첨부 1. FAQ

제도화 및 이용자 평가 FAQ

1 금번 "내부업무망 SaaS 이용 제도화(이하 제도화)"가 기존의 규제특례(혁신금융서비스)와 비교할때 이용자 관점(금융회사 등)에서 가장 큰 다른점은?

▶ **금융회사에서 내부업무망에서 SaaS 이용 시 준수해야하는 엄격한 정보보호통제장치 마련은 동일**하나, **해당 정보보호통제항목에 대한 평가를 이용자(금융회사 등)가 자율적으로 평가**하고 그 결과를 정보보호위원회에 보고할 필요 (다만, 기존 혁신금융서비스에서 진행되던 제공자 평가는 동일하게 CSP 안전성 평가 형태(10개 필수항목)로 침해사고대응기관이 담당)

- '금융사들이 손쉽게 클라우드 기반 소프트웨어를 활용하도록 망분리 규제를 개선합니다.
('26.1.19., 금융위원회·금융감독원 보도자료 中 〈개정안 주요내용〉) -

망분리 규제 예외가 허용되는 만큼, 이를 **보완**하기 위한 엄격한 **정보보호통제장치 마련을 의무화**한다. 구체적으로 금융회사는 **▲침해사고 대응기관**(금융보안원 등) **평가를 거친 SaaS를 이용**, **▲접속 단말기**(컴퓨터, 모바일단말 등)에 대해 **보호대책 수립**, **안전한 인증방식 적용**, **최소권한 부여** 등 엄격한 보안관리, **▲중요정보 입력·처리·유출** 여부 **모니터링 및 통제**, ▲SaaS 내 **데이터의 불필요한 공유·처리 방지**나 **허용되지 않은 외부 인터넷 접근 통제**, ▲SaaS 이용 **네트워크 구간 암호화 수립 적용** 등 규율을 마련 운영해야하며
동 **정보보호통제 이행 여부**를 **반기에 1회 평가**하고 금융사 내 **정보보호위원회**(위원장:CISO)**에 보고**하여야 한다.

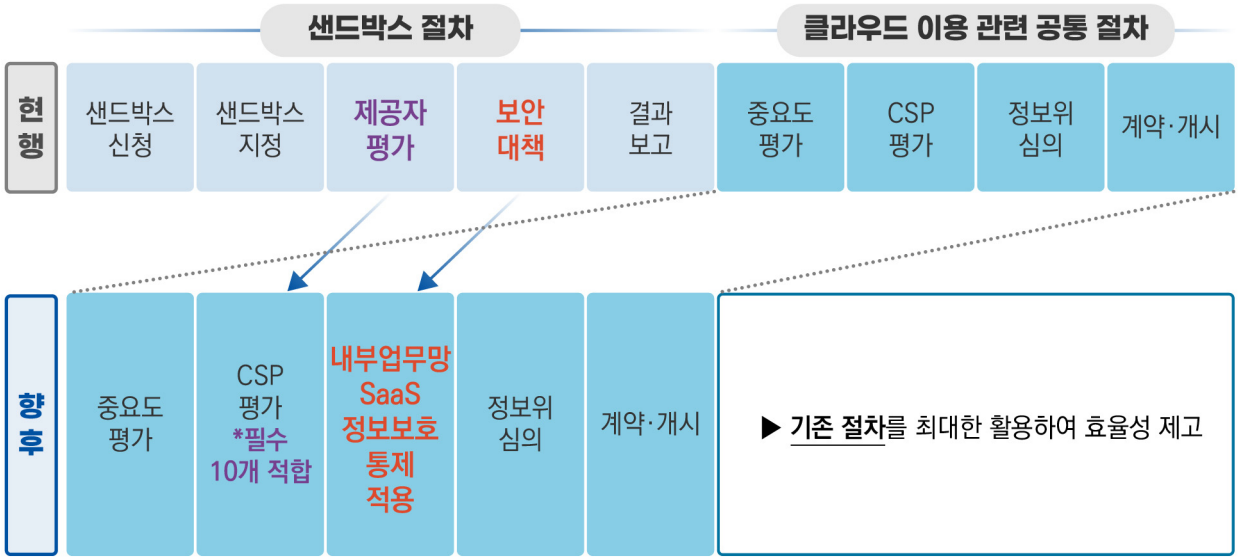
2 금번 제도화 정보보호통제항목이 기존 혁신금융서비스 제공자, 이용자 평가와 구체적으로 다른점이 있다면?

▶ 클라우드 사업자에 대한 평가는 동일하게 침해사고대응기관(금융보안원)이 담당하나, 기존 절차를 최대한 활용하여 평가의 효율성을 제고하기 위해 CSP안전성평가(필수10개 항목)로 일원화하고, 금융회사 별 보안대책은 기존 이용자평가와 거의 유사하나(21개→9개 항목으로 통합조정), "SaaS정보보호 통제를 위한 상시 관리 체계 확보"는 새롭게 추가

※ 샌드박스 부가조건 및 제도화 반영사항

구분	샌드박스 부가조건	제도화 반영사항
제공자 검증	▸CSP 안전성 평가에 더해 **별도 평가**를 추가 수행하고, – **별도 평가결과**가 '**적합**'일 것	▸CSP 안전성 평가로 일원화 – 필수항목 **평가결과**가 **'적합'**일 것
이용자 검증	▸ **별도 '보안대책'** 수립·이행(**21개** 항목)	▸**핵심내용** 반영(**9개** 항목)

※ 업무절차 비교



3 금번 제도화 이후 SaaS를 내부업무망에서 이용 시, 개정 감독규정시행세칙 제2조의3제4항에 따른 정보보호통제를 수행하기만 하면, 감독규정 제14조의2에 따른 이용보고(CSP 안전성 평가 등)는 별도로 필요 없는지?

▶ **필요함.** 개정 감독규정시행세칙 제2조의3제4항에 따른 정보보호통제 항목은 내부업무망에서 SaaS 이용 시 추가로 필요한 보호조치로서, 클라우드를 이용하는 금융기관 등은 내부업무망 이용과 무관하게 클라우드서비스에 대한 이용보고가 필요. 다만, 기존 제공자평가가 CSP 안전성 평가(필수10개)와 통합됨에 따라 처리 효율성이 제고되는 측면

4 금번 제도화 이후 기존 혁신금융서비스 지정 및 업무 개시한 SaaS는 모두 시행세칙 개정(안)의 '망분리 적용 예외'로 인정되는지? 이 경우, 혁신금융서비스 지정 공고문에 따라 반기 1회 이행 여부 보고 대상도 변경되는 것인지?

▶ 기존 혁신금융서비스로 지정 및 부가조건을 모두 준수하여 업무개시를 보고한 건에 한하여 지속 이용 가능하며, 보안대책의 이행 여부는 시행세칙 개정(안)에 따라 정보보호위원회에 보고하는 것으로 변경 적용

5 전자금융감독규정 시행세칙 제2조의3(망분리 적용 예외) ④항의 '정보보호통제'와 관련하여 별도의 가이드가 있는지?

▶ 금융보안원에서 「내부업무망 SaaS망분리 예외 적용에 따른 보안해설서」를 배포할 예정

6 금번 제도화 시 내부업무망에서 이용하는 SaaS는 모두 시행세칙 개정(안)의 '망분리 적용 예외'에 인정되는지?

▶ 내부업무망에서 SaaS를 이용하여 가명정보를 처리하는 경우에는 망분리 예외로 인정되지 않으며, 기존과 같이 혁신금융서비스 신청이 필요

7 내부업무망에 도입한 SaaS를 이용하여 외부 서비스를 연계해도 되는지? (예: 웹 검색, 외부 SaaS 연동 등)

▶ 내부업무망에서 SaaS를 사용하는 것은 망분리 예외를 인정받는 것이지, 망분리 원칙 자체를 폐기한 것이 아님. 따라서, 내부업무망에 도입한 SaaS는 승인된 업무 목적으로만 사용되어야 하며, 해당 SaaS를 통해 외부 인터넷이나 다른 서비스로 확장하는 행위는 엄격히 제한됨

8 내부업무망에 도입한 SaaS A와 B를 서로 연계하는 것은 가능한지? (예: 보안SaaS 알람을 협업SaaS로 전송 등)

▶ 내부업무망에 도입한 SaaS가 모두 전자금융감독규정 시행세칙 제2조의3을 준수한 경우에만 상호 연동 가능

제공자 평가 FAQ

9 금번 제도화 시 '개정 시행세칙 [별표7]'에 따르면 "침해사고대응기관의 평가결과 '충족'을 획득한 SaaS를 이용하고 관련서류를 최신 상태로 유지"라고 되어 있는데 여기서 관련서류는 무엇이고 최신과 관련된 기한은 어느정도 인지?

▶ 관련서류는 침해사고대응기관인 금융보안원의 **'SaaS 제공자 평가 현황 목록**(평가결과 '충족' 여부 포함)' 및 이용하고자 하는 SaaS 제공자**에 대한 침해사고대응기관의 'CSP 안전성 평가결과**(전자금융감독규정 〈별표2의2 중, SaaS 및 필수 항목)'를 말하며, 유효기간이 만료된 목록 및 평가결과는 최신으로 인정받을 수 없음

10 침해사고대응기관인 금융보안원이 SaaS 제공자 평가와 관련하여 제공하는 구체적인 정보는?

▶ 금융보안원은 **"SaaS 제공자 평가 현황 목록"**을 레그테크포털 및 CSP 안전성 평가 통합지원 시스템에 공개하며, 금융회사 및 전자금융업자는 이를통해 각 SaaS의 평가결과가 '충족'인지 확인 가능. 단, 각 SaaS에 대한 세부 평가내용까지 확인이 필요한 경우에는 CSP 안전성 평가 통합지원시스템에서 요청 필요

11 침해사고대응기관이 SaaS 제공자 평가와 관련하여 제공하는 "충족"리스트에 특정금융회사 등이 도입하려는 SaaS 제공자가 없는 경우에는 서비스를 도입할 수 없는지?

▶ "충족" 목록에 없는 SaaS 제공자는 **평가가 수행되지 않았거나** 평가 결과 **"충족"을 얻지 못한 경우**이므로, **CSP 안전성 평가 통합지원시스템에서 평가 세부내용(평가 여부 및 결과) 확인 필요**. 평가가 **수행되지 않은 SaaS 건**은 **금융회사의 수요*에 따라** CSP의 평가일정 등을 고려하여 침해사고대응기관에서 **순차적으로 평가 실시**

* 금융보안원은 주기적으로 금융회사 및 전자금융업자 대상으로 수요조사 실시 예정

12 특정 SaaS를 내부망에서 이용하기 위해 혁신금융서비스로 지정받아 침해사고 대응기관의 제공자 평가결과를 이미 획득한 바 있는데, 금번 제도화 이후에도 침해사고 대응기관에 동일하게 특정 SaaS의 평가를 의뢰해야 하는것인지?

▶ 이미 평가 완료된 SaaS 제공자 평가 결과는 제도화 이후에도 유효한 것으로 인정(SaaS 제공자 평가 현황 목록에서 확인 가능). 단, 최신 평가결과가 나오는 경우 이전 평가결과는 만료되므로 최신화 유지 필요

13 침해사고대응기관이 "충족"으로 평가한 SaaS 제공자를 금융회사 등이 도입·이용중인 상황에서, 최근의 추가 평가과정에서 "충족" 평가를 받지 못하게 되면 그 즉시 해당 SaaS 이용이 중지 되는지?

▶ 도입 당시의 평가 결과는 '충족'이었으나 이후 평가에서 '충족'이 아니게 된 경우, 즉시 서비스를 중지하여야 하나 자체 보안대책 마련 및 계약 관계 등을 고려하여 **최대 차년도 말까지 유예 가능**. **침해사고대응기관의 차년도 평가 결과**에서 '충족'을 다시 받는다면 서비스 재계약 및 지속 이용이 가능하나, **'충족'을 받지 못한다면 해당 SaaS는 더 이상 이용 불가**

[참고]

① 평가결과 "충족"일 경우 금융회사 도입가능

② 평가결과 "충족"이 아닌 경우 금융회사 신규 도입 불가

③ 금융회사 이용 중, 최신 제공자 평가결과가 "충족"이 아니게 된 경우

- 차년도말까지 유예가능하며, 차년도 마지막 평가결과까지 "충족"이 아닐 경우 이용 지속 불가

예시) A금융회사가 M365 **'26.1월 업무개시** 후 **'26.7월 M365 평가결과 충족이 아닐 경우 '27년말까지 이용가능**
하지만 **'27년말까지 M365 평가결과가 "충족"으로 되지 않는 경우에는 '28년부터 M365 이용 불가**

첨부 2. CSP 안전성 대표평가 평가항목(필수, SaaS)

▶ 〈별표2의2〉 SaaS 적용 필수항목 12개 중, 2개 제외*

* 11.1.2., 11.2.1. 평가 항목은 고유식별정보 및 개인신용정보 처리와 관련한 항목으로 평가범위에서 제외

구분		평가항목
1. 정보보호 정책 및 법규 준수	1.3. 법 및 정책 준수	1.3.1. 이용자가 법령 등 의무준수를 위해 필요한 사항을 지원 및 협조하도록 체계가 마련되어있는가?
	1.4. 보안 감사	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 모니터링되고, 비인가 된 접근 및 변조로부터 보호되고 있는가?.
5. 업무연속성 계획 및 재해복구	5.1. 장애대응	5.1.2. 클라우드서비스 중단이나 피해가 발생한 경우 장애보고 절차에 따라 장애상황을 기록하고 이용자에게 현황을 파악할 수 있도록 관련 정보를 제공하는가?
	5.2. 서비스 가용성	5.2.1. 가상화 서버, 설비 등 정보처리설비의 장애로 인해 서비스가 중단되지 않도록 관련 설비를 이중화하고, 백업 체계를 마련하고 이행하는가?
6. 침해사고 대응 및 관리	6.2. 침해사고 대응	6.2.1. 침해사고 발생 시 침해사고 대응절차에 따라 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알리고 있는가?
7. 사용자 인증 및 접근통제	7.2. 접근권한 관리	7.2.2. 이용자의 정보처리시스템과 관련된 단말기 및 전산자료에 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련하고 적용하고 있는가?
8. 가상화 및 인프라 보안	8.1. 가상화 보안	8.1.2. 이용자가 클라우드서비스 이용 중 가상자원을 삭제 할 경우 삭제대상과 관련된 모든 자원이 복구되지 않는 방법으로 삭제되는가? * 가상머신(이미지, 백업, 스냅샷 등), 가상 스토리지, 가상 소프트웨어, 가상환경 설정 정보 등
		8.1.3. 가상자원에 대한 무결성을 보장하고 가상자원 손상 시 이용자에게 안내하고 있는가?
		8.1.5. 가상자원 관리 시스템*과 가상 소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 관리적, 물리적, 기술적 보호대책을 수립·이행하고 있는가? * 가상자원을 제공하기 위한 웹사이트(클라우드 포탈, 클라우드 콘솔, API 등)
10. 암호화 및 데이터 보호	10.1. 데이터 보호	10.1.6. 이용자의 클라우드서비스 이용 계약 종료 시 이용자의 모든 가상자원은 복구가 불가능하도록 삭제하고 있는가?
11. 물리적 보안	11.1. 물리적 보호구역	11.1.2. 고유식별정보 및 개인신용정보 처리 시 전산실 내 무선통신망 사용을 제한(통제) 하고 있는가?
	11.2. 정보처리 시설 및 장비보호	11.2.1. 고유식별정보 및 개인신용정보를 처리하는 모든 정보처리시스템을 국내에 설치하고 있는가?