5. 암호화 및 키 관리	필수 사항 (전자금융감독규정상 규율사항)	- 제31조제1항내지제2항, 제32조제2호, 제33조제1항, 개인정보보호법、신용정보보호법、정보통신망법 등 관계법령에 따른 정보의 저장 및 송수신 시 암호화 조치
	추가 사항	- 클라우드서비스 제공자 등 외부자의 키접근 가능성 등을 고려하여 키의 수명주기별 보안관리 방안 수립
6. 로깅	필수 사항 (전자금융감독규정상 규율사항)	- 제13조제1항제11호, 제13조제4항, 제18조제3호, 제25조
	추가 사항	- 클라우드 관리 콘솔 관리자 등 주요 계정에 대한 활동 내역 로깅 및 주기적 검토
7. 가상 환경 보안	필수 사항 (전자금융감독규정상 규율사항)	- 해당사항 없음
	추가 사항	- 가상 이미지 템플릿을 최신 상태로 유지하고, 이미지 무결성 등 보안사항을 주기적으로 점검
8. 보안 모니터링 및 취약점 분석·평가	필수 사항 (전자금융감독규정상 규율사항)	- 제14조제1호내지제2호, 제14조제6호내지제7호, 제15조제1항제1호내지제2호, 제15조제2항내지제3항, 제16조제1항, 제37조의2
	추가 사항	- 클라우드서비스 내 주요 변경 사항에 대한 실시간 경보 설정 및 모니터링 실시
		- 주요 정보처리시스템의 경우 침해사고 대응기관의 통합보안관제 적용
9. 인적보안	필수 사항 (전자금융감독규정상 규율사항)	- 제8조제1항제2호내지제3호
	추가 사항	- 클라우드서비스 제공자 및 클라우드서비스 운영을 위탁받은 관리형 서비스 제공자 등의 권한과 책임을 식별하고 관리

<별표 2의5> <신 설>

클라우드컴퓨팅서비스 위수탁 계약서 주요 기재사항(제14조의2 관련)

금융회사 또는 전자금융업자가 클라우드컴퓨팅서비스 제공자와 위수탁 계약 체결 시 아래의 사항을 포함하여야 한다. 다만, 제14조의2제1항제1호에 따라 비중요업무로 분류된 경우 기본 사항만을 포함하고, 중요업무로 분류된 경우 기본 사항과 추가 사항을 모두 포함하여야 한다.

가. 기본 포함사항

- 클라우드서비스 이용 대상 업무 및 시스템 개요
- 위탁하는 업무 데이터에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 통보필요 사항
- 감독당국 또는 내외부 감사인의 조사· 접근 수용 의무
- 비상대응훈련, 취약점 분석·평가, 침해사고 대응훈련 등 협조 사항
- 클라우드서비스 제공자의 보안관리 수준 등에 관한 사항
- 정보보호 의무 및 서비스 연속성 보장 등 보안 요구사항
- 서비스에 악영향을 미칠 수 있는 경우 계약 해지 권한 보유
- 서비스 제공 수준(SLA) 모니터링 및 시정조치 권리
- 고객정보보호 및 비밀유지
- 위탁계약 종료 시 데이터 파기
- 관련 법률 준수 및 보고 관련 의무

나. 추가 포함사항

- 금융회사 등이 위탁한 정보처리가 실제 수행되는 위치
- 서비스 제공 중단 시 데이터 접근권한 등 비상대책에 관한 사항
- 위탁업무를 다른 수탁자나 금융회사로 이전할 경우 지원의무 및 전환계획
- 합병·분할, 계약상 지위의 양도, 재위탁 등 중요 상황 발생시 대책
- 재위탁 또는 재위탁의 변경 등 금융회사의 동의가 필요한 사항
- 재위탁 관련 클라우드서비스 제공자의 관리·감독 의무