AGR-VII-2019-②-83

금융분야 클라우드컴퓨팅서비스 이용 가이드

2019. 1.

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

CONTENTS

제 1 장 가이드 개요 ····· 1

1. 목적 ····· 2
2. 구성 ····· 3
3. 활용 ····· 3
4. 용어 ····· 4

제 2 장 클라우드서비스 이용 절차 ·· 7

1. 사전 준비 (제3~5장) ····· 9
2. 계약 체결 (제6장) ····· 11
3. 보고 및 이용 (제7장) ····· 11
4. 이용 종료 (제8장) ····· 12

제 3 장 업무 선정 및 평가 ····· 13

1. 이용대상 선정 ····· 14
2. 중요도 평가 실시 ····· 15

제 4 장 계획 수립 ····· 19

1. 업무 연속성 계획 수립 ····· 21
2. 출구 전략 수립 (업무 연속성 계획에 포함) ··· 26
3. 안전성 확보조치 방안 수립 ····· 30
4. 업무 위수탁 운영기준 마련 ····· 44

제 5 장 계약 준비 ····· 47

1. 클라우드서비스 제공자 평가 ····· 48
2. 정보보호위원회 심의·의결 ····· 51

제 6 장 계약 체결 ····· 53

1. 서비스 위탁 관련 명시사항 ····· 56
2. 보안 관련 명시사항 ····· 67
3. 출구 전략 이행을 위한 명시사항 ····· 70
4. 책임관계 명확화 ····· 72

제 7 장 보고 및 이용 ····· 75

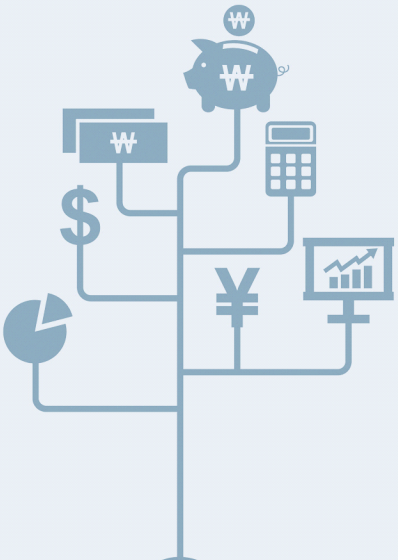
1. 서류 구비 및 사전 보고 ····· 76
2. 서류 최신성 유지 및 수시 보고 ····· 78
3. 리스크 관리 ····· 81

제 8 장 이용 종료 ····· 83

첨 부 ····· 85
1. 클라우드서비스 이용 관련 감독규정 주요 개정 내용 ····· 86
2. 해외 금융권 클라우드서비스 규제 사례 ····· 88
3. 전자금융감독규정 시행세칙의 망분리 대체 정보보호통제 수칙 ····· 89
4. 클라우드서비스 이용 가이드 관련 FAQ ····· 90

부 록 **금융분야 클라우드컴퓨팅서비스 제공기준 ····· 93**
1. 평가 대상 ····· 94
2. 평가 절차 및 방법 ····· 95
3. 평가항목 기준 ····· 100

별 첨 **금융분야 클라우드컴퓨팅서비스 이용 관련 참고자료 ····· 115**
1. 전자금융감독규정 개정.시행 보도자료 (금융위원회, '19.12.7.) ····· 117
2. 관련 규정 ····· 129



금융분야
클라우드컴퓨팅서비스
이용 가이드

제 1 장

가이드 개요

1. 목적
2. 구성
3. 활용
4. 용어

제 1 장 가이드 개요

1 목적

이 가이드는 금융회사 또는 전자금융업자(이하 '금융회사')가 「전자금융감독규정」(이하 '감독규정') 제14조의2에 따라 클라우드컴퓨팅서비스(이하 '클라우드서비스')를 이용하고자 할 경우 요구되는 세부절차를 안내하고 금융시스템 안전성 및 금융소비자 보호를 위해 필요한 보안사항을 권고하는 것을 목적으로 한다.

〈금융분야 클라우드서비스 이용 관련 기본 방향〉

□ **금융회사의 클라우드서비스 이용**은 「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조 제5항 및 제6항에 따라 정보처리 위탁에 해당하며,
ㅇ 「자본시장법」 제42조 및 「금융기관의 업무위탁 등에 관한 규정」 제3조에 따른 업무위탁에 해당됨
※ 클라우드서비스 이용은 정보를 제공하는 것이 아닌, 위탁 처리 하는 것임

□ 전자금융업무와 관련된 정보처리시스템을 위탁할 경우 **클라우드서비스 제공자**는 감독규정 제3조제3호 또는 제4호에 따라 **전자금융보조업자**에 해당

□ 클라우드서비스를 이용한다고 해서 금융회사의 **책임이 면제되는 것이 아니며**, 고객 손해 발생 시 금융회사가 **1차적 손해배상 책임의 주체**이고, 클라우드 제공자는 수탁자로서 **연대배상책임을 부담**

◆ 클라우드는 아웃소싱의 하나로 「정보처리 업무위탁」에 해당

◆ 클라우드서비스 제공자는 「전자금융보조업자」로서 제한적으로 감독을 받음

- **보조업자의 책임** : 클라우드 서비스 제공자의 고의·과실은 **금융회사의 고의 · 과실로 간주**
- **금융회사 준수사항** : 보안 · 비상 · 백업대책 등을 수립·운영하고 보안점검을 실시해야 함
- **감독 · 검사** : 금융회사의 정보처리업무 위탁계약 시정 · 보완 요구권(법 제40조제2항), 보조업자에 대한 수탁계약서 · 부속자료 등의 제출요구권 보유(법 제40조제3항,4항,5항)

2 구성

이 가이드는 본문(제2장~제8장)과 부록으로 구성되어 있다.

본문에서는 금융회사가 클라우드서비스 이용 시 준수해야 할 절차, 기타 보안대책 등을 단계적으로 설명하고 있으며, 부록에서는 금융회사가 감독규정 제14조의2제1항제2호에 따라 클라우드서비스 제공자의 건전성 및 안전성을 평가하기 위해 필요한 세부기준을 제시한다.

3 활용

① 이 가이드는 감독규정('19.1.1. 시행) 제14조의2(클라우드서비스 이용절차 등)의 준수를 위해 활용할 수 있다.

※ 이 가이드는 상용 클라우드서비스 이용에 대한 것으로, 금융회사 또는 지주사 내에서 감독규정 제11조제11호 및 제12호, 제15조제1항제5호를 준수하면서 非상용 프라이빗 클라우드서비스 등을 활용하는 경우는 이 가이드의 적용 대상이 아님

② 이 가이드는 금융회사가 클라우드서비스를 이용함에 있어 적절한 보안대책*을 수립·운영하기 위해 활용할 수 있다.

* 단, 개별 금융회사 또는 업무 특성에 따라 보안대책의 적용 여부는 금융회사가 최종적으로 판단하여야 함

③ 이 가이드에 포함되지 않거나 중복되는 내용이 있는 경우 「전자금융거래법」, 「신용정보의 이용 및 보호에 관한 법률」, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」, 「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「금융기관의 업무위탁 등에 관한 규정」, 「금융회사의 정보처리 업무 위탁에 관한 규정」 등 관련 법령과 그 하위규정을 우선하여 적용한다.

4 용어

이 가이드에서 사용되는 용어는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조 및 감독규정 제2조의 정의를 따른다.

▶ 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "클라우드컴퓨팅"(Cloud Computing)이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 "정보통신자원"이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
2. "클라우드컴퓨팅기술"이란 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술로서 가상화 기술, 분산처리 기술 등 대통령령으로 정하는 것을 말한다.
3. "클라우드컴퓨팅서비스"란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.
4. "이용자 정보"란 클라우드컴퓨팅서비스 이용자(이하 "이용자"라 한다)가 클라우드컴퓨팅서비스를 이용하여 클라우드컴퓨팅서비스를 제공하는 자(이하 "클라우드컴퓨팅서비스 제공자"라 한다)의 정보통신자원에 저장하는 정보(「국가정보화 기본법」 제3조제1호에 따른 정보를 말한다)로서 이용자가 소유 또는 관리하는 정보를 말한다.

▶ 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령

제2조(클라우드컴퓨팅기술) 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 "법"이라 한다) 제2조제2호에서 "대통령령으로 정하는 것"이란 다음 각 호의 어느 하나에 해당하는 기술을 말한다.

1. 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 "정보통신자원"이라 한다)을 가상으로 결합하거나 분할하여 사용하게 하는 기술
2. 대량의 정보를 복수의 정보통신자원으로 분산하여 처리하는 기술
3. 그 밖에 정보통신자원의 배치와 관리 등을 자동화하는 기술 등 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신자원을 활용하는 기술

제3조(클라우드컴퓨팅서비스) 법 제2조제3호에서 "대통령령으로 정하는 것"이란 다음 각 호의 어느 하나에 해당하는 서비스를 말한다.

1. 서버, 저장장치, 네트워크 등을 제공하는 서비스
2. 응용프로그램 등 소프트웨어를 제공하는 서비스
3. 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스
4. 그 밖에 제1호부터 제3호까지의 서비스를 둘 이상 복합하는 서비스

▶ 감독규정

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "전산실"이라 함은 전산장비, 통신 및 보안장비, 전산자료 보관 및 출력장비가 설치된 장소를 말한다.

2. "전산자료"라 함은 전산장비에 의해 입력·보관·출력되어 있는 자료를 말하며 그 자료가 입력·출력되어 있는 자기테이프, 디스크, 디스켓, 콤팩트디스크(CD) 등 보조기억매체를 포함한다.
3. "정보처리시스템"이라 함은 전자금융업무를 포함하여 정보기술부문에 사용되는 하드웨어(hardware)와 소프트웨어(software)를 말하며 관련 장비를 포함한다.
4. "정보기술부문"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 정보를 수집·가공·저장·검색·송신 또는 수신을 행하는 금융회사 또는 전자금융업자의 업무, 인력, 시설 및 조직을 말한다.
5. "정보보호" 또는 "정보보안"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 수집·가공·저장·검색·송신 또는 수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 기술적·물리적·관리적 수단을 강구하는 일체의 행위를 말하며 사이버안전을 포함한다.
6. "정보보호시스템"이라 함은 정보처리시스템 내 정보를 유출·위변조·훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램을 말한다.
7. "해킹"이라 함은 접근을 허가받지 아니하고 전자금융기반시설에 불법적으로 침투하거나 허가받지 아니한 권한을 불법적으로 갖는 행위 또는 전자금융기반시설을 공격하거나 해를 끼치는 행위를 말한다.
8. "컴퓨터악성코드"(이하 "악성코드"라 한다)라 함은 컴퓨터에서 이용자의 허락 없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 이용자에게 피해를 주는 프로그램을 말한다.
9. "공개용 웹서버"라 함은 인터넷 이용자들이 웹페이지를 자유롭게 보고 웹서비스(월드 와이드 웹을 이용한 서비스를 말한다)를 이용할 수 있게 해주는 프로그램이 실행되는 장치를 말한다.
10. "정보통신망"(이하 "통신망"이라 한다)이라 함은 유·무선, 광선 등 정보통신 수단에 의하여 부호·문자·음향·영상 등을 처리·저장 및 송·수신할 수 있는 정보통신 조직형태를 말한다.
11. 삭제

금융분야
클라우드컴퓨팅서비스
이용 가이드

제2장

클라우드서비스 이용 절차

1. 사전 준비 (제3~5장)
2. 계약 체결 (제6장)
3. 보고 및 이용 (제7장)
4. 이용 종료 (제8장)

제 2 장 클라우드서비스 이용 절차

금융회사는 클라우드서비스 이용 시 다음 절차에 따라 필요한 조치를 수행함으로써 감독규정 제14조의2(클라우드서비스 이용 절차)를 준수하고 적절한 보안수준을 확보하여야 한다.

※ 개정된 감독규정의 시행('19.1.1.) 이전 비중요 정보처리시스템 지정을 통해 클라우드서비스를 이용 중인 경우 감독규정 상 의무가 일부 배제되나(감독규정 부칙 제2조) 보안수준 확보를 위해 동 절차를 참고할 수 있다.

〈클라우드서비스 이용 절차도〉

단계	필요 조치	지원 및 보고
사전 준비	• 이용 대상 선정 및 중요도 평가 • 업무연속성 계획 및 안전성확보조치 방안 수립 • 업무 위수탁 운영기준 보완 • 제공자 후보 선정 및 평가 • 정보보호위원회 심의·의결	제공자 평가 지원 ← 금융보안원
계약 체결	• 클라우드서비스 이용 계약 체결	
보고 및 이용	• 서류 구비 및 사전 보고 • 서류 최신성 유지 및 수시 보고	사전·수시보고 → 금융감독원 ← 검사 실시 등
이용 종료	• 출구 전략 이행	

※ 각 단계별 세부사항은 제3장부터 제8장까지 내용 참조

1 사전 준비 (제3~5장)

1) 업무 선정 및 평가 (제3장)

가. 이용 대상 정보처리업무 선정

- 금융회사는 정보처리 업무 중 정보처리의 규모, 클라우드서비스 이용에 따른 비용절감, 업무 효율성 증가 등을 종합적으로 검토하여 클라우드서비스 이용 여부를 결정하여야 한다.

나. 이용 대상 정보처리업무 중요도 평가

- 금융회사는 해당 업무가 취급하는 정보의 중요도*, 클라우드서비스 이용이 전자금융거래의 안전성 및 신뢰성에 미치는 영향 등을 바탕으로 중요도 평가를 수행하여야 한다.

  * 중요정보(고유식별정보 또는 개인신용정보)의 포함 여부 등

2) 계획 수립 (제4장)

가. 업무연속성 계획 및 안전성 확보조치 방안 수립

- 금융회사는 클라우드서비스 이용에 따른 업무연속성 계획, 안전성 확보조치 방안 등을 수립하여야 한다.
  - 특히, 업무연속성 계획에는 금융회사의 클라우드서비스 이용 중단 또는 종료 시 데이터의 반환 및 파기 절차, 위탁계약의 종료, 중단, 변경 시 데이터 반환·파기에 관한 사항 등(이하 '출구 전략')이 반영되어야 한다.

나. 업무 위수탁 기준 보완 (클라우드서비스 이용관련)

- 금융회사는 중요도가 높은 업무의 위탁을 추진하는 경우 감독규정 별표 2의3(업무위탁 운영기준 보완사항)의 내용을 내부 『업무 위수탁 기준*』에 반영하고 준수하여야 한다.

  * 클라우드서비스 이용은 업무위탁에 해당하므로 「자본시장법」 제42조제7항에 따른 『업무위탁 운영기준』 또는 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따른 『업무 위수탁 기준』 등도 준수 필요

3) 계약 준비 (제5장)

가. 클라우드서비스 제공자의 건전성·안전성 등 평가

- 금융회사는 계약 준비단계에서 클라우드서비스 제공자의 건전성 및 안전성을 평가하여야 하며,

  ※ 「[부록] 금융분야 클라우드컴퓨팅서비스 제공기준」 참고

  - 평가결과에 따라 보완조치를 요구하거나 다른 클라우드서비스 제공자를 대상으로 신규 평가 실시 등을 추진할 수 있다.

  ※ 평가결과의 수용 및 계약 추진 여부에 대한 판단 기준은 금융회사가 자율적으로 정함

나. 정보보호위원회 심의·의결

- 금융회사는 업무추진 과정의 객관성·공정성 제고, 책임인식 강화를 위해 다음 사항을 정보보호위원회에서 심의·의결하여야 한다.
  - 자사 정보처리업무의 중요도 평가결과
  - 클라우드서비스 제공자의 건전성·안전성 등 평가결과
  - 자체 업무 위수탁 운영기준

2 계약 체결 (제6장)

가. 클라우드서비스 이용 계약 체결

- 금융회사는 클라우드서비스 이용 계약 체결 시 감독규정 별표2의3 중 '위수탁 계약서 주요 기재사항'을 반영하여야 한다.
  - 특히, 데이터 처리 위치, 훈련(비상대응, 침해사고대응) 및 취약점 분석 평가 등에 대한 협조, 위탁업무의 이전·반환 등에 관한 사항이 누락되지 않도록 하고,
  - 금융회사의 클라우드서비스 이용 관련 금융당국 검사·감독이 원활하게 수행될 수 있도록 금융당국의 조사·접근(데이터센터 등 현장방문 포함)에 협조할 의무를 반드시 명시하여야 한다.

3 보고 및 이용 (제7장)

가. 관련 서류 구비 및 금융당국 보고

- 클라우드서비스를 이용하고자 하는 모든 금융회사는 클라우드서비스 이용과 관련하여 다음의 서류를 구비하여야 한다.
  - 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 각 호의 서류
  - 이용 대상 정보처리업무의 중요도 평가 기준 및 결과
  - 클라우드서비스 이용 관련 업무연속성 계획 및 안전성 확보조치
  - 클라우드서비스 이용 관련 정보보호위원회 심의·의결 결과
- 특히, 「이용 대상 정보처리업무 중요도 평가」 결과 중요도가 높은 업무에 대해서는 클라우드서비스를 실제 이용하려는 날의 7영업일 이전에 금융감독원장에게 상기 서류를 보고하여야 한다.

나. 서류 최신성 유지 및 수시 보고

- 금융회사는 클라우드서비스 이용 관련 서류를 최신 상태로 유지하고, 금융감독원장 요청 시 지체 없이 제공하여야 한다.

  * 관련 서류의 최신성 유지 의무는 금융감독원장 보고 의무와 관계없이 모든 정보처리업무의 클라우드서비스 이용에 적용

- 금융회사는 다음의 변경사항이 발생하는 경우, 발생일로부터 7영업일 이내에 발생 사유, 관련 자료 및 대응계획을 포함하여 금융감독원장에게 보고하여야 한다.
  - 클라우드서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등의 사유로 클라우드서비스 이용 계약에 중대한 변경사항이 발생한 경우
  - 클라우드서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 아니한 경우
  - 이용 대상 정보처리업무의 중요도 평가 기준·결과, 업무연속성 계획 및 안전성 확보조치에 관한 중대한 변경사항이 발생한 경우

다. 리스크 관리

- 금융회사는 클라우드서비스 이용 시 사전에 수립한 업무연속성 계획 및 안전성 확보조치 등을 준수하여 리스크를 관리하고, 필요 시 클라우드서비스 제공자에게 협조를 요청하여야 한다.

4 이용 종료 (제8장)

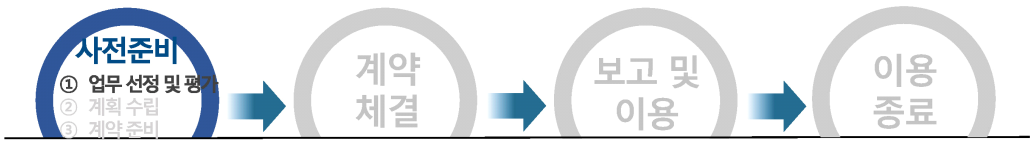
- 금융회사는 클라우드서비스 이용이 종료(업무 장애·지연 등으로 인한 일시적 서비스 이전 등 포함)되는 경우 사전 수립된 출구 전략에 따라 적절한 조치를 취해야 한다.

제3장

업무 선정 및 평가

1. 이용대상 선정
2. 중요도 평가 실시

제 3 장 업무 선정 및 평가



- ✔ 이용 대상 업무 선정 기준 제시
- ✔ 업무 중요도 평가 기준 제시

1 이용대상 선정

- 금융회사는 정보처리업무 중 클라우드서비스 이용에 따른 효율성 등을 감안하여 이용대상을 선정하여야 한다.
  - 다음의 예시와 같이 자체 시스템 구축에 비하여 클라우드서비스 이용이 유리하다고 판단되는 경우 클라우드서비스 이용을 적극 고려할 수 있다.

> ① AI, 빅데이터 등 신기술 활용으로 대량의 컴퓨팅 자원이 단기간에 요구되는 경우
> ② 신규 또는 파일럿 서비스를 구축하여야 하나, 시스템 사용량 규모에 대한 사전 예측이 어려운 경우
> ③ 시스템 사용량의 변동이 매우 큰 서비스인 경우
> ④ 짧은 시간 안에 구축이 필요하거나 기술 변화에 대한 민첩한 대응이 요구되는 경우
> ⑤ 사전 테스트 등 임시적으로 대용량의 시스템이 필요한 경우
> ⑥ 클라우드서비스 도입 또는 전환에 필요한 초기 투자비용보다 클라우드서비스 이용에 따른 운영비용 절감이 더 크다고 판단되는 경우
> ⑦ 자체 시스템을 안전하게 보유·운영할 역량이 부족하나, 내부 운영 인력 등이 클라우드서비스 이용에 필요한 역량을 충분히 갖추고 있는 경우
> ⑧ 기타 금융회사의 전략 이행을 위해 필요하다고 판단되는 경우

- 그러나, 금융회사의 핵심 업무 수행을 위한 정보처리에 대해서는 효율성 이외에도 업무 중요도, 취급 정보의 민감도, 경영전략 등 다양한 요소를 종합적으로 고려해야 한다.

2 중요도 평가 실시

금융회사는 개별 업무 특성과 다음 사항을 고려하여 자체적으로 중요도 평가 기준을 수립하고, 클라우드서비스 이용 대상 업무에 대해 중요도 평가를 실시하여야 한다.

> ▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**
> 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**

가. 고유식별정보* 또는 개인신용정보** 처리 시 중요 업무로 취급

* 개인정보보호법 제24조제1항에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 면허번호, 외국인등록번호 등이 해당

** 「신용정보의 이용 및 보호에 관한 법률」 제2조제2호에 따라 신용정보 중 개인의 신용도와 신용거래능력을 판단할때 필요한 정보

※ 다만, 전자금융거래와 관련이 없고 고객정보와 무관한 정보 처리 시 해당되지 않음 (예, 내부직원 정보)

나. 고유식별정보 또는 개인신용정보를 직접 처리하지 않는 경우에도 아래 사항을 고려하여 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미칠 경우 중요 업무로 취급

① 처리 정보의 중요도 및 정보 위·변조·유출 시 금융회사 및 금융소비자에 미칠 수 있는 영향

② 업무 중단 발생 시 주요 금융 기능 이행 및 운영·법적·평판 리스크에 미치는 영향

③ 업무 중단이 금융회사의 수익 및 운영 비용에 미치는 영향

④ 사고 또는 장애 발생 시 타 시스템의 업무 연속성 저해 수준 등 타 시스템과의 연계성

⑤ 복구 목표시간 등 해당 정보처리시스템의 업무 중요도

⑥ 운영, 개발, 테스트 시스템 등 정보처리시스템의 용도

⑦ 고객 또는 사내직원 등 이용자 유형에 따른 해당 정보처리시스템 이용자 수 등

참고 주요국 금융권 지침 내 업무 중요도 평가 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 - 4.1 중요도 평가

1) 금융회사(위탁 기관)는 업무 위탁 전 대상 업무를 평가하여 중요 업무를 선별해야 한다. 금융회사는 CEBS 지침의 가이드라인 1 (f)에 근거하여 업무의 중요성 평가를 수행해야하며 특히 클라우드서비스 제공 업체에 대한 위탁과 관련하여 다음 사항을 모두 고려해야한다.
   (a) 위탁하는 업무의 중요성 및 내재한 위험 프로파일(즉, 금융회사의 비즈니스 연속성과 고객에 대한 의무에 있어 중요한/결정적인 업무)
   (b) 중단으로 인한 직접적인 운영 영향 및 법적 위험과 평판 위험
   (c) 업무 방해가 금융회사의 수익에 미칠 수 있는 영향
   (d) 기밀성 훼손 또는 데이터 무결성 위배가 금융회사 및 고객에게 미칠 수 있는 잠재적 영향

2. (미국-FFIEC) 아웃소싱 클라우드 컴퓨팅 - 2. 상당한 주의(Due Diligence) 中

금융 기관이 전략 계획을 달성하기 위해 제3자를 사용한다고 해서 제3자 활동이 안전하고 건전한 방식으로, 그리고 관련 법률 및 규정을 준수하여 수행되는지 확인하는 이사회 및 경영진의 책임이 줄어들지 않는다. 클라우드서비스 공급자에게 아웃소싱 하는 것은 비용 절감, 유연성, 확장성, 향상된 부하 균형 조정 및 속도와 같은 잠재적인 이점 때문에 금융 기관에 유리할 수 있다. 중요한 기능의 위탁을 승인하기 전에, 이러한 조치가 이사회 및 고위 경영진이 승인한 해당 기관의 전략 계획 및 회사 목표와 일치하는지 확인하는 것이 중요하다.

3. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 3.6

(3.6) 다른 유형의 기업은 다른 요구사항을 적용해야 하며, 이는 위탁하는 기능의 유형에 따라 결정될 수 있다. 위탁하는 기능이 심각한(critical or important) 것인지, 중요 위탁(material outsourcing)에 해당하는지 여부가 특히 관련이 있으며, 공인 지불 기관 및 공인 전자 화폐 기관의 경우 기관이 중요 운영 기능(important operational functions)과 관련이 있는지 여부가 특히 관련 있다. 이러한 용어는 위탁과 관련된 용어이며 다음과 같은 핸드북 또는 규정에 정의되어 있다.

- Critical or important - 업무 수행상의 결함이나 실패로 인해 공식 인가, 규제 시스템에 따른 기타 의무, 재무 실적에 관한 기업의 조건 및 의무 또는 관련 서비스 및 업무의 건전성 연속성에 큰 영향을 미치는 경우 해당 기능은 중대하거나 중요하다고 간주한다(고위 관리자 배치 및 시스템 통제 Senior Management Arrangements, Systems and Controls (SYSC 8.1.4R). MiFID 조직 규정의 제 30조에 비슷한 정의가 있다.
- Material outsourcing - FCA 안내서에 정의된 바와 같이 서비스의 취약점 또는 실패 시 기업이 임계 조건을 만족할 수 없거나 기업 원칙을 준수할 수 없을 정도로 중요한 위탁 서비스를 말한다.
- 중요 운영 기능(Important operational functions) - 2011년 전자 화폐 규칙(Electronic Money Regulations 2011) 및 2017년 지불 서비스 규정(Payment Services Regulations 2017)에 따라, 업무 수행상의 결함이나 실패로 인해 다음 사항에 심각한 영향을 미친다면 해당 기능이 중요하다고 여겨진다.
  (a) 공인 기관의 규정 및 공식 허가 요구사항에 대한 컴플라이언스
  (b) 공인 기관의 재무 실적
  (c) 공인 기관의 건전성 또는 연속성

우리는 위탁 관련 규정을 해석하고 적용하는 접근 방식을 설명하는 자료를 발표했다.

4. (싱가포르-MAS) 아웃소싱 가이드라인 - 부칙2 중요 아웃소싱

1. 기관은 아웃소싱 계약의 중요성을 평가해야 한다. MAS에서는 중요성을 평가할 때 정성적인 판단이

개입되며 각각의 기관에서 직면하는 상황이 서로 크게 다를 수 있다는 점을 인지하고 있다. 기관에서 고려해야 하는 요인을 예로 들면 다음과 같다.

(a) 아웃소싱 할 비즈니스 업무 활동의 중요도(예: 수익 및 이윤에 대한 기여도 관련)

(b) 소득, 지급능력, 유동성, 펀딩 및 자본과 리스크 프로필 등에 아웃소싱이 미칠 수 있는 잠재적인 영향력

(c) 서비스 제공업체가 서비스를 이행하지 못하거나 기밀성 또는 보안 침해 문제가 발생하는 경우 기관의 평판 및 브랜드 가치, 기관이 비즈니스 목표, 전략과 계획을 달성할 능력 등에 미치는 영향(예: 고객 정보 누출)

(d) 서비스 제공업체가 서비스를 이행하지 못하거나 기밀성 또는 보안 침해가 발생하는 경우 기관의 고객에게 미치는 영향

(e) 서비스 제공업체가 서비스를 이행하지 못하는 경우 기관의 계약 상대방 및 싱가포르 금융 시장에 미치는 영향

(f) 아웃소싱 비용이 기관의 운영 비용 총액에서 차지하는 비율

(g) 아웃소싱 실패 시 치러야 하는 비용. 이 경우 기관은 아웃소싱 된 업무 활동을 사내로 들여오거나 다른 서비스 제공업체로부터 유사한 서비스를 알아보아야 하며, 이 비용은 기관의 운영 비용 총액의 일부분을 차지한다.

(h) 기관이 여러 업무를 같은 서비스 제공업체에 아웃소싱 하는 경우 특정 서비스 제공업체에 대한 통합 노출 리스크

(i) 서비스 제공업체에 운영 문제가 생기는 경우 적절한 내부 통제 수단을 유지하고 규제 요구사항에 부합할 능력

2. 규정 준수, 사내 감사, 재무 회계 및 보험계리 등(인증 업무 활동을 수행하는 것 외) 리스크 관리 또는 내부 통제 업무 전량 또는 상당량을 아웃소싱 하는 경우 이는 중요 아웃소싱 계약으로 간주된다.

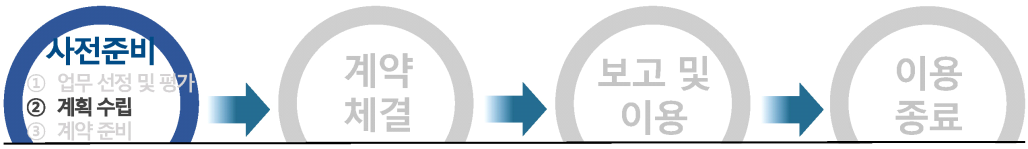
금융분야
클라우드컴퓨팅서비스
이용 가이드

제4장

계획 수립

1. 업무 연속성 계획 수립
2. 출구 전략 수립
   (업무 연속성 계획에 포함)
3. 안전성 확보조치 방안 수립
4. 업무 위수탁 운영기준 마련

제 4 장 계획 수립



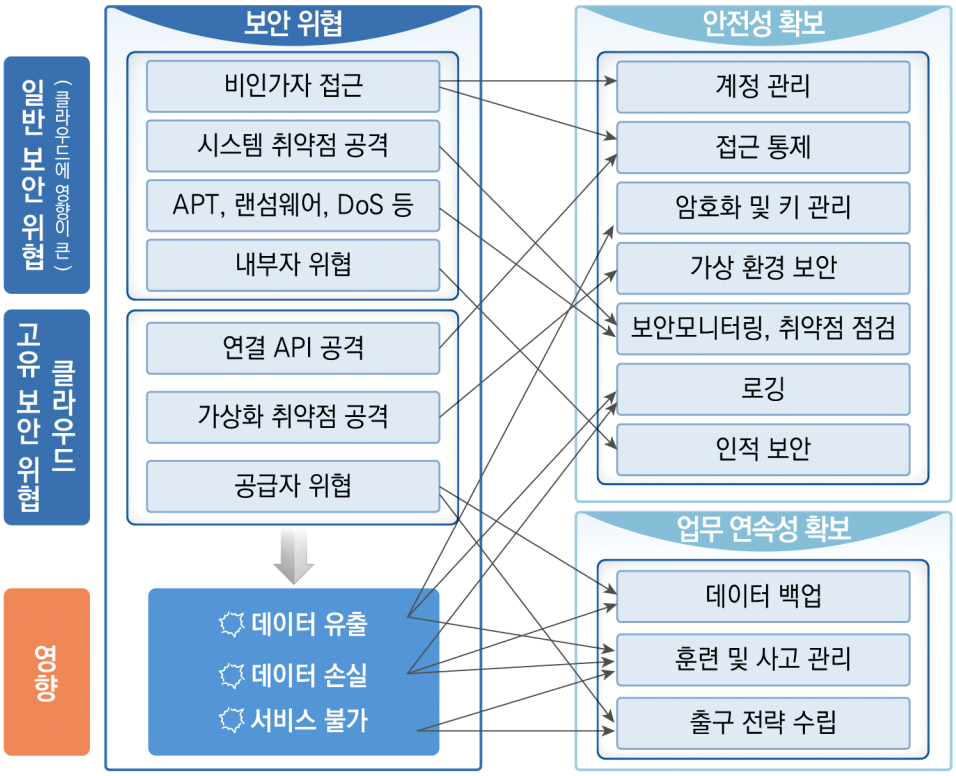
안전한 클라우드서비스 이용을 위한 사전 계획 수립

- ✔ 업무 연속성 계획 (출구전략 포함)
- ✔ 안전성 확보조치 방안

➤➤ ✔ 업무 위수탁 운영 기준 마련

※ 클라우드서비스 관련 보안 위협

금융회사 대상으로 발생할 수 있는 일반적인 보안 위협 중 클라우드서비스 이용 시 그 영향이 큰 위협이 있으며, 클라우드서비스 고유의 보안 위협도 일부 존재한다. 금융회사는 **업무 연속성 계획 및 안전성 확보조치 방안 수립 시 이를 적극 고려**하여야 한다.



1 업무 연속성 계획 수립

금융회사는 클라우드서비스에 대해 예상치 못한 재해 또는 사고 발생 시 업무 연속성에 미칠 수 있는 영향을 파악하고, 데이터 백업, 재해복구 및 침해사고대응 훈련 계획, 출구 전략 등을 포함한 업무 연속성 계획을 수립하여 이행하여야 한다.

> ▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**
> ④ 제3항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.
> 3. 클라우드컴퓨팅서비스 이용 관련 **업무 연속성 계획** 및 안전성 확보조치에 관한 사항

가. 데이터 백업

- 백업할 데이터를 선정하고, 업무 중요도에 따라 데이터 이중화 또는 소산 등 다양한 방법을 고려하여 클라우드서비스 제공자의 데이터 손실 사고 등에 대비할 것
  - 또한, 데이터 복원 테스트 및 데이터 무결성 테스트를 정기적으로 안전하게 수행할 것
- 백업 데이터를 위한 적절한 접근 통제를 실시하고, 관련 법령에 따라 암호화 등 적절한 보호조치를 취할 것

나. 훈련 및 사고 관리

- 금융회사가 관련 규정에 따라 위기대응행동매뉴얼 및 비상대책을 마련하고, 비상대응훈련 및 재해복구전환훈련을 연 1회 이상 실시(감독규정 제23,24조)할 때 대상 시스템이 클라우드서비스 이용을 이유로 제외되지 않도록 할 것
  - 필요 시 클라우드서비스 제공자에 협조를 요청하여 합동으로 훈련을 진행하여야 하며, 클라우드서비스 제공자의 자체 재해복구 훈련 계획 및 주기적인 훈련 실시 여부를 확인할 것

- 사고 발생 시 클라우드서비스 제공자와 금융회사 간의 역할 분담 및 대응 절차를 문서화하여 관리하고, 관련 규정에 따라 침해사고대응훈련(감독규정 제37조의4) 수행 시 대상 시스템이 클라우드서비스 이용을 이유로 제외되지 않도록 할 것
  - 금융회사와 클라우드서비스 제공자 간 비상 연락 체계를 사전에 확보하고, 상황 발생 시 관련 규정에 따라 신속히 대응할 것

    ※ 중요도가 높은 시스템의 경우 필요 시 해당 클라우드서비스 제공자와 침해사고대응기관 간 핫라인을 구축할 것
- 업무 별 복구목표시간 및 복구목표시점을 정하고 클라우드서비스 제공자와 사전 협의할 것

〈업무 연속성 계획 수립 관련 참고 규정〉

▶ **감독규정**

제23조(비상대책 등의 수립·운용) ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립·준수하여야 한다.

1. 상황별 대응절차
2. 백업 또는 재해복구센터를 활용한 재해복구계획
3. 비상대응조직의 구성 및 운용
4. 입력대행, 수작업 등의 조건 및 절차
5. 모의훈련의 실시
6. 유관기관 및 관련업체와의 비상연락체제 구축
7. 보고 및 대외통보의 범위와 절차 등

② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다.

1. 파업 시 핵심전산업무 종사자의 근무지 이탈에 따른 정보처리시스템의 마비를 방지하기 위하여 비상지원인력을 확보·운영할 것
2. 비상사태 발생 시에도 정보처리시스템의 마비를 방지하고 신속히 원상복구가 될 수 있도록 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문 업체를 활용하는 방안을 수립·운영할 것
3. 비상지원인력이 사용법을 충분히 이해하고 업무운용이 가능한 수준으로 전산시스템 운영지침서, 사용자매뉴얼 등을 쉽고 자세하게 작성하고 최신상태로 유지할 것
4. 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시할 것

③ 금융회사 또는 전자금융업자는 제1항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하여야 한다.

④ 「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의 「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립·준수하고 이를 금융위원회에 알려야 한다.
⑤ 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운영하여야 한다.
⑥ 제4항에 따른 행동매뉴얼 또는 제5항에 따른 비상대책에는 제1항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.
⑦ 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다.
⑧ (생략)
⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24시간 이내로 한다.
⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 **매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련**을 실시하여야 한다.

제24조(비상대응훈련 실시) ① 금융회사 또는 전자금융업자는 제23조제4항에 따른 **행동매뉴얼** 또는 같은 조 제5항에 따른 **비상대책**에 따라 **연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고**하여야 한다. 이때, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다.
②~③ (생략)
④ 금융회사 또는 전자금융업자는 제1항 및 제2항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.

제37조의4(침해사고대응기관 지정 및 업무범위 등)
①~④ (생략)
⑤ 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 **연 1회 이상 침해사고 대응 및 복구훈련 계획을 수립·시행**하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게 제출하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다.
1.~4. (생략)
⑥~⑦ (생략)

참고 주요국 금융권 지침 내 업무연속성 확보 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 - 4.8 비상계획 및 출구전략 中

26) CEBS 지침 6.1, 6(6)(e) 및 8(2)(d)에 명시된 바와 같이, 금융회사는 위탁 서비스 제공 업체가 실패하거나 부적절하게 수준으로 악화된 상태로 서비스를 제공하는 경우 사업의 연속성을 유지하기 위한 계획을 수립하고 이행해야한다. 이러한 준비에는 비상 계획 및 명확하게 정의 된 출구 전략이 포함되어야 한다. (중략)

2. (미국-FFIEC) 아웃소싱 클라우드 컴퓨팅 - 7. 업무 연속성 계획

금융 기관의 비즈니스 연속성 계획 프로세스에는 아웃소싱 활동을 포함하여 전체 비즈니스의 복구, 재개 및 유지 관리가 포함된다. 금융 기관은 클라우드 컴퓨팅 서비스 공급자에게 아웃소싱 하는 것을 고려할 때, 서비스 제공 업체와 네트워크 제공자가 금융 기관의 운영 지속성을 보장 할 수 있는 적절한 계획과 자원을 보유하고 있는지, 예기치 않은 중단이 발생할 경우 운영을 복구 및 재개 할 수 있는 능력이 있는지를 판단할 필요가 있다.

3. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 〈위탁 시 고려사항 - 연속성 및 비즈니스 계획〉

기업은 예상치 못한 위탁 서비스 중단 시 계속해서 기능을 수행하고 규제 사항을 준수할 수 있도록 적절한 조치를 취해야한다. 기업은 다음을 수행해야한다.

- 예상치 못한 혼란이 운영 연속성에 미칠 수 있는 영향 및 가능성을 고려해야한다.
- 사고 복구를 포함하여 운영 연속성을 유지하기 위한 전략과, 상호 소통 및 전략의 적절성과 유효성을 정기적으로 테스트하기 위한 계획을 문서화해야 한다.
- 정기적으로 업데이트 및 테스트를 실시하여 효율성을 확보해야 한다.
- 파산이나 기타 혼란 상황이 발생했을 때 규제 기관이 데이터에 접근할 수 있도록 조치를 취해야 한다.

4. (싱가포르-MAS) 아웃소싱 가이드라인 - 5.7 비즈니스 연속성 관리

5.7.1 기관은 아웃소싱 계약으로 인해 자사 비즈니스 연속성이 저해되지 않도록 주의해야 한다. 특히 기술 리스크 관리 공지에 따라 중요 시스템으로 규정된 시스템을 각별히 주의한다. 기관은 MAS에서 발간한 비즈니스 연속성 관리("BCM") 가이드라인에 기재된 건실한 실무 관례 및 표준을 이용하여 아웃소싱이 자사 리스크 프로필에 미치는 영향을 평가하고 효과적인 BCM을 실행한다.

5.7.2 BCM 가이드라인과 같은 맥락에서, 기관은 아웃소싱 계약으로 인해 발생하는 상호의존 리스크를 적절히 완화할 수 있는지 평가하고 자체적으로 확인해야 한다. 이렇게 해야 서비스가 중단되거나 오류가 발생하는 경우, 또는 아웃소싱 계약이 예기치 않게 해지되거나 서비스 제공업체가 파산하는 경우에도 자사 비즈니스를 결함 없이 사려 깊게 영위할 수 있다. 여기에는 다음과 같은 조치를 취하는 것이 포함되어야 한다.

(a) 서비스 제공업체에 아웃소싱 계약의 성격, 범위 및 복잡성에 상응하는 만족스러운 비즈니스 연속성 계획(이하 "BCP")이 마련되어 있는지 확인한다. 아웃소싱 계약서에 서비스 제공업체의 BCP 요구 사항, 특히 복구 목표 시간(Recovery Time Objectives, 이하 "RTO") 및 복구 목표 지점(Recovery Point Objectives, 이하 "RPO")과 운영 능력 재개 등에 관한 항목을 포함해야 한다.

(b) 사전 예방적인 형태로 서비스 제공업체의 BCP 준비 상태를 확인한다. 또는 가능한 경우 합동 테스트에 참가한다. 서비스 제공업체가 자사 BCP 계획을 정기적으로 테스트하고 테스트를 통해 RTO, RPO 및 운영 능력 재개의 실현 가능성을 검증해야 한다. 그러한 테스트는 기관과 서비스 제공업체가 복구 프로세스에 익숙해지는 데 도움이 되고, 관계 당사자들의 조직력을 개선하는

효과도 있다. 기관은 서비스 제공업체에 서비스 제공업체의 이행 능력에 영향을 미칠 수 있는 테스트 결과가 나온 경우 그러한 사실을 자사에 알리도록 요구해야 한다. 또한 기관은 서비스 제공업체에 서비스 제공업체의 BCP 계획에 중대한 변동이 발생하였거나 기관에 제공되는 서비스에 중대한 영향을 미칠 가능성이 있는 불리한 상황이 전개되는 경우 그러한 사실을 모두 자사에 알리도록 요구해야 한다.

(c) 불리한 상황 또는 아웃소싱 계약의 해지 등과 같은 상황을 타개하기 위한 계획과 절차를 마련하여 기관이 비즈니스를 계속해서 영위할 수 있어야 하며, 이전에 서비스 제공업체에 제공한 모든 문서, 거래 기록 및 정보를 즉시 서비스 제공업체의 소유로부터 회수하여 삭제, 파기하거나 사용할 수 없게 만들어야 한다.

5.7.3 기관은 자사 BCP 계획의 기능성과 효과를 보장하기 위하여 아웃소싱 계약의 성격, 범위 및 복잡성에 상응하는 정기적이고 온전하며 유의미한 BCP 테스트를 고안하여 수행해야 한다. 온전하고 유의미한 테스트를 실시하기 위해 기관에서는 자사 BCP 검증 및 자사 임직원의 인식과 준비성 평가 과정에 서비스 제공업체를 관여시키는 것이 좋다. 이와 마찬가지로, 기관은 자사 서비스 제공업체의 BCP 및 재해 복구 연습에 참가해야 한다.

5.7.4 기관은 비즈니스 연속성 계획에서 최악의 상황을 가정한 시나리오를 감안해야 한다. 이러한 가상 시나리오의 몇 가지 예를 들면 아웃소싱 계약이 예기치 못하게 해지되어 서비스 제공업체를 이용할 수 없는 경우, 서비스 제공업체의 파산 및 광역 서비스 중단으로 인하여 기관과 서비스 제공업체 양측 모두에 부수적인 피해가 발생하는 경우 등이 있다. 금융 체제에 대한 기관의 상호의존도가 높은 경우, 기관의 비즈니스 연속성 준비성도 그에 따라 높은 수준으로 유지해야 한다. 감당할 수 없는 비용을 발생시키지 않고 운영을 재개하기 위한 현실적인 대안을 파악하는 것 또한 상호의존 리스크를 완화하는데 필수적이다.

2 출구 전략 수립 (업무 연속성 계획에 포함)

클라우드서비스 제공자의 파산, 서비스 중단, 서비스 품질 저하, 규제 환경의 변화 또는 기타 금융회사의 필요에 따른 이용 중단 등에 대비하여 클라우드서비스 이용 전환 및 종료에 대한 출구 전략을 사전 수립하여 문서화하여야 한다.

> ▶ **감독규정 [별표 2의3] 업무위탁 운영기준 보완사항 中**
>
> **3. 비상대책 등에 관한 사항**
>
> - 합병·분할, 계약상 지위의 양도, 재위탁 등 중요 상황 발생 시 대책(업무 연속성 계획 포함)에 관한 사항
> - 위탁업무를 다른 수탁자 또는 클라우드컴퓨팅 업무를 위탁한 금융회사 및 전자금융업자에 이전시키는 경우 업무 장애·서비스지연, 이전을 지원할 의무 등 전환계획에 관한 사항
> - 위탁계약의 종료, 중단, 변경 시 데이터 반환·파기에 관한 사항

출구 전략은 이행 지표와 세부 이행 절차로 구성되며, 업무 연속성 계획에 포함하여야 한다.

가. 출구 전략 이행 지표 설정

- 출구 전략 이행이 필요한 상황을 사전에 정의하고, 해당 상황을 판단할 수 있는 지표를 설정하고 모니터링 할 것
- 출구 전략 이행에 대한 성공 기준*을 사전에 정의할 것

  * (예) 서비스 제공 또는 규제 체제 준수에 부정적 영향을 미치지 않으며 서비스 제공의 연속성과 품질에 지장을 주지 않고 클라우드서비스 위탁 계약을 종료

나. 출구 전략 이행 절차 정의

- 출구 전략 이행 절차에 대한 전사적인 기본 방향 및 정책을 수립하고, 이행에 필요한 조직별 역할 및 책임을 사전에 정의할 것

- 개별 정보처리시스템에 대한 출구 전략 세부 이행 절차를 정의하고, 이행에 필요한 인적·물적 자원과 예상 소요시간을 정의할 것

> **※ 출구 전략 세부 이행 절차 내 필수 포함 사항**
> - 출구 전략 방법(이전, 대체, 재개발 등)
> - 대체 사업자 또는 솔루션
> - 기존 클라우드서비스 제공자 시스템에서 데이터를 복구할 수 없도록 파기하는 절차 및 방법
> - 업무 연속성을 유지하면서 기존 업무 및 데이터를 대체 시스템에 이전하는 절차 및 방법
> - 이전 시점 및 소요시간, 인력 및 비용

다. 출구 전략 수립 관련 고려사항

- 중요도가 높은 정보처리시스템에 대해서는 출구 전략을 보다 정밀하게 수립하고, 대안을 충분히 마련할 것
- 중요도가 높은 정보처리시스템에 대해서는 출구 전략 이행이 용이한 구현 방식을 고려할 것

> **※ 구현 방식에 따른 출구 전략 이행 용이성**
> - (IaaS) 컨테이너 방식 이용 시 출구 전략 이행이 용이하고, 클라우드서비스 제공자의 관리 서비스 등에 의존도가 높으면 이행 용이성이 떨어짐
> - (PaaS, SaaS) 클라우드서비스 제공자가 자체 인프라가 아닌 제3의 IaaS 제공자 인프라를 이용하여 서비스를 제공하는 경우 상대적으로 출구 전략 이행 용이

- 출구 전략 관련 훈련 및 이행을 위해 클라우드서비스 제공자의 지원을 충분히 받을 수 있도록 계약서에 관련 내용을 명시할 것

※ 출구 전략 이행을 위해 필요한 계약서 명시사항은 「제6장 계약 체결」 참조

참고 주요국 금융권 지침 내 출구 전략 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 - 4.8 비상계획 및 출구전략

26) (중략) 이러한 준비에는 비상 계획 및 명확하게 정의 된 출구 전략이 포함되어야 한다. 또한 위탁 계약에는 위탁 서비스 제공 업체가 제공하는 활동을 다른 위탁 서비스 제공 업체로 이전하거나 금융 회사로 재편성 할 수 있는 종료 및 종료 관리 조항이 포함되어야 한다.

27) 위탁 기관은 필요한 경우 서비스 제공 또는 규제 체제 준수에 부정적 영향을 미치지 않으며 서비스 제공의 연속성과 품질에 지장을 주지 않고 클라우드 위탁 계약을 종료할 수 있도록 해야 한다. 이를 위해 금융회사는 다음을 수행해야 한다.

(a) 적절하고 포괄적이며 문서화 되고 충분히 테스트 된 출구 계획을 개발하고 구현한다.

(b) 대체 솔루션을 식별하고 전환 계획을 개발하여 전환 단계에서 데이터 위치 문제 및 비즈니스 연속성 유지를 고려하여 통제되고 충분히 검증된 방법으로 클라우드 서비스 제공자의 기존 업무 및 데이터를 제거하고 대체 솔루션으로 전달할 수 있도록 한다.

(c) 위탁 계약 종료 시 금융회사가 다른 서비스 제공 업체 또는 금융회사의 직속 관리에게 순서대로 이전할 수 있도록, 위탁 계약에 클라우드 서비스 제공자에게 금융회사를 충분히 지원할 의무가 포함되도록 해야 한다.

28) 출구 전략을 개발할 때 금융회사는 다음 사항을 고려해야 한다.

(a) 받아들일 수 없는 수준의 서비스를 식별하기 위한 주요 위험 지표 개발

(b) 출구 전략을 이행하는 데 필요한 인적/물적 자원과 소요 시간을 식별하기 위하여 위탁된 활동에 상응하는 비즈니스 영향 분석을 수행

(c) 출구 계획 및 전환 활동을 관리하는 역할 및 책임 지정

(d) 전환 성공 기준을 정의

29) 금융회사는 지속적인 서비스 모니터링과 클라우드 서비스 공급자가 제공하는 서비스 감독에 있어 출구 계획을 유발할 수 있는 지표를 포함해야 한다.

2. (미국-FFIEC) 아웃소싱 클라우드 컴퓨팅 - 3. 공급 업체 관리 中

서비스 제공 업체의 해약은 특히 소규모 금융 기관의 경우 클라우드 컴퓨팅에서 복잡해질 수 있는 공급 업체 관리의 또 다른 측면이다. 계약 및 서비스 수준 협약은 데이터의 소유권, 위치, 형식 및 분쟁 해결에 대해 구체적이어야 한다.

3. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 〈위탁 시 고려사항 - 출구전략〉

기업은 원할 경우 서비스 제공에 차질 없이 규정을 준수하면서 위탁 계획을 해지할 수 있어야한다. 기업은 다음을 수행해야한다.

- 이해되고 문서화 되며 충분히 검증된 출구 계획 및 해지 약정을 세워야 한다.
- 대체 서비스 제공자로 전환하고 비즈니스 연속성을 유지하는 방법을 인지하고 있어야 한다.
- 위탁 제공자는 기업 및 새로운 위탁 제공자(들)와 완벽하게 협력하여 원활히 전환될 수 있도록 보장해야 할 의무를 지닌다.
- 해지 시 서비스 제공자의 시스템에서 데이터를 제거하는 방법을 알고 있어야한다.
- 편중된 위험을 모니터링하고 위탁 제공자가 파산할 경우 취할 조치를 고려해야 한다.

4. (싱가포르-ABS) 클라우드 컴퓨팅 구현 가이드 - Section3: 6. 출구 계획

출구 계획은 아웃소싱 계약의 중요도 및 금융회사의 운영에 미치는 잠재적 영향에 따라 내용이 달라져야

한다. 출구 계획 수립 시 다음 사항을 고려하여야 한다.

- 데이터가 복구할 수 없도록 삭제하기 위해 사용하는 절차 및 도구
- 위탁 계약 종료 시 모든 금융회사 데이터(고객정보 등)를 삭제하고 모든 데이터가 복구할 수 없다는 것을 확인할 것
- 서비스 연속성을 위한 위탁된 서비스의 이전성(제3자에게 이전 또는 금융회사로 복귀)
  서비스 연속성을 위한 데이터 복구 시 금융회사는 다음 사항이 적절한지 확인해야 함
- CSP가 출구 절차를 지원하기 위한 법적 계약. 이 계약은 서비스 제공자가 기 협의된 주기로 출구 계획 테스트를 지원하도록 함. 이는 데이터가 금융회사로 반환되는 형식 및 방식과, 공급업체의 계약상 의무 지원 내용을 포함해야함. 금융회사가 CSP가 제공한 연계 공급업체 소프트웨어를 사용하는 경우, 계약이 종료될 때 해당 데이터를 사용할 수 있어야 함.
- 추출하여 금융회사에 반환해야 하는 데이터 요소는 위탁 계약 시작 시 합의되어야 하며, 위탁 계약에 중대한 변경이 있을 때마다 검토되어야 함

3 안전성 확보조치 방안 수립

클라우드서비스 관련 보안사고의 예방을 위해 계정관리, 접근통제 등 필수 보안 통제가 구현되도록 안전성 확보조치 방안을 수립하여 이행하여야 한다.

> ▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**
> ④ 제3항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.
> 3. 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 **안전성 확보조치**에 관한 사항

다만, 업무 중요도 평가 결과에 따라 수행 범위를 조정할 수 있다.

〈업무 중요도 별 적용 범위(예시)〉

항목 \ 중요도	중요	비중요
계정 관리	◎	◎
접근 통제	◎	◎
내부 시스템·단말기와의 연계	◎	◎
암호화 및 키 관리	◎	△
로깅	◎	○
가상 환경 보안	◎	○
보안 모니터링 및 취약점 분석 평가	◎	○
인적 보안	◎	◎

※ ◎: 강력 권고, ○: 권고, △: 금융회사 재량
다만, 권고 여부와 무관하게 법규에서 요구되는 사항은 필수

가. 계정 관리

- 각 관리자 및 이용자에 대한 개별 계정을 생성할 것
  - 기능과 역할에 따라 그룹을 구분하고, 적절한 권한을 그룹별로 할당하여 관리할 것

〈그룹 구분 예시〉

그룹	권한
보안 관리자	보안 그룹 및 규칙 생성/수정/삭제
개발자	개발 인스턴스 시작/중지/종료 권한
운영자	프로덕션 시작/중지/종료 권한
계정 관리자	사용자 추가/삭제

- 특별 권한이 있는 계정(이하, 특권 계정)을 정의하고 집중 관리를 실시할 것

※ (집중 관리 예시) 사용 이력·접근 기록 로깅 및 주기적 검토, 멀티팩터 인증, 설정 변경 요청·승인 절차 공식화, 특권 계정 관리자와 일반 사용자 계정 관리자 분리 등

나. 접근 통제

- 클라우드서비스 제공자 구간에 위치한 정보처리시스템에 대해 동일 클라우드서비스를 이용하는 외부기관의 통신망과 분리·차단하고 접속을 금지할 것
  - 내부망 정보처리시스템이 클라우드서비스 제공자 구간에 위치한 경우, 인터넷 등 외부통신망과도 분리·차단하고 접속을 금지할 것

※ 금융회사 전산실 내 물리적 망분리 구조를 논리적으로 구현

- 보안관리 등 모든 시스템 원격 접근 절차를 문서화하여 관리하고, 정기적으로 검토할 것
- 특권 계정은 금융회사 내 별도로 분리된 관리용 단말기에서만 접근 가능하도록 할 것

※ 금융회사 단말기와 클라우드서비스 시스템 간 연결 관련 세부 내용은 「다. 금융회사 내부 시스템과의 연계」 참조

- 관리서비스 이용 등으로 클라우드서비스 제공자가 시스템 또는 소프트웨어에 접근 권한이 있는 경우 클라우드서비스 제공자의 관리 기록을 로깅하고, 주기적으로 검토할 것

참고 접근통제 및 네트워크 정보보호 요구사항(출처: KISA 클라우드 정보보호 안내서)

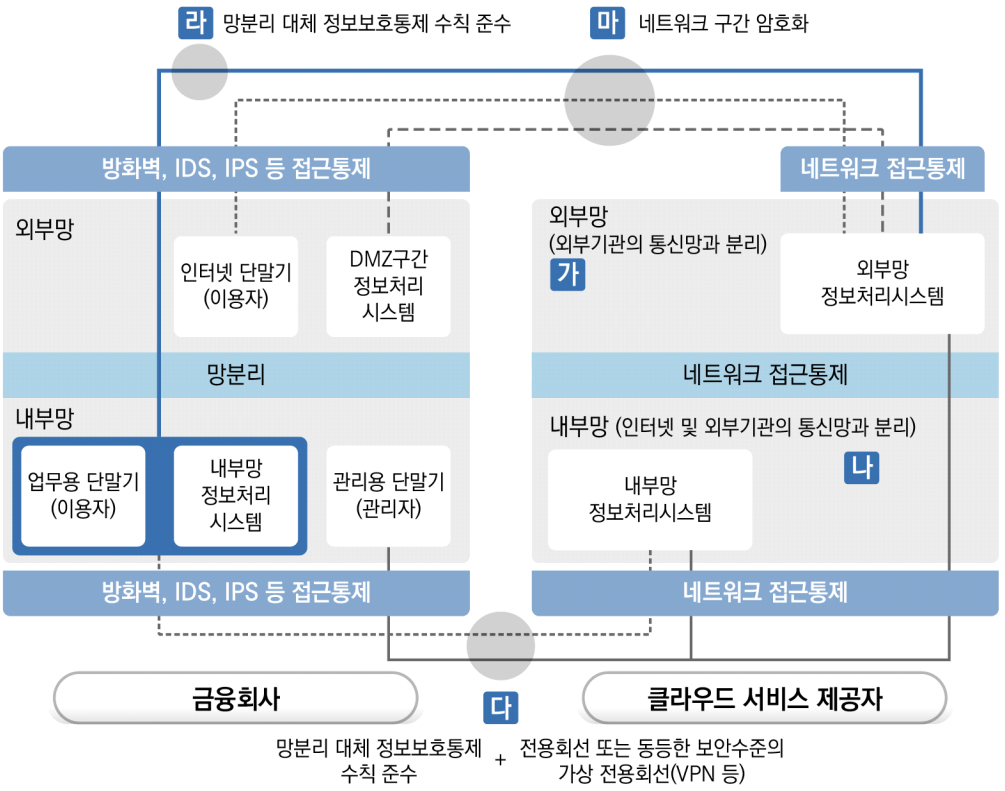
접속 관리 및 제한	① 서비스 연결은 승인하기 전에 모든 사용자(또는 단말기)의 접속은 정책에서 규정된 절차에 따라 인증하고, 접속로그를 관리하며 모니터링을 해야 한다. • 인증 시 사용하는 패스워드 조합 규칙 준용 - 세 가지 종류 이상의 문자구성으로 8자리 이상의 길이로 구성된 문자열 - 두 가지 종류 이상의 문자구성으로 10자리 이상의 길이로 구성된 문자열 • 로그인 횟수제한(5회), 잠김해제(120초) 준용 • 하나의 사용자가 동시에 여러 세션을 소유하는 것을 제한 ② 통신 세션의 기밀성을 보장하기 위해 안전한 암호 기술을 적용한다. • 통신세션 기밀성은 SSL/TLS, VPN 등 안전한 보호기술 적용 ③ 내부정책에서 제한하는 모바일 단말기의 통제 대책을 마련한다.
계정 분할 및 권한 최소화	① 서로 다른 이용자 계정의 충돌을 최소화하기 위하여 접근을 허용하는 영역이나 권한 등을 분리한다. ② 사용자에 부여하는 역할·권한을 최소한의 범위로 제한해야 한다. ③ 정책서의 계정관리 주기에 따라 점검 및 이용자 변경 사항은 즉시 정책에 반영한다.
네트워크	① 네트워크 접근통제를 H/W 형태, S/W 형태, API 형태 중 어떤 것을 선택할 것인지 고려해야 한다. ※ 클라우드서비스 업체에서 제공하는 방식에 대해 확인필요 • H/W 형태: 기존 온프레미스 환경과 동일 • S/W 형태: 서버에 접근통제 솔루션을 설치하는 방식으로 여러 대를 설치해야 할 수 있음 • API 형태: 기존의 네트워크 솔루션 기반의 접근통제 방식과는 다른 개념으로 성능 및 네트워크와 무관하게 원하는 방식으로 그룹을 묶어서 접근통제 가능 ② 네트워크 트래픽 도청이나 데이터 유출 방지를 위해 통신 암호화를 적용하여 관리한다. ③ 사용자의 네트워크 접속·인증을 위한 신분확인 메커니즘을 도입한다. ④ 네트워크 가용성이 침해하는 서비스거부공격(DoS)에 대한 대책을 마련한다. ⑤ 이(異)기종 네트워크의 연동에 따른 보안대책을 고려한다. ⑥ 네트워크 장애에 대비하여 네트워크 분할 또는 이중화하여 관리한다. ⑦ 네트워크 장애에 대비하여 보안관제 체계 구축을 고려한다.

다. 내부 시스템·단말기와의 연계

- 업무용 단말기 및 내부망 정보처리시스템을 클라우드서비스 제공자 구간에 위치한 내부망 정보처리시스템에 연결하거나, 관리용 단말기를 클라우드서비스에 연결해야 하는 경우 다음 사항을 준수할 것
  - 감독규정 시행세칙의 망분리 대체 정보보호통제 수칙
  - 전용회선 또는 전용회선과 동등한 보안수준을 갖춘 가상의 전용회선(VPN 등) 사용

- 업무용 단말기 및 내부망 정보처리시스템을 클라우드서비스 제공자 구간에 위치한 외부망 정보처리시스템에 연결해야 하는 경우 감독규정 시행세칙의 망분리 대체 정보보호통제 수칙을 준수할 것
- 단말기 및 정보처리시스템을 클라우드서비스 제공자 구간에 위치한 외부망 정보처리시스템에 연결해야 하는 경우 암호화된 통신채널을 사용할 것

〈금융회사 내부 시스템 연계 시 보호대책 (예시)



※ 내부 시스템·단말기 연계 시 보호대책은 고유식별정보 및 개인신용정보 처리 여부와 무관하게 준수(개발망, SaaS 구축 등의 경우에도 동일 원칙 적용)

라. 암호화 및 키 관리

- 고유식별정보, 개인신용정보 등 민감 데이터를 암호화하고, 암호화 키의 생성부터 폐기까지 전 단계 관리를 위한 세부 정책을 마련할 것
  - 필요 시 HSM(Hardward Security Modules)을 이용하여 키 관리를 강화할 것
- 암호화 키는 접근이 통제된 보안네트워크*에 저장하고, 클라우드서비스 제공자의 직원이나 동일 클라우드서비스를 이용하는 외부 기관이 접근할 수 없도록 할 것

  * (예) 금융회사 내부 시스템, 클라우드서비스 제공자의 보안네트워크 서비스 등

〈암호화 관련 참고 규정〉

▶ 고유식별정보 암호화(개인정보보호법)

제24조(고유식별정보의 처리 제한) ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

제24조의2(주민등록번호 처리의 제한) ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

▶ 개인신용정보 암호화(신용정보의 이용 및 보호에 관한 법률)

제17조(수집·조사 및 처리의 위탁) ④ 신용정보회사등은 제2항에 따라 신용정보의 처리를 위탁하기 위하여 수탁자에게 개인신용정보를 제공하는 경우 특정 신용정보주체를 식별할 수 있는 정보는 대통령령으로 정하는 바에 따라 암호화 등의 보호 조치를 하여야 한다.

▶ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조(개인정보의 보호조치) ① 정보통신서비스 클라우드서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치

마. 로깅

- 접근기록, 가동기록 및 보안로그 등을 기록·유지하여, 추후 사고 발생 시 조사(포렌식 조사 포함) 및 대응이 가능하도록 하고, 증거 수집 또는 획득 방법 등을 수립할 것

> ▶ **감독규정 제13조(전산자료 보호대책) 中**
>
> ④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동으로 기록·유지되어야 한다.
>
> 1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록,
> 2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
> 3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근 기록

- 로그데이터를 위한 적절한 접근통제를 실시하고 관련 법령에 따라 암호화 등 적절한 보호조치를 취할 것
  - 특히, 보안로그의 경우 독립적인 시스템에 보관하는 등 무결성 및 가용성이 보장될 수 있도록 관리할 것

바. 가상 환경 보안

- 클라우드서비스 하드웨어, 가상 이미지, 가상화 관리 소프트웨어(하이퍼바이저 등)에 대한 잠재적 위협을 고려하여 취약점 점검, 보안 모니터링 등을 실시할 것

- 가상 네트워크, 컨테이너 등 활용 시 표준 이미지, 개별 서비스별 보안 설정을 체계적으로 관리하고 모니터링 할 것
  - 이 때, 가상 이미지 템플릿 등을 최신 상태로 유지하고, 현재 이미지 구성, 패치 상태, 이미지 무결성 등을 주기적으로 점검할 것

참고 서버 및 가상화 보안 정보보호 요구사항(출처: KISA 클라우드 정보보호 안내서)

공통	① 바이러스, 웜, 트로이목마 등의 악성코드 예방을 위해 서버 및 가상환경을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 적용한다. 특히, 가상환경의 경우 이상 징후 발견 시 사용 중지 및 격리 조치를 수행할 수 있는 체계를 갖추고 운영한다.
가상화 보안	① 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립한다. ② 가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 한다. ③ 호스트 OS 및 하이퍼바이저를 모니터링 하고 악성코드 감염예방을 위해 주기적인 보안 패치를 시행한다. ④ 가상화 실행 이력은 스냅샷 등 이미지 형태로 저장·관리하는 방안 등 안전한 저장 방법으로 관리한다. ⑤ 가상화 OS의 내·외부 데이터 이용에 대한 로그 정보를 관리한다. ⑥ 가상머신별 자원 사용량 제한하여 특정 가상머신의 자원이 남용되지 않도록 한다. ⑦ 호스트와 가상영역 간의 경계를 명확히 구분하고 운영한다.
서버 보안	① 클라우드서비스 운영 시 시스템에 대해 기술적 보호대책을 수립하고 적용한다. • 웹서버, DB서버, 클라우드 인프라 관리서버 등 운영 시 다음의 보호대책 적용 - 송·수신 시 SSL/TLS 통신 적용, 불필요한 서비스 및 포트 차단 - 접근권한 설정, 백신설치 및 OS 최신 패치 - 불필요한 소프트웨어, 스크립트, 실행파일 등 설치 금지 - 불필요한 페이지(테스트페이지) 및 에러처리 미흡에 따른 시스템 정보 노출 방지 - 주기적인 보안패치 및 취약점 점검 실시 등 ② 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호한다. ※ 보안솔루션 구축 시 고려사항 기존 IT환경에서는 일반적으로 H/W 형태 보안솔루션(Firewall, IPS, IDS, Web Application firewall 등)을 구축하지만, 가상환경에서는 유연한 확장성을 고려하여 S/W 방식으로 구축하는 것이 일반적이다. 따라서 확장성이 반드시 보장되어야 한다면 호스트 기반의 보안솔루션을 설치하는 것이 적합한 방법이다.

사. 보안 모니터링 및 취약점 분석·평가

- 중요 로그를 실시간으로 모니터링하고 주기적으로 분석할 것
- 침입 탐지/방지 시스템, 웹 방화벽, DDoS 대응 장비 등 보안 시스템을 적절한 위치에 배치하여 공격을 탐지·대응할 것
- 연 1회 이상(홈페이지는 6개월에 1회 이상) 실시하는 취약점 분석·평가 수행 시 클라우드서비스를 이용하는 전자금융기반 시스템을 포함하여야 하며, 필요 시 클라우드서비스 제공자에 협조를 요청할 것
  - 이 때, 일반 취약점뿐만 아니라 클라우드 컴퓨팅 고유의 위협을 고려하여 수행할 것

▶ 감독규정 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)

①~⑤ (생략)

⑥ 금융회사 또는 전자금융업자는 제1항 또는 제3항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.

아. 인적 보안

- 금융회사 내 클라우드서비스 이용자 및 관리자를 대상으로 주기적인 클라우드서비스 보안 교육을 실시하고, 클라우드서비스 제공자의 직원 보안 교육 계획 및 결과(대상 직원 수, 이수 시간 등) 등을 공유 받아 검토할 것

참고 주요국 금융권 지침 내 보안조치 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 - 4.5 데이터 및 시스템 보안

15) CEBS 가이드라인 8(2)(e)에 명시된 바와 같이, 위탁 계약은 위탁 서비스 제공 업체가 금융회사가 전송하는 정보의 기밀성을 보호하도록 의무화 해야 한다. 금융회사는 CEBS 가이드라인 6(6)(e) 지침에 따라 위탁 서비스 제공 업체가 제공하는 서비스의 연속성을 보장하기 위한 조치를 취해야한다. CEBS 가이드라인 8(2)(b) 및 지침을 바탕으로 품질 및 성과와 관련된 금융회사의 각 요구는 서면 위탁 계약 및 서비스 수준 계약에 반영되어야 한다. 이러한 보안 측면 또한 지속적으로 모니터링 되어야 한다(가이드라인 7).

16) 앞 단락의 목적 상, 금융회사는 위탁하기 전에 관련 결정을 알리기 한 목적으로 최소한 다음을 수행해야한다.

(a) 민감도와 보호 필요성에 따라 프로세스 및 관련 데이터와 시스템을 식별 및 분류
(b) 위험기반 평가를 통해 클라우드 제공자에게 위탁하려는 업무, 프로세스 및 관련 데이터와 시스템 선정
(c) 데이터 및 시스템에 대한 적정한 보호수준을 정의하고, 전송 중 데이터, 메모리 내 데이터 및 유휴 데이터 등에 대해 암호화 조치 등을 고려

17) 그 결과, 금융회사는 클라우드 서비스 제공 업체와 서면으로 계약을 맺도록 해야 하며, 무엇보다도 제16조 (c)항에 의거한 클라우드 업체의 의무가 명시되어있다.

18) 금융회사는 CEBS 가이드라인의 가이드라인 7에 따라 활동 및 보안 조치의 성과를 지속적으로 모니터링하고 업무 위탁이 이전 문단을 준수하는지 여부를 적절하게 검토해야 한다. 금융회사는 신속하게 필요한 시정 조치를 취해야 한다.

2. (미국-FFIEC) 아웃소싱 클라우드 컴퓨팅 - 5. 정보 보안

다른 형태의 아웃소싱과 마찬가지로, 클라우드 컴퓨팅 모델에서 정보 보안은 주요 고려 대상이다. 금융 기관은 클라우드 컴퓨팅 서비스 제공 업체와 관련 업무를 통합하기 위해 정보 보안 정책, 표준 및 관행을 수정해야 할 수도 있다. 위험도가 높은 상황에서는 금융 기관이 서비스 제공 업체가 효과적인 통제를 유지하고 있다고 충분히 확신할 수 있도록 지속적인 모니터링이 필요할 수 있다.

금융 기관이 효과적인 ID 및 액세스 관리를 통해 포괄적인 데이터 목록 및 적절한 데이터 분류 프로세스를 유지하고 고객 데이터에 대한 액세스를 적절하게 제한하는 것이 중요하다. 여러 클라이언트가 네트워크 리소스를 공유하는 멀티 테넌트(multi-tenant) 클라우드 배치는 암호화와 테넌트의 접근을 각자의 데이터로만 제한하기 위해 적절히 통제 한다는 추가적인 보장을 통해 데이터 보호의 필요성을 높인다. 데이터 처리 절차, 백업 데이터의 적합성 및 가용성, 여러 서비스 제공 업체가 시설을 공유하고 있는지 여부를 확인하는 것이 주요 고려 사항이다. 금융 기관이 데이터가 만족스럽게 보호되고 데이터에 대한 액세스가 적절히 통제되고 있다고 확신하지 못하는 경우, 서비스 업체와 제3자 관계를 체결하는 것이 바람직하지 않을 수 있다. 클라우드에 데이터를 저장하면 보안 사고의 빈도와 복잡성이 높아질 수 있다. 따라서 금융 기관의 관리 프로세스는 금융 기관 및 서비스 제공 업체의 네트워크에 대한 보안 관련 위협, 사건 및 사건에 대한 효과적인 모니터링 방안; 포괄적인 사고 대응 방법론; 조사 및 증거 수집을 위한 적절한 포렌식 전략의 유지 방안을 포함해야한다.

서비스 계약 체결 시 데이터가 서비스 제공 업체의 저장 매체에서 완전히 제거되거나 삭제되지 않을 가능성은 전통적인 형태의 아웃소싱보다 클라우드 컴퓨팅 환경에서 더 큰 위험을 초래할 수 있다. 타사 관계를 시작하기 전에 클라우드 컴퓨팅 서비스 공급자가 NPPI가 저장된 모든 위치에서 NPPI를 제거 할 수 있도록 하는 것이 좋다.

3. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 〈위탁 시 고려사항〉 中

[위험관리]

위탁 관련 규칙 및 지침의 기본 원칙은 기업이 위탁 계약으로 인해 발생한 위험을 식별하고 관리한다는 것이다. 따라서 기업은 다음을 수행해야한다.

- 관련 위험을 식별하고 위험을 완화하기 위한 단계를 식별하기 위해 위험 평가를 시행해야 한다.
- 위험 평가를 문서화해야 한다.
- 데이터 및 정보 보안 관리 시스템 요구 사항, 사이버 위험 및 관련 규제 기관의 규칙과 지침을 포함하여 현재 업계의 우수 사례를 파악하여 의사 결정 시 참고한다.
- 서비스를 제공하거나 이용하는 데 관련된 고객, 기업 및 직원이 서로 다른 위치 또는 관할 구역 (예: UK, EEA 또는 비 EEA)에 있는 경우, 법 및 규제 관련 위험이 다른지 검토해야 한다.

• 기업이 책임지는 규제 서비스와 관련된 전반적인 운영 위험을 평가하고 이를 관리하도록 책임을 할당해야 한다.
• 집중 위험(concentration risk)을 모니터링하고 위탁 제공자가 실패할 경우 취할 조치를 고려해야 한다.
• 사업 복구 계획 발의안을 포함하여 발생하는 모든 위반 사항 또는 기타 관련 사건에 대해 신속하고 상세한 통지를 요구해야 한다.
• 계약서가 위반 사례 및 기타 유해 사례를 개선할 수 있는지 확인해야 한다.

[데이터 보안]

기업은 서비스 제공자와 기업이 관리하는 기술 자산을 포함한 보안 위험 평가를 수행해야한다. 기업은 다음을 수행해야한다.

• 서비스 제공자와의 관계를 체결하면 기업의 데이터를 저장, 처리 및 관리 할 수 있는 관할권을 설정하는 데이터 레지던시 정책에 동의해야 한다. 이 정책은 주기적으로 검토해야 한다.
• 서비스 제공자의 데이터 손실 및 침해 통지 프로세스를 이해하고 기업의 위험 수용범위 및 법적 또는 규제적 의무 사항과 부합하는지 확인해야 한다.
• 데이터를 어떻게 분리할 지 고려해야 한다(퍼블릭 클라우드를 사용하는 경우).
• 보안 위험을 완화하기 위한 적절한 조치를 취하여 기업의 전반적인 보안 문제를 수용할 수 있도록 해야 한다.
• 데이터 민감도 및 데이터 전송, 저장 및 암호화 방법을 고려해야 한다.

[변경 관리]

프로세스와 절차가 변경되면 위험이 발생할 수 있다. 우리는 기업이 포괄적인 변경 관리 프로세스를 수행할 것으로 기대하지만, 다음 사항에 특히 유의해야한다.

• 기술 서비스 제공의 변화를 위한 조항 마련
• 변경 사항에 대한 테스트 수행 방법을 수립

3. (싱가포르-ABS) 클라우드 컴퓨팅 구현 가이드 - Section 4. 클라우드 위탁 시 주요 통제 권고 사항

1) 암호화

• 데이터 백업을 포함하여 모든 민감한 데이터는 저장 및 처리 상태 모두에서 적절한 암호화 제어를 받을 것
• 암호화 알고리즘, 해당 키 길이, 데이터 흐름 및 처리 논리에 대한 세부 사항은 전문가 검토를 통해 잠재적인 약점 및 노출 지점을 식별할 것
• 암호화 키의 생성, 저장, 사용, 폐기, 만료, 갱신, 보관에서 암호화 키의 수명주기를 관리하기 위한 세부 정책 및 절차를 마련할 것
• 보안 키가 HSM (Hardware Security Module) 내에서 안전하게 생성되고 관리되도록 하려면 암호화 키에 대해 엄격한 제어를 수행할 것
• 암호화 키와 HSM의 위치, 소유권 및 관리에 대한 세부 사항은 금융회사와 CSP간에 합의할 것. 금융회사는 암호 키와 HSM를 직접 관리할 필요성과 역량을 검토할 것.
• HSM 및 기타 암호화 자료는 접근이 철저히 통제된 분리된 보안네트워크에 저장하고, CSP의 다른 고객이 사용하는 서브넷이나 직원 접근 구간에서 접근이 불가하도록 할 것
• CDN (Content Delivery Network)을 사용하는 경우 암호화 키 및 인증서 관리를 위한 적절한 제어가 있는지 확인할 것. 견고한 조직 신원 통제를 위해 EV(Extended Validation) 또는 OV(Organisation Validation) 인증서를 사용하는 것이 좋음. 안전한 인증서 관리 프로토콜도 고려되어야 함
• 금융회사에 속한 암호화 키 및 SSL 개인키 컨테이너를 CSP 환경에 도입해야하는 경우 적합한 키 의식(key ceremonies)을 포함하여 신중하게 설계된 프로세스를 마련해야함
• 금융회사 데이터의 암호화에 사용되는 암호화 키는 고유해야하며 클라우드 서비스의 다른 사용자와

공유하지 않아야 함
- 암호화 요구 사항에 대한 기타 지침은 MAS 기술 위험 관리 지침(MAS Technology Risk Management Guidelines)에서 가져올 것

2) 토큰화
- 토큰화 솔루션에 대해 신중한 위험 평가(risk assessment and evaluation)를 수행하여 고유한 특성을 식별하고, 민감데이터에 대한 모든 상호작용 및 접근을 식별해야함
- CSP는 토큰을 원래 데이터 값으로 복원할 수 있는 어떠한 수단도 없어야 함(토큰화 시스템 또는 토큰화 로직에 대한 접근이나 통제 수단 등)
- 토큰화를 수행하는 시스템은 금융회사가 직접 관리해야함

3) 전용 장비 또는 프라이빗 클라우드 : 특별히 민감한 자원이 사용되는 경우, 금융회사는 전용 장비 또는 프라이빗 클라우드를 고려할 수 있음. 이 경우 위치 및 데이터 제어 환경을 단순화할 수 있음
- 프라이빗 클라우드 구조를 계획할 때, CSP의 관리적·물리적 접근을 포함한 환경에 대한 모든 접근을 고려할 것
- 프라이빗 클라우드 구조를 계획할 때, CSP는 전용 하드웨어 및 위치를 계약을 통해 보장할 것
- 시스템 및 데이터의 백업 위치를 검토할 것. 모든 민감한 금융회사 데이터의 위치에 대해 데이터 레지던시(data residency) 요구사항을 고려할 것
- 보안 모니터링 제어가 환경의 격리를 보장하는지 확인할 것
- 송수신(ingress & egress) 트래픽 방화벽 규칙이 효과적인지 확인할 것
- 자산이 효과적으로 관리되고, 시스템이 노후화되지 않았는지 확인할 것

4) 변경 관리 및 특권 사용자 접근 관리(PUAM)
- 변경 관리 절차는 CSP와 금융회사 간에 상호 합의할 것. 이러한 절차에는 변경 요청 및 승인 절차, 보고 구성 요소 등을 포함하고, 공식화할 것
- 변경 관리 거버넌스는 일반 서비스 수준 관리 회의에 통합되도록 할 것
- 변경 관리의 역할, 책임 등 긴급 및 표준 변경 절차를 합의할 것
- 특권 사용자(users with privileged system access)는 명확하게 정의하고, 주기적인 사용자 접근 기록 검토를 받을 것(월 1회 권장)
- 특권 사용자 접근은 명확하게 추적되고 보고되도록 하고, 변경 요청 동의/승인에 연동되어야 함. CSP가 변경요청 기록을 금융회사에 공개할 필요는 없음.
- 모든 특권 사용자 접근은 모니터링하고, 주기적으로 동료 검토(peer review)를 받을 것. 이 검토 주기는 클라우드 내 자산의 중요도에 비례하게 설정.
- 특권 사용자 관리 기능 업무는 별도로 분장하여, 다른 사용자 관리 기능과 분리할 것

5) 가상 환경 보안 : HW, OS 이미지, 가상화 관리 SW(하이퍼바이저 등)에 대한 잠재적 위협을 고려할 것
- 가상 이미지 침투 테스트 실시
- 가상 이미지에 무결성 보장을 위한 제어 실시
- 관리 인터페이스는 운영 서브넷에서 접근할 수 없는 분리된 관리 네트워크에 위치할 것
- 암호화가 사용되는 경우, 암호화 키는 가상 이미지 및 정보 자산과 별도로 저장할 것
- 공격을 탐지하고 조기 경보를 제공하기 위해 보안 모니터링을 실시할 것

6) 사용자 접근 관리 및 의무 분리
- 식별 및 접근관리는 클라우드 아웃소싱 계약 수행 시 가장 중요한 고려사항이며, 기술 및 비즈니스 사용자 접근 관리를 모두 포함할 것. 책임 보장을 위한 명확한 사업주가 식별되어야하고, 정의된 각 역할의 소유권을 보장해야함
- 일관성을 유지하기 위해 금융회사의 식별 및 접근 관리 정책 및 표준은 CSP 내 해당 금융회사가

사용하는 모든 환경에서 적용되어야 함
- 최종사용자(특히 기업 사용자의 경우)는 액티브 디렉터리 자격 증명 절차를 사용하여 금융회사의 기존 프로세스 및 인프라를 활용할 수 있음
- 사용자 접근 관리는 업무분장 및 수행자/승인자(maker/checker) 통제를 확실히 할 것. 특히 CSP가 접근 권한이 있거나, 시스템 및 SW를 관리하는 경우 더욱 철저히 할 것. 역할 접근 권한의 변경 내역은 독립적인 감사 담당자가 정기적으로 검토할 것
- CSP가 금융회사의 시스템이나 SW에 접근할 수 있는 경우, 식별 및 접근 관리 문서에 기록해야하며, 요구사항의 정확도와 문서상의 설정이 시스템 상태와 일치하는지를 연1회 이상 검토할 것.
- 서비스, 일반 및 관리자 계정의 접근 및 사용은 적절한 특권 사용자 접근 관리 제어 및 활동을 통해 관리하고, 모든 활동은 추후 검토를 위해 기록할 것
- 클라우드에 개발, 품질보증 및 생산 환경이 있는 경우, 접근을 엄격하게 통제할 것. 개발자 및 테스터는 생산 환경에 쓰기 권한이 없어야하고, 생산 지원자는 책임 영역에 따라 읽기 접근을 제한할 것

7) 합동 재해복구 훈련
- CSP는 재난 복구 및 비즈니스 연속성 계획을 개발하고 계획을 금융회사와 공유할 것
- CSP는 필요한 인증(예: ISO27001, ISO27018)을 획득해야하며 해당 프로세스는 독립적인 제3자가 감사하고, 금융회사가 이 감사 보고서를 확인할 수 있을 것
- CSP와 금융회사 직원을 모두 포괄하는 통신 계획 또는 자동 전화 구조(automated call tree)를 만들 것
- 금융회사의 위기 관리 팀이 CSP의 복구 계획을 완전히 알고 있는지 확인할 것
- CSP와 DR 테스트를 수행 할 때, 실제 재해 이벤트에 대한 준비 수준을 확인하기 위해 현장 점검 또는 직전에 통지한 훈련을 수행할 것
- 테스트 중 명시된 결함을 기록하고 서비스 관리 회의를 통해 시정 조치를 모니터링할 것

8) 보안 모니터링 및 사고 관리
- 클라우드 서비스의 보안 및 안정성에 영향을 줄 수 있는 활동을 분석하기 위해 네트워크, 시스템 및 응용 프로그램 수준에서 적절한 탐지 메커니즘을 마련할 것
- 다양한 모니터링 시스템에서 보안 로그의 자동 분석, 상관관계 및 분류를 제공하기 위해 SIEM 시스템과 같은 적절한 모니터링 인프라가 있어야 함
- 가능한 경우 CSP의 SIEM 아키텍처의 데이터를 금융회사의 핵심 침입 탐지 기능에 활용하는 방법도 고려할 수 있음
- 로그의 무결성 및 가용성이 유지되도록 로그를 독립적인 시스템에 보관하는 등 안전하고 강력한 보안 로깅 인프라를 마련할 것
- 네트워크 침입 탐지/방지 시스템(NIDPS), 웹 방화벽(WAF), DDoS 장비 및 데이터 유출 방지 시스템과 같은 적절한 보안 시스템 및 조치를 전략적 위치에 배치하여 보안 침해 및 지속적인 공격을 탐지하고 완화할 것
- 아웃소싱 계약의 중요도에 따라, 보안이벤트의 능동적인 모니터링과, 보안 사고에 대한 시기적절한 대응을 위해 24x7 기반으로 운영되는 보안 운영 센터(Security Operations Center, SOC)를 강력하게 권장할 것
- 컴퓨터사고대응팀(CERT) 또는 보안사고대응팀(SIRT)을 구성하여 보안 사고에 대해 적시 대응할 것. CSP와 금융회사 팀 간의 역할 분담 및 조정을 공식화할 것
- 보안 사고의 정의와 심각도에 대한 수준을 금융회사와 CSP 간에 적절히 정의하고 합의할 것
- 보안 사고의 보고 레벨, 통보, 봉쇄 및 종결을 위한 기준 및 성능 요구 사항(SLA)을 금융회사와 CSP간에 적절히 정의하고 합의할 것

- 보안 사고 대응 계획 검토 및 테스트는 CSP에 의해 정기적으로 수행되어야하며 적절한 경우 금융회사를 참여시킬 것
- 보안 사고 및 근본 원인 분석 관련 보고서 접근 권한에 대해 금융회사와 CSP 간에 합의할 것. 상업, 보안 또는 지적재산권을 이유로 CSP가 해당 보고서를 금융회사에 공개하지 않을 경우, 상호 수용할 수 있는 제3자가 접근하도록 합의할 수 있음

9) 침투테스트 및 취약점 관리 : 외부 서비스 애플리케이션을 운영 또는 고객 정보를 처리하는 경우 주기적인 취약점 점검 및 침투테스트 필요

- CSP 침투테스트 보고서는 기본 시스템의 보안에 대한 확신을 얻는 데 사용할 수 있음. 다만, 침투테스트 범위에 서비스 제공 관련 모든 시스템을 포함하고 있는지 확인할 것
- 테스트 시 하이퍼바이저 점핑(hypervisor jumping), 취약한 API와 같이 클라우드 컴퓨팅 고유 위협을 고려할 것
- 테스트 수행자는 클라우드 환경 및 가상화에 특화된 보안 이슈를 인식하여 이러한 환경에서 발생할 수 있는 문제의 유형을 파악할 것
- 금융회사는 테스트의 기술적 한계를 확인하기 위해 취약점 점검 및 침투테스트 실시 전에 CSP와 협의할 것
- 모든 취약점에 대해 위험을 평가하고, 추적 및 적절히 관리/조치 할 것
- 식별된 취약점의 조치에 CSP가 책임이 있는 경우 이는 계약서에서 합의된 SLA/기한 내에 조치할 것

10) 관리용 원격 접근 : 원격 접근(CSP의 시스템 관리를 위한 원격 접근, 금융회사의 클라우드 환경 플랫폼 및 시스템에 대한 원격 접근)은 리스크를 유발하므로 엄격하게 관리해야 함

- 모든 시스템 원격 접근 절차(보안 통제 관리 절차 포함)에 대한 자세한 문서를 제작할 것. 정확성과 최신성을 보장하기 위해 이 문서를 정기적으로 검토할 것
- 클라우드 컴퓨팅 인프라에 대한 모든 인터페이스를 가능한 한 일관성 있게 유지하여 원격 접근 통제가 균일하게 적용되도록 할 것.
- 이러한 인터페이스는 별도의 분리된 데이터 흐름을 제공하여 안전하고 감사 가능한 시스템 및 데이터 접근 방법을 보장할 것
- 투팩터 인증, VPN 암호와와 같은 원격 접근 보안 수단을 구현할 것
- 가능한 경우, 원격 접근 네트워크 트래픽은 정의된 출발지와 목적지를 갖고 있을 것.
- 최종 사용자 컴퓨팅 장치 제어 실시(예: 기계 인식을 이용한 하드웨어를 통한 인증, 가상 데스크톱 인터페이스를 이용하여 악성코드 및 무권한 접속 위험 감소 등)
- 특권 사용자의 원격 접근은 승인된 예외 또는 긴급상황(break glass procedures)에서만 허용되어야 하며 시간 제한을 둘 것. 특권 사용자의 원격 접속은 본질적으로 위험하므로 엄격하게 제어할 것
- 모든 특권 사용자의 원격 접근은 독립된 자격있는 직원이 적합성을 검토해야함

11) 안전한 SW 개발 라이프사이클(SDLC) 및 코드 리뷰 : 온프레미스 환경과는 다르게 개발 라이프사이클이 관리되어야함. 데이터의 안전한 소거 및 환경 정리가 반드시 고려되어야 함

- 콘텐츠 버전 관리 및 한 환경에서 다른 환경으로의 소스코드 마이그레이션을 위한 엄격한 프로세스 관리 절차를 명확하게 정의하고, 릴리즈 관리 프로세스의 일부로 관리할 것
- 코드 배치를 위한 업무 분장을 명확히 할 것
- 소스 코드 저장소에 대한 접근과 개발 및 테스트 환경에 대한 특권 접근은 일부 승인된 직원 개인으로 제한할 것
- 암호화되지 않은 실 업무 데이터는 클라우드 환경에서 테스트용으로 사용 금지. 테스트 데이터는 CSP 환경으로 전송되기 전에 비식별화할 것
- 환경에 대한 운영 체제 이미지는 엄격하게 통제할 것

- 소스 코드가 중요한 목적으로 사용되는 경우, 위험도 평가를 수행하여 필요한 경우 금융회사 자체 네트워크에서 바이너리를 컴파일한 후 바이너리를 클라우드에 복사하여 사용할 것

12) 로그 및 백업 보안

- 금융회사는 CSP와 협력하여 서비스의 로깅 기능을 이해하여 "원치 않은" 데이터 로깅이 없음을 확인할 것
- 포렌식에 적합한 로그 데이터 획득 방법 등을 포함한 포렌식 조사 요구사항을 수립할 것
- 백업 및 로그 데이터를 위한 적절한 접근 통제를 실시할 것
- 금융회사는 백업할 내용을 선정하고, 적절한 경우 민감한 데이터를 암호화할 것
- 금융회사는 백업 목적으로 사용 된 암호화 키를 충실히 관리할 것
- 데이터 복원 기능을 정기적으로 테스트하고, 이러한 테스트는 데이터 유출 위험을 최소화하기 위해 안전하게 수행할 것

[서비스 시나리오별 클라우드 보안 지침]

시나리오	암호화 및 토큰화	전용 장비	변경 관리 및 PUAM	가상환경 보안	UAM 및 업무 분장	합동 재해 복구 훈련	보안 모니터링/ 사고관리	침투 테스트/ 취약점 분석	관리용 원격 접근	안전한 SDLC 및 코드 리뷰	로그 및 백업 보안
인터넷 뱅킹/ 지급 포털	◎	◎	◎	◎	◎	◎	◎	◎	◎	○	◎
CRM	◎	△	◎	◎	◎	◎	◎	◎	◎	○	◎
사기 방지 서비스	◎	△	◎	◎	◎	◎	◎	◎	◎	○	◎
HR 포털	◎	△	◎	◎	◎	◎	◎	◎	◎	○	◎
데이터룸	◎	△	◎	◎	◎	△	◎	◎	◎	○	○
서비스 관리	◎	△	◎	◎	◎	◎	◎	◎	◎	○	○
마이크로사이트	△	△	◎	◎	◎	△	◎	◎	◎	○	○
설문	△	△	◎	◎	◎	△	◎	◎	◎	○	△
데이터 분석	◎	△	◎	◎	◎	○	◎	◎	◎	○	○
이메일 보안 제품	◎	△	◎	◎	◎	◎	◎	◎	◎	○	◎
보안 운영 센터(SOC)	◎	△	◎	◎	◎	◎	◎	◎	◎	○	◎
인증 서비스	◎	△	◎	◎	◎	◎	◎	◎	◎	○	◎
테스팅	△	△	△	○	◎	△	○	◎	◎	△	○
개발 운영	△	△	△	○	◎	△	○	◎	◎	△	○
컨텐츠전달 네트워크 (CDN)	△	△	◎	◎	◎	◎	◎	◎	◎	△	○

* ◎: 강력 권고, ○: 권고, △: 금융회사 재량

4 업무 위수탁 운영기준 마련

금융회사는 클라우드서비스 이용 시 자체 업무 위수탁 운영기준을 마련하고 준수해야한다.

▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**

① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.

3. 〈별표 2의3〉에서 정하는 사항을 반영한 **자체 업무 위수탁 운영기준의 마련 및 준수**

금융회사는 업무 중요도 평가 결과 중요도가 높은 업무를 위탁하는 경우 관련 규정*에 따라 기 수립·운영 중인 자체 업무 위수탁 운영기준에 〈감독규정 [별표 2의3]〉 업무위탁 운영기준 보완사항을 반영하고 이를 준수해야 한다. 또한, 중요도가 낮은 업무를 위탁하는 경우 금융회사 필요에 따라 자체적으로 판단하여 반영한다.

* 「자본시장법」 제42조제7항 또는 「금융기관의 업무위탁 등에 관한 규정」 제3조의2

〈감독규정 [별표 2의3]〉

업무위탁 운영기준 보완사항

금융회사 및 전자금융업자가 클라우드컴퓨팅서비스 제공자에게 규정 제14조의2 제3항 각호에 해당하는 정보처리 업무의 위탁을 추진하는 경우 「자본시장과 금융투자업에 관한 법률」 제42조제7항에 따른 업무위탁 운영기준 또는 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따른 자체 업무위수탁 운영기준에 다음 각 호의 사항을 반영하고 이를 준수하여야 한다.

1. 위수탁계약의 결정·해지 절차 및 재위탁에 관한 사항

- 위탁업무에 대한 자체 중요도 평가 실시에 관한 사항
- 재위탁 및 재위탁의 변경 시 동의에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항 통보에 관한 사항

2. 위탁업무의 모니터링에 관한 사항

- 정보처리의 물리적 위치에 관한 사항

- 클라우드서비스 제공자의 보안관리 수준 등에 관한 사항
- 유·무형의 위탁업무 처리에 관한 최신 정보 등록·관리, 위탁업무의 품질 또는 서비스수준 등에 관한 사항

3. 비상대책 등에 관한 사항

- 합병·분할, 계약상 지위의 양도, 재위탁 등 중요 상황 발생시 대책(업무 연속성 계획 포함)에 관한 사항
- 위탁업무를 다른 수탁자 또는 클라우드컴퓨팅 업무를 위탁한 금융회사 및 전자금융업자에 이전시키는 경우 업무 장애·서비스지연, 이전을 지원할 의무 등 전환계획에 관한 사항
- 위탁계약의 종료, 중단, 변경 시 데이터 반환·파기에 관한 사항

4. 위탁업무 관련 조사·접근권 확보에 관한 사항

- 감독당국 또는 내외부 감사인의 조사·접근권(현장방문 포함) 확보에 관한 사항

5. 위수탁 계약서 주요 기재사항

- 클라우드컴퓨팅서비스가 제공되는 물리적 위치
- 재위탁 또는 재위탁의 변경 등 금융회사 또는 전자금융업자의 동의가 필요한 사항
- 위탁하는 업무, 데이터에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 등 금융회사 또는 전자금융업자에 대한 통보가 필요한 사항
- 감독당국 또는 내외부 감사인의 조사·접근(현장방문 포함) 수용 의무
- 계약의 파기 또는 종료, 기타 위탁업무의 원활한 이행이 어려운 경우 해당 위탁업무의 이전 및 반환 등에 관한 사항
- 위탁 및 위탁업무 관련 준거법 준수의무 및 자율규제에 대한 협조
- 비상대응훈련(재해복구전환훈련 포함), 취약점 분석·평가, 침해사고대응훈련 등의 협조에 관한 사항
- 위탁업무 모니터링 지원에 관한 사항
- 전송 정보에 대한 정보보호 의무 및 서비스 연속성 보장 등의 보안 요구사항
- 재위탁 관련 클라우드서비스 제공자의 관리·감독 의무에 관한 사항
- 재위탁 또는 재위탁 변경에 따른 보안리스크 증가 등 서비스에 악영향을 미칠 수 있는 경우 원위탁자의 계약해지 권한 보유에 관한 사항

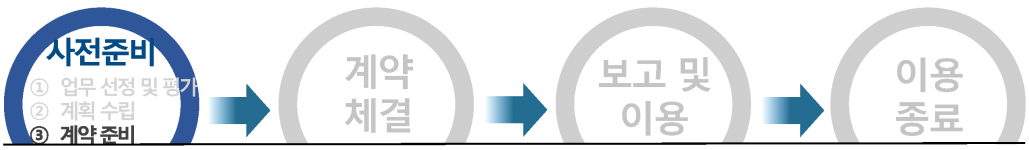
금융분야
클라우드컴퓨팅서비스
이용 가이드

제 5 장

계약 준비

1. 클라우드서비스 제공자 평가
2. 정보보호위원회 심의·의결

제 5 장 계약 준비



- 클라우드서비스 제공자 선정 전 평가
- 계약 체결 전 정보보호위원회 심의·의결

1 클라우드서비스 제공자 평가

- 「[부록] 금융분야 클라우드컴퓨팅서비스 제공기준」에 따라 클라우드서비스 제공자를 평가하고, 그 결과에 따라 계약 추진 및 이용 여부를 최종 결정하여야한다.

> ▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**
> ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.
> 2. 〈별표 2의2〉의 항목을 포함한 클라우드컴퓨팅서비스 **제공자의 건전성 및 안전성 등 평가**

- 또한, 고유식별정보 또는 개인신용정보를 처리하는 업무의 경우, 해당 정보를 처리하는 모든 시스템(해당 정보가 일시적으로 처리되는 시스템 포함*)을 국내에 설치하여야 하고,

  * 해당 정보가 처리되는 경우 관리시스템도 포함됨

  - 해당 전산실 내에 무선통신망이 설치되어있지 않아야 한다는 점을 고려하여 제공자를 선정한다.

※ 정보처리시스템 국내 설치 예외

- 개정된 감독규정 시행('19.1.1.) 이전에 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따라 정보처리 업무를 국외 소재 전산센터에 위탁하여 클라우드서비스를 이용하고 있는 경우 예외(감독규정 부칙 제2조)
- 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 감독규정 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자(국내 설치 요건 및 무선통신망 설치 금지 예외)

▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등)

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 전자지급결제대행업자는 제외한다)가 **제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.**

참고 주요국 금융권 지침 내 제공자 평가 관련 부분

1. (미국-FFIEC) 아웃소싱 클라우드 컴퓨팅 - 2. 상당한 주의(Due Diligence)

금융 기관이 전략 계획을 달성하기 위해 제3자를 사용한다고 해서 제3자 활동이 안전하고 건전한방식으로, 그리고 관련 법률 및 규정을 준수하여 수행되는지 확인하는 이사회 및 경영진의 책임이 줄어들지 않는다.
클라우드 서비스 공급자에게 아웃소싱하는 것은 비용 절감, 유연성, 확장성, 향상된 부하 균형 조정 및 속도와 같은 잠재적인 이점 때문에 금융 기관에 유리할 수 있다. 중요한 기능의 위탁을 승인하기 전에, 이러한 조치가 이사회 및 고위 경영진이 승인한 해당 기관의 전략 계획 및 회사 목표와 일치하는지 확인하는 것이 중요하다.
Outsourcing Booklet에 자세히 나와 있듯이 제공자가 비용, 서비스 품질, 규제 요구 사항 준수 및 위험 관리 측면에서 기관의 요구 사항을 충족하는지 확인하기 위해 실사 검토가 수행된다. 클라우드 컴퓨팅과 관련된 잠재적인 문제는 다음과 같다.

- 데이터 분류(Data classification)
  - 클라우드에 배치 될 데이터 (예: 기밀, 중요, 공개)의 민감도
  - 적절히 보호되고 있음을 보장하기 위해 어떤 통제를 사용해야 하는가
  - 클라우드 서비스 제공 업체가 비공개 개인 정보(NPPI) 및 기관이나 고객에게 해를 끼칠 수 있는 기타 데이터를 적절하게 암호화하거나 보호하는가
- 데이터 분리(Data segregation)
  - 금융 기관의 데이터가 다른 클라우드 클라이언트의 데이터와 리소스를 공유하는가.
    예를 들어 데이터가 동일한 네트워크를 통해 전송되고 다른 클라이언트에서도 사용되는 서버에 저장 및 처리되는가

- 그러하다면 서비스 제공 업체는 금융 기관의 데이터의 무결성과 기밀성을 보장하기 위해 어떤 통제를 해야하는가

• 복구 가능성(Recoverability)
- 서비스 제공 업체는 재해에 어떻게 대응하고 지속적인 서비스를 보장하는가
- 금융 기관의 재해 복구 및 비즈니스 연속성 계획에는 이러한 형태의 아웃소싱, 서비스 제공 업체의 재해 복구 및 비즈니스 연속성 계획, 필수적인 커뮤니케이션 링크의 가용성에 대한 적절한 고려가 포함되어 있는가

2. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 〈위탁 시 고려사항〉 中

[서비스 제공자 감독]

기업은 규제 체제 하에서 모든 의무를 완수할 책임이 있으며, 책임을 서비스 제공자에게 위임할 수는 없다. 기업은 다음 사항을 고차원적으로 수행해야한다.

• 제공받는 서비스를 명확히 밝히고, 기업과 서비스 제공자(들) 간의 책임과 의무가 어디서 시작되고 끝나는지 명확히 밝혀야 한다.
• 서비스 제공자의 일상적인 관리와 전략적 관리에 대한 책임을 할당해야 한다.
• 직원이 위탁 업무를 감독하고 테스트할 수 있고 발생하는 위험을 식별, 모니터링 및 완화할 수 있으며 기존 제3자 제공자의 해약 또는 이전을 적절하게 관리하기 위해, 충분한 기술과 자원을 갖추고 있는지 확인해야 한다.
• 분쟁 해결을 위한 적절한 조치가 존재하는지 확인해야 한다.

3. (싱가포르-MAS) 아웃소싱 가이드라인 - 5.4 서비스 제공업체 평가

5.4.1 아웃소싱 계약을 재협상 또는 갱신하기 위해 고려 중일 때 기관은 서비스 제공업체를 대상으로 적절한 실사를 실시하여 아웃소싱 계약과 관련된 리스크를 평가해야 한다.

5.4.2 기관은 서비스 제공업체의 모든 관련 측면을 평가해야 한다. 예를 들어 아웃소싱 계약을 이행할 때 해당 서비스를 기관에서 직접 수행하는 것과 같이 높은 관리 수준을 적용하여 규제 대상 기관으로서의 의무에 부합할 수 있는 역량의 보유 여부 등이 대표적이다. 실사를 할 때에는 서비스 제공업체가 갖추고 있는 물리적, IT 보안 관리 실태, 서비스 제공업체의 업계 평판 및 재무 안정성(서비스 제공업체의 윤리적, 전문적 표준 포함) 및 아웃소싱 계약에 따라 부과되는 의무를 이행할 수 있는 능력 등도 감안해야 한다. 서비스 제공업체 현장 방문 및 서비스 제공업체에 대한 독립적인 검토 및 시장 피드백(가능한 경우)도 획득하여 기관의 평가를 보완해야 한다. 현장 방문은 평가를 실시하는 데 요구되는 필수적인 지식과 기술을 보유한 인물이 수행해야 한다.

5.4.3 실사에는 서비스 제공업체와 관련된 모든 주요 정보를 평가하는 과정이 포함되어야 한다. 평가 대상 정보로는 서비스 제공업체의 다음과 같은 정보가 포함된다.

(a) 계약 기간 내 아웃소싱 계약을 이행하고 지원할 경력 및 역량
(b) 재무 안정성 및 리소스(실사는 비즈니스 전략 및 목표, 감사를 받은 재무제표, 주요 지분 후원사의 계약 안정성 및 불리한 조건에서도 서비스 약속을 이행할 수 있는 능력 등을 검토한 결과를 근거로 서비스 제공업체의 생존 능력을 판단하는 신용 평가와 비슷하게 실시해야 함)
(c) 기업 관리, 업계 평판 및 사내 문화, 규정 준수 및 보류 중이거나 발생 가능한 송사
(d) 보안 및 내부 통제, 감사 적용 범위, 보고 및 모니터링 환경
(e) 리스크 관리 프레임워크 및 역량 - 예를 들어 아웃소싱 계약과 관련된 기술 리스크 관리6 및 비즈니스 연속성 관리7 등
(f) 재해 복구 준비성 및 재해 복구 전적

(g) 하도급 계약업체의 성공적인 운용 여부 및 하도급 계약업체에 대한 의존도
(h) 보험 적용 범위
(i) 외부 환경(예: 서비스 제공업체가 사업 활동을 영위하는 사법권의 정치, 경제, 사회 및 법적 환경)
(j) 관련 법률 및 규정을 준수할 역량 및 관련 법률과 규정을 준수하는 것과 관련된 전적

5.4.4 또한 기관은 자사 아웃소싱 계약의 일부분을 담당하는 서비스 제공업체 소속 직원들이 기관에서 해당 직무 역할을 수행하는 담당자를 채용할 때 적용하는 채용 정책(자사 직원에 적용되는 기준과 일관성 있음)에 부합하는지 확인해야 한다. 다음은 이 평가에서 고려해야 하는 사항을 몇 가지 예로 들어본 것이다(전체가 아님).
(a) 징계 또는 형사 처벌의 성격을 지닌 각종 법적 절차의 대상이 된 경험 여부
(b) 각종 불법 행위의 유죄를 인정받은 전적이 있는지 여부(특히 사기, 사칭 또는 부정행위 관련 사건)
(c) 사기 또는 사칭 행위로 인한 민사상 책무를 인정한 적이 있는지 여부
(d) 재정적으로 건실한 인물인지 여부
이 평가에서 불리한 사실이 발견되는 경우 이는 아웃소싱 계약과의 관련성과 계약에 미치는 영향력이라는 측면에서 고려해야 한다.

5.4.5 평가 프로세스 중에 실시하는 실사는 문서로 기록해야 하며 아웃소싱 계약의 모니터링 및 관리 프로세스의 일환으로 정기적으로 다시 수행해야 한다. 실사 프로세스는 성격에 따라 다양한 형태를 띨 수 있으며, 계약의 리스크 정도와 서비스 중단 또는 보안과 기밀성 침해 등이 기관에 미치는 영향 등에 따라서도 달라질 수 있다(예: 아웃소싱 계약을 기관 산하 그룹 내부에서 체결하는 경우 축소된 실사만으로 충분할 수 있음8). 기관은 실사 평가에 충분히 최신 버전인 정보를 사용해야 한다. 또한 기관은 실사 평가에서 알아낸 사실을 감안하여 서비스 제공업체를 대상으로 감사를 실시할 빈도와 범위를 결정해야 한다.

2 정보보호위원회 심의·의결

금융회사는 중요도 평가 결과, 자체 업무 위수탁 운영기준 및 클라우드서비스 제공자 평가 결과에 대해 정보보호위원회를 개최하여 심의·의결하여야 한다.

▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**
② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 **정보보호위원회의 심의·의결**을 거쳐야 한다.

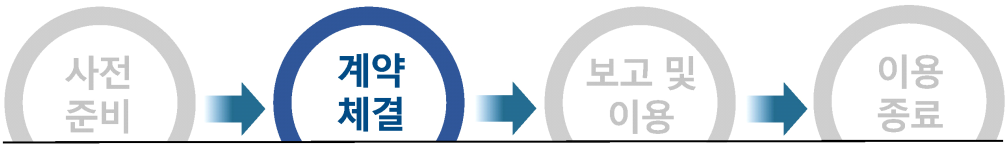
금융분야
클라우드컴퓨팅서비스
이용 가이드

제 6 장

계약 체결

1. 서비스 위탁 관련 명시사항
2. 보안 관련 명시사항
3. 출구 전략 이행을 위한 명시사항
4. 책임관계 명확화

제 6 장 계약 체결



✔ 금융회사의 안전한 계약 체결을 위한 계약서 필수 명시사항

계약 체결 시 요구사항을 적극 반영하기 위해서는 기업 계약서 작성(Enterprise Agreement) 방식이 유리하며, 클라우드서비스 제공자 약관 형태 계약(Click-through Agreement)은 비즈니스 시급성이 잠재적 리스크보다 우위일 때만 제한적으로 이용할 필요

▶ 감독규정 [별표 2의3] 업무위탁 운영기준 보완사항 中

5. 위수탁 계약서 주요 기재사항

- 클라우드컴퓨팅서비스가 제공되는 물리적 위치
- 재위탁 또는 재위탁의 변경 등 금융회사 또는 전자금융업자의 동의가 필요한 사항
- 위탁하는 업무, 데이터에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 등 금융회사 또는 전자금융업자에 대한 통보가 필요한 사항
- 감독당국 또는 내외부 감사인의 조사·접근(현장방문 포함) 수용 의무
- 계약의 파기 또는 종료, 기타 위탁업무의 원활한 이행이 어려운 경우 해당 위탁업무의 이전 및 반환 등에 관한 사항
- 위탁 및 위탁업무 관련 준거법 준수의무 및 자율규제에 대한 협조
- 비상대응훈련(재해복구전환훈련 포함), 취약점 분석·평가, 침해사고대응훈련 등의 협조에 관한 사항
- 위탁업무 모니터링 지원에 관한 사항
- 전송 정보에 대한 정보보호 의무 및 서비스 연속성 보장 등의 보안 요구사항
- 재위탁 관련 클라우드서비스 제공자의 관리·감독 의무에 관한 사항
- 재위탁 또는 재위탁 변경에 따른 보안리스크 증가 등 서비스에 악영향을 미칠 수 있는 경우 원위탁자의 계약해지 권한 보유에 관한 사항

▶ 금융기관의 업무위탁 등에 관한 규정 [별표3] 업무 위수탁 기준 中

7. 위수탁 계약서 주요 기재사항

- 위수탁업무의 범위(공급주기, 내용, 형태 등)
- 업무수행의 수단
- 정보제공 책임(수탁자 내부의 영업상 중요정보 포함)
- 수탁자에 대한 감사 권한
- 업무위수탁에 대한 수수료 및 보상금

- 위탁업무에서 발생하는 자료에 대한 위탁금융회사의 소유권과 당해 금융회사의 물적설비 및 지적재산권 등의 이용조건
- 고객정보의 보호 및 비밀유지에 관한 사항
- 업무의 연속성을 확보하기 위한 백업시스템 확보 등 비상계획
- 면책조항, 보험가입, 분쟁해결(중재, 조정 등) 방법
- 수탁자의 책임한계
- 계약의 파기 또는 종료(위탁금융회사의 계약해지권, 자료의 복구방법 등)에 관한 규정
- 감독당국의 검사 수용의무
- 재위탁시 발생한 손해에 대해 원위탁자의 연대배상책임에 대한 내용
- 수탁자가 업무 재위탁시 원계약 준수 명시
- 준거법 및 관할법원(업무위수탁 상대방이 외국에 소재하는 경우)
- 기타 업무위수탁에 따른 리스크관리 등을 위하여 필요한 사항 등

▶ 금융회사의 정보처리 업무 위탁에 관한 규정 제4조(정보처리의 위탁) 中

③ 금융회사는 제1항에 따른 정보처리 위탁계약을 체결할 경우 데이터에 대한 접근통제, 전산사고 등에 따른 이용자 피해에 대한 위·수탁회사간의 책임관계, 수탁회사에 대한 감독당국의 감독·검사 수용의무, 수탁회사의 분쟁해결 과정에서의 재판관할 등을 계약 내용에 반드시 포함하여 위탁에 따라 발생할 수 있는 책임관계를 명확히 하여야 한다.

클라우드서비스 제공자와 계약 시 아래 분야별 명시사항을 계약서 등에 포함하되, 업무 중요도 평가 결과에 따라 중요도가 낮은 업무의 경우 금융회사가 선택적으로 포함할 수 있다.

1 서비스 위탁 관련 명시사항

가. 서비스 범위 및 물리적 위치에 관한 사항

- 클라우드서비스를 이용하는 업무, 처리되는 데이터, 데이터가 처리되는 물리적 위치(시·군 단위까지 기재하고, 금융당국 요청 시 세부 위치 별도 제출) 명시
- 고유식별정보 또는 개인신용정보를 처리하는 경우, 해당 정보를 처리하는 모든 시스템(해당 정보가 일시적으로 처리되는 시스템 포함*)을 국내에 설치하여야 하고,

  * 해당 정보가 처리되는 경우 관리시스템도 포함됨

  - 해당 전산실 내에 무선통신망이 설치되어있지 않아야 함
- 금융회사의 데이터가 국외에서 처리되는 경우(고유식별정보·개인신용정보 이외) 정보 처리, 보안 관리 등에 대한 해당 국가의 법적 의무사항에 대해 사전에 파악하여 통지할 것
  - 관련 법적 의무사항이 신규 발생되거나 개정되는 경우 이를 파악하여 통지할 것

참고 주요국 금융권 지침 내 물리적 위치 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 - 4.6 데이터와 데이터 처리 위치

19) CEBS 가이드라인 4(4)에 명시된 바와 같이 금융회사는 감독 당국의 효과적인 감독에 있어 발생 가능한 데이터 보호 위험 때문에 EEA 외부에서 수행되는 위탁 계약을 체결하고 관리 할 때 특별한 주의를 기울여야한다.

20) 금융회사는 클라우드 환경으로 위탁할 때 데이터 및 데이터 처리 위치 고려 사항에 대해 위험 기반 접근 방식을 채택해야 한다. 평가는 법적인 위험 및 규정 준수 문제, 위탁 서비스가 제공되거나 제공될 가능성이 있는 국가 및 데이터가 저장되거나 저장 될 가능성이 있는 국가와 관련된 잠재적인 위험 영향을 다루어야 한다. 평가에는 해당 관할권보다 넓은 정치 및 보안 안정성에 대한 고려가 포함되어야 한다(해당 관할 구역에서 시행중인 법률 (데이터 보호에 관한 법률 포함). 클라우드 서비스 제공 업체의 실패 시 적용될 도산법(Insolvency law) 조항을 포함하여 해당 관할 지역의 법 집행 조항을 준수해야 한다. 금융회사는 이러한 위험이 위탁 업무의 중요성에 비례하여 허용 가능한 한도 내에서 유지 되도록 해야 한다.

2. (미국-FFIEC) 아웃소싱 클라우드 컴퓨팅 - 6. 법적, 규제, 평판 고려 사항

퍼블릭 클라우드 컴퓨팅 모델을 배포하기 전 금융 기관에 대한 주요 고려 사항에는 법률, 규제 및 평판 위험을 명확하게 식별하고 완화하는 것이 포함된다. 고객 데이터가 해외에서 저장되거나 처리될 수 있기 때문에, 클라우드 컴퓨팅의 특성상 관련 법규 준수의 복잡성이 증가할 수 있다. 클라우드 컴퓨팅 서비스 공급자가 해외에서 데이터를 처리 및 저장하거나 금융 기관의 데이터를 다양한 법률 및 규제 관할 구역 아래에서 운영되는 다른 고객의 데이터와 함께 사용하는 환경에서는, 규정을 평가할 수 있는 금융 기관의 능력이 더 복잡하고 어려울 수 있다.

금융 기관은 호스팅 국가 내의 법률 및 규정의 적용 가능성과 해당 데이터에 대한 액세스를 통제할 수 있는 금융 기관의 능력을 이해해야 한다. 클라우드 컴퓨팅 서비스 공급자와의 계약은 개인 정보 보호 법률 준수, 보안 사고에 대한 대응 및 보고, 고객 및 규제 당국에 위반 사실을 알리기 위한 규제 요구 사항 충족과 관련한 금융 기관의 책임에 대해 서비스 제공 업체의 의무를 명시해야 한다.

3. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 〈위탁 시 고려사항〉 中

[법·규제적 고려사항 中]

- 서비스 제공자의 사업장이 위치한 관할지와 그것이 기업의 위탁 계약에 어떤 영향을 미치는지 확인해야 한다.
- 서비스 제공자와의 계약이 영국의 관할권과 법률로 규제되는 지 알아야한다. 그렇지 않은 경우 기업, 감사원 및 관련 규제 기관이 데이터 및 사업장에 효과적으로 접근할 수 있어야한다. (데이터 및 사업장 접근에 관한 아래 섹션 참조)
- 개인정보 보호 규정(GDPR)을 통해 발생할 수 있는 추가 법적 또는 규제적 요구사항을 고려해야 한다.

[효율적인 데이터 접근 中]

- 영국 규제 당국이 효과적으로 접근할 수 없는 관할 구역에 데이터가 저장되지 않아야 한다. 관할 구역의 광범위한 정치적 및 안보적 안정성과 관할 구역에서 시행중인 법률(데이터 보호 포함), 관할 구역의 국제적 의무가 고려되어야 한다. 이는 사법 관할 구역 내의 법 집행 규정을 고려해야한다.

[개인정보보호규정(GDPR)]

기업은 개인정보 보호 규정(GDPR) 및 필요한 경우 데이터 보호법(2018)을 준수해야 한다. 데이터 보호

요구 사항은 FCA 안내서와 별도이며, 각 요구 사항은 별도로 충족해야 한다. GDPR은 정보 위원회(ICO, Information Commissioner's Office)가 감독한다. 따라서 기업은 클라우드 컴퓨팅에 관한 ICO의 지침 및 기타 관련 지침을 따라야 한다. 관련 있는 경우, 기업은 유럽 경제 지역 외부로 개인 정보를 전송하는 것에 대한 ICO 지침을 참고해야 한다.

4. (싱가포르-MAS) 아웃소싱 가이드라인 – 5.10 싱가포르 국외에서의 아웃소싱

5.10.1 외국에서 서비스 제공업체와 계약을 체결하거나 아웃소싱 된 직무 역할을 외국에서 수행하는 아웃소싱 계약의 경우, 외국의 경제적, 사회적 및 정치적 상황과 사건사고가 기관에 불리한 영향을 미칠 수 있는 국가적 리스크에 기관을 노출시킬 가능성이 있다. 그와 같은 상황과 사건사고로 인해 서비스 제공업체가 기관과의 계약서 약관대로 서비스를 이행할 수 없게 될 수 있다. 기관은 그러한 아웃소싱 계약의 리스크 관리 과정에서 실사의 일환으로, 지속적으로 다음과 같은 요인을 감안해야 한다.

(a) 정부 정책
(b) 정치적, 사회적, 경제적 상황
(c) 외국의 법적, 규제적 상황 전개 및
(d) 기관에서 서비스 제공업체를 효율적으로 모니터링하는 능력 및 자사 비즈니스 연속성 관리 계획과 출구 전략을 실행할 능력

또한 기관은 서비스 제공업체 측에서 아웃소싱 계약과 관련하여 정립한 재해 복구 계획 및 위치를 알고 있어야 한다. 정보 및 데이터를 외국의 주요 현장 또는 백업 현장으로 이동할 수 있기 때문에, 전송 매체와 관련된 리스크(실물 또는 전자 파일 등 형식 불문)도 감안해야 한다.

5.10.2 싱가포르 국외에 위치한 서비스 제공업체와 체결한 중요 아웃소싱 계약의 경우 MAS에서 기관의 싱가포르 국내 비즈니스 업무 활동을 감독 관리하는 업무(즉 장부, 계좌 및 문서)를 적시에 수행하는데 방해가 되지 않는 방식으로 체결하여 이행해야 한다. 특히 주의할 부분은 다음과 같다.

(a) 기관은 원칙적으로 기밀 유지 조항 및 협약을 대체로 지키는 사법권에서 비즈니스를 영위하는 서비스 제공업체에만 한정하여 아웃소싱 계약을 체결해야 한다.
(b) 기관은 서비스 제공업체에서 MAS 또는 MAS가 지명한 대행기관이 정보에 즉시 액세스하는 과정을 법무 또는 행정적 제약 사항에 의해 방해 받을 가능성이 있는 사법권에 소재한 서비스 제공업체와는 아웃소싱 계약을 체결하지 말아야 한다. 기관은 적어도 MAS에서 관련 정보를 요청하는 경우 즉시 서비스 제공업체로부터 해당 정보를 회수할 수 있도록 총력을 기울여야 한다. 기관은 MAS에 기관에서 아웃소싱 계약을 체결할 때 MAS에 서비스 제공업체를 점검할 권한을 제공하였으며, 기관과 서비스 제공업체의 아웃소싱 계약과 관련된 정보, 보고서 및 알아낸 사실 등의 데이터에 액세스할 권한을 허가하였음을(본문의 5.9단에 따라) 서면으로 확인해주어야 한다.
(c) 기관은 해외 권한 당국이 자사의 고객 정보에 대한 액세스 권한을 원하는 경우 또는 본문의 5.9단에 명시된 기관과 MAS의 액세스 권한이 제한 또는 거부되는 상황이 발생하는 경우 그러한 사실을 MAS에 알려야 한다.

나. 접근권 및 감사권 수용 의무에 관한 사항

- 금융당국, 침해사고대응기관, 금융회사 사내·사외 감사(정보보호담당자 포함) 및 금융회사가 임명한 제3자(이하 '금융당국 및 내외부 감사인')는 데이터센터 등 현장방문을 포함한 조사·접근을 수행*할 수 있음

  * 금융회사가 지정한 제3자의 감사보고서 검토로 내외부 감사인(금융당국, 침해사고대응기관 이외)의 조사·접근을 일부 대체할 수 있음

  - 클라우드서비스 제공자는 이를 수용하며, 현장방문, 관련 자료 제출 요구 및 검사에 적극 협조하여야 함

- 금융당국 및 내외부 감사인은 클라우드서비스에 이용되는 모든 범위의 장치, 시스템, 네트워크 및 데이터에 접근할 수 있음

- 금융당국은 클라우드서비스 제공자를 대상으로 감독·검사를 수행할 수 있고,

  - 내외부 감사인은 클라우드서비스 제공자를 대상으로 감사를 수행할 수 있으며, 필요 시, 다수 금융회사가 연합하여 합동(또는 합동 수행을 임명받은 제3자를 통해)으로 감사를 수행할 수도 있음

- 금융당국 및 내외부 감사인은 클라우드서비스 제공자에게 제3자 인증 또는 내부 감사 보고서의 제출을 요구할 수 있고,

  - 금융회사 업무와 관련된 대상에 대해 내부 감사 보고서의 보완을 요구할 수 있음

- 금융당국 및 내외부 감사인은 감독·검사 및 감사 수행 또는 인증·감사 보고서 검토 결과 지적된 사항에 대해 지체 없이 조치할 것을 요구할 수 있음

참고 주요국 금융권 지침 내 감사권 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 – 4.3 접근 및 감사권, 4.4 접근권 상세

[For 금융회사]

6) CEBS 가이드라인 8 (2) (g)와 클라우드 위탁의 목적에 따라 금융회사는 클라우드 서비스 제공자와 서면 계약을 맺고 있는지 확인해야한다. 서면 계약 후 클라우드 서비스 공급자는 의무를 이행한다.
   (a) – 금융회사,
      – 그 목적을 위해 금융회사로부터 임명된 제3자,
      – 영업장(본사 및 운영센터)에 접근 가능한 금융회사의 감사원
      에게 위탁 서비스를 제공하는 데 사용되는 모든 범위의 장치, 시스템, 네트워크 및 데이터를 제공할 의무(접근권)
   (b) – 금융회사,
      – 그 목적을 위해 금융회사로부터 임명된 제3자,
      – 금융회사의 감사원
      에게 위탁 서비스와 관련된 제한 없는 검사 및 감사권 부여
7) 접근권과 감사권의 효과적인 행사는 계약상의 약정에 의해 방해되거나 제한되어서는 안 된다. 감사의 수행이나 특정 감사 기법의 사용이 다른 고객의 환경에 위험을 초래할 수 있는 경우, 기관이 요구하는 유사한 수준의 보증을 제공하기 위한 대체 방법을 합의해야 한다.
8) 금융회사는 위험 기반 방식으로 감사 및 액세스 권한을 행사해야한다. 금융회사가 자체 감사 자원을 사용하지 않는 경우, 다음 도구 중 적어도 하나를 사용하는 것을 고려해야한다.
   (a) 동일한 클라우드 서비스 제공자의 다른 고객과 연합하여 합동감사팀을 조직하여 함께 수행하거나 제3자에 의해 수행하는 것을 고려(감사 자원을 더욱 효율적으로 사용하고 고객과 클라우드 서비스 제공자 모두의 조직적 부담을 줄이기 위하여)
   (b) 클라우드 서비스 제공자가 제출하는 제3자 인증 또는 아래 사항을 충족하는 클라우드 서비스 제공자의 내부감사 보고서 채택을 고려
      • 인증 또는 감사 보고서의 범위가 금융회사에 의해 주요사항으로 식별된 시스템(즉, 프로세스, 애플리케이션, 인프라, 데이터 센터 등) 및 통제를 포함하도록 보장한다.
      • 금융회사는 지속적으로 인증 또는 감사 보고서의 내용을 철저히 평가하고, 특히 핵심 통제가 차기 버전의 감사 보고서에서 다루어지고, 인증 또는 감사 보고서가 폐기되지 않았음을 확인한다.
      • 인증 또는 감사자의 적격성이 만족된다. (인증 또는 감사 회사의 교체, 전문성, 자격, 기본 감사 파일에 있는 증거의 재확인/검증)
      • 널리 인정된 표준에 따라 인증이 발급되고 감사가 수행되며, 주요 통제의 운영 효율성에 대한 테스트가 수행된다.
      • 금융회사가 시스템 또는 통제에 대해 인증 및 감사 보고서의 범위 확대를 요청할 수 있는 계약적 권한을 가진다. 범위 변경 요청의 횟수와 빈도는 합리적이어야 하며, 위험 관리 관점에서 타당해야 한다.
9) 클라우드 솔루션이 기술적으로 매우 복잡함을 고려하여, 금융회사는 감사를 수행하는 직원이 내부 감사원 또는 대신하여 감사를 수행하는 인력이거나 클라우드 서비스 제공자가 지정한 감사원임을 확인해야 한다. 또는 제3자 인증이나 서비스 제공 업체의 감사 보고서를 검토하는 직원이 클라우드 솔루션을 효과적이고 적절하게 감사 및/또는 평가를 수행하기 위해 올바른 기술과 지식을 획득했는지 확인해야한다.

[For 관할당국]

10) CEBS 가이드라인 가이드라인 8(2)(h)과 클라우드 위탁의 목적에 따라 금융회사는 클라우드 서비스 제공 업체와 서면으로 계약을 맺어야 한다. 서면 계약 후 클라우드 서비스 공급자는 의무를 이행한다.
   (a) 금융회사를 감독하는 관할 당국에게 클라우드 서비스 제공자의 영업장(본사 및 운영센터)에 대한

모든 접근을 허용한다. 이는 금융회사에 서비스를 제공하기 위해 사용되는 모든 범위의 디바이스, 시스템, 네트워크, 데이터를 포함한다.(접근권)

(b) 금융회사를 감독하는 관할 당국에게 위탁 서비스와 관련된 제한 없는 검사 및 감사권 부여한다. (감사권)

11) 금융회사는 계약상의 약정이 관할 당국이 감독 기능 및 목표를 수행하는 것을 방해하지 않도록 보장해야한다.

12) 관할 당국이 접근 및 감사권을 행사함으로써 얻는 정보는 Directive 2013/36/EU (CRD IV)제53조 이후에 언급 된 전문 비밀 및 기밀 유지 요건을 따라야한다. 관할 당국은 기밀 유지, 전문 비밀 및 정보 교환에 관한 연방법의 조항을 준수하지 못하게 하는 어떠한 종류의 계약 또는 선언을 하지 말아야한다.

13) 관할 당국은 감사 결과를 토대로 필요한 경우 금융회사에 직접 조치를 취하여 식별된 모든 결함을 처리해야 한다.

14) 제6항 및 제10항에 언급 된 협정에는 다음 규정이 포함되어야 한다.

(a) 접근 권한을 행사하려는 당사자(기관, 관할 당국, 감사관 또는 기관 또는 관할 당국을 위해 행동하는 제3자)는 계획된 현장 방문 전, 관련 사업장에 대한 현장 방문에 대하여 합리적인 기간에 통지한다. (응급 상황이나 위기 상황으로 인해 사전 통지가 불가능한 경우가 아니라면)

(b) 클라우드 서비스 제공 업체는 현장 방문과 관련하여 해당 관할 당국 및 기관 및 감사원과 완전히 협력해야 한다.

2. (미국-FFIEC) 아웃소싱 클라우드 컴퓨팅 – 3. 공급 업체 관리, 4. 감사

[공급 업체 관리]

클라우드 컴퓨팅 서비스 제공자를 관리할 때, 서비스 제공 업체가 고객 정보 및 기타 중요한 데이터를 보호하기 위한 금융 기관의 법률 및 규정 요구 사항에 익숙하지 않은 경우 추가 통제 사항이 필요할 수 있다. 또한 그러한 서비스 제공자를 이용하면 해당 기관이 감당할 수 없거나 완화할 수 없는 위험을 초래할 수 있다. 이러한 리스크의 한 예로 서비스 제공 업체가 규제 요구 사항을 충족하기 위한 변경 사항을 구현하지 않는 경우가 있다. 이러한 상황에서 경영진은 기관이 서비스 제공자를 고용할 수 없다고 판단할 수 있다. 서비스 제공 업체의 해약은 특히 소규모 금융 기관의 경우 클라우드 컴퓨팅에서 복잡해질 수 있는 공급 업체 관리의 또 다른 측면이다. 계약 및 서비스 수준 협약은 데이터의 소유권, 위치 및 형식 및 분쟁 해결에 대해 구체적이어야 한다.

[감사]

금융 기관은 제3자 서비스 제공자의 사용과 관련된 위험 및 위험 완화를 효과적으로 평가하기 위해 서비스 업체의 내부 통제의 적절성을 결정해야 한다. 감사원은 이러한 통제가 적절하게 기능하는지 여부를 평가하여 이를 지원한다.

금융 기관의 감사 정책 및 관행에 따라 아웃소싱 클라우드 컴퓨팅에 대한 수용 가능한 IT 감사 범위를 제공하기 위해 조정이 필요할 수 있다. 또한 공유 환경 및 가상화 기술을 평가하는 데 충분한 전문 지식을 갖춘 인력과 추가 교육을 받은 내부 감사원을 보강해야 할 수도 있다.

3. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 – 〈위탁 시 고려사항〉 中

[서비스 제공자 감독]

기업은 규제 체제 하에서 모든 의무를 완수할 책임이 있으며, 책임을 서비스 제공자에게 위임할 수는 없다. 기업은 다음 사항을 고차원적으로 수행해야한다.

- 제공받는 서비스를 명확히 밝히고, 기업과 서비스 제공자(들) 간의 책임과 의무가 어디서 시작되고 끝나는지 명확히 밝혀야 한다.

• 서비스 제공자의 일상적인 관리와 전략적 관리에 대한 책임을 할당해야 한다.
• 직원이 위탁 업무를 감독하고 테스트할 수 있고 발생하는 위험을 식별, 모니터링 및 완화할 수 있으며 기존 제3자 제공자의 해약 또는 이전을 적절하게 관리하기 위해, 충분한 기술과 자원을 갖추고 있는지 확인해야 한다.
• 분쟁 해결을 위한 적절한 조치가 존재하는지 확인해야 한다.

[사업장 방문]

SYSC 8.1.8R(9)은 UCITS 투자 회사가 "위탁 업무 관련 데이터뿐만 아니라 서비스 제공자의 사업장에 효과적으로 접근" 할 수 있도록 요구한다.

이와 별도로, MiFID 조직 규칙 제 31 조 제 2 항(i)은 "투자 회사, 감사원 및 관할 당국은 위탁 기능 관련 데이터에 효과적으로 접근할 수 있고, 이 조항에 따라 효과적인 감시를 목적으로 필요하다고 판단하는 서비스 제공자의 사업장에 효과적으로 접근할 수 있다. 그리고 관할 당국이 그러한 접근권을 행사할 수 있다."고 설명한다.

우리는 '사업장'을 포괄적인 범위의 사업장으로 간주한다. 여기에는 본사, 운영 센터가 포함될 수 있지만 반드시 데이터 센터가 포함되는 것은 아니다.

이러한 요구 사항이 규칙 또는 직접 적용 가능한 조항으로 적용되는 기업의 경우, 해당 계약은 사업장 방문을 허용해야 한다. 그러므로 사업장이 효과적인 감독 수행과 관련이 있음에 초점을 두어야 한다. 반드시 모든 사업장을 방문할 필요는 없다. 예를 들어 서비스 제공자는 보안상의 이유로 데이터 센터와 같은 일부 장소에 대한 방문을 제한할 수 있다.

기업은 또한 관련 법규의 특정 요구 사항을 알고 있어야한다. 예를 들어, Solvency II 규정 274조는 보험 또는 재보험 사업이 "서비스 제공자의 사업장에 대한 현장 검사 수행을 포함하여 외주 기능 및 활동과 관련된 모든 정보에 효과적으로 접근"할 것을 요구한다.

특정 고려 사항은 다음과 같다.

[기업 및 감사원 방문]

• 기업은 관련 법률 및 규정에 따라 해당 사업장을 현장 방문할 수 있어야한다. 이 권리는 제한할 수 없다.
• 기업은 긴급 상황이나 위기 상황이 있는 경우를 제외하고는 이 방문에 대한 합당한 사전 서면 통보를 제공할 수 있다.
• 기업은 감사원을 선임할 수 있다. 이는 기업의 회계 감사원이어야 하며 위탁 제공자가 선임한 감사원이 아니어야 한다.
• 기업 및(또는) 감사원 방문 범위는 해당 법적 및 규제 요구 사항에 따라 기업 및 자회사가 이용하는 서비스로 제한될 수 있다.

[규제 담당자 방문]

• 규제 기관이 필요하다고 판단하고 관련 법률 및 규정 요구 사항에 따라 필요한 경우에만 위탁 제공자의 사업장에 방문 가능하다. 기업은 이 외의 조건을 더 이상 규정해서는 안 된다.
• 위탁 제공자는 그러한 방문 중에 규제 당국의 합리적인 요청에 협조해야 한다.
• 규제 기관은 긴급 상황이나 위기 상황을 제외하고 업무 시간과 위탁 제공자가 지정한 시간 또는 합당한 통지를 통해 방문할 수 있다.
• 규제 기관에서 참석하는 직원에 대한 제한은 없다. 그러나 규제 기관은 참석할 직원에 관한 정보를 제공할 수 있고 제공할 것이다.
• 방문하는 동안 규제 기관은 해당 금융 서비스 법규에 따라 규제 대상 기업 또는 자회사에 대한 서비스를 볼 수 있어야한다. 규제 기관은 위탁 제공자의 운영을 축소시키거나 중단할 수 있다.

4. (싱가포르-MAS) 아웃소싱 가이드라인 – 5.9 감사 및 점검

5.9.1 기관의 아웃소싱 계약은 기관이 자사 비즈니스 업무 활동을 효율적으로 관리하는 데 지장을 주거나

MAS에서 주어진 감독 역할 및 목표를 수행하는 데 방해가 되어서는 안 된다.

5.9.2 기관은 중요 아웃소싱 계약을 위한 자사 아웃소싱 계약서 전체에 다음과 같은 조항을 포함해야 한다.

(a) 기관에서 서비스 제공업체 또는 그 하도급 계약업체를 대상으로 사내 또는 사외 감사기관의 주도로, 또는 기관에서 지명한 대행업체가 주도하여 감사를 실시할 수 있어야 한다. 그리하여 서비스 제공업체 및 그 하도급 계약업체에 대하여 작성된 보고서 및 발견된 사실을 입수해야 하며, 이는 서비스 제공업체 또는 그 하도급 계약업체의 사내 또는 사외 감사기관이나 아웃소싱 계약과 관련하여 서비스 제공업체 및 그 하도급 계약업체에서 지명한 대행업체 등이 작성하도록 한다.

(b) MAS 또는 MAS에서 지명한 각종 대행업체에서 기관의 계약상의 관리를 행사하여 다음과 같은 행위를 할 수 있도록 한다(필요한 경우 또는 편의에 따라).

(i) 서비스 제공업체 및 그 하도급 계약업체에 접근하여 이를 점검하고 기관 측에서 제공하여 서비스 제공업체 및 그 하도급 계약업체에서 보관 또는 처리 중인 거래 기록 및 문서, 정보 등을 입수한다.

(ii) 서비스 제공업체 또는 그 하도급 계약업체에 대한 보고서 및 발견된 사실 기록에 액세스한다. 이러한 기록은 서비스 제공업체 및 그 하도급 계약업체의 사내 또는 사외 감사 기관, 또는 아웃소싱 계약과 관련하여 서비스 제공업체 및 그 하도급 계약업체에서 지명한 대행업체에서 작성한다.

5.9.3 중요 아웃소싱 계약을 위한 아웃소싱 계약서에는 서비스 제공업체가 가능한 한 최대한 MAS 또는 기관의 요청에 부응하도록 서비스 제공업체 또는 그 하도급 계약업체에 요구하는 조항, 서비스 제공업체 및 그 하도급 계약업체가 MAS 측에 아웃소싱 계약과 관련하여 자사 보안 및 통제 환경에 대한 각종 보고서를 제출하도록 하는 조항도 포함해야 한다.

5.9.4 기관은 서비스 제공업체 및 해당 서비스 제공업체가 아웃소싱 계약에서 고용한 하도급 계약업체(예: 재해 복구 및 백업 서비스 제공업체 등) 모두 아웃소싱 계약에서 이러한 기대 사항에 부합하도록 해야 한다. MAS에서는 기관 측에 당청에서 보유한 점검 권한을 행사할 의향이 있음을 합당한 유예 기간을 두고 통보하며 알아낸 사실들을 해당 기관과 공유한다(경우에 따라).

5.9.5 기관은 자사의 모든 아웃소싱 계약을 대상으로 독립적인 감사 및/또는 전문가 평가를 실시해야 한다. 감사 및 전문가 평가의 빈도를 결정할 때, 기관은 아웃소싱 계약의 성격과 리스크 정도 및 기관에 미치는 파급력 등을 감안해야 한다. 감사 및 전문가 평가의 범위에는 서비스 제공업체 및 그 하도급 계약업체의 보안17 및 통제 환경 실태 평가, 사고 관리 프로세스(중대한 위반, 서비스 중단 또는 기타 중요한 문제에 대하여) 및 아웃소싱 계약과 관련한 기관의 본 가이드라인 준수 실태 등을 포함해야 한다.

5.9.6 서비스 제공업체 및 그 하도급 계약업체를 대상으로 한 독립적인 감사 및/또는 전문가 평가는 기관의 사내 또는 사외 감사기관, 서비스 제공업체의 사외 감사기관18 또는 기관에서 지명한 대행업체가 수행해도 좋다. 지명된 인물은 계약 내용대로 의무를 이행하는 데 필요한 지식과 기술을 보유하고 있어야 하며, 아웃소싱 계약을 이행하는 팀 또는 부서와 관련이 없는 인물이어야 한다. 고위 경영진은 감사 결과 알아낸 사실을 처리하기 위해 적시에 적절한 시정 조치를 취하도록 해야 한다19. 기관과 서비스 제공업체는 적절한 프로세스를 마련하여 시정 조치를 만족스럽게 완수할 수 있도록 해야 한다. 서비스 제공업체가 감사 결과 알아낸 사실을 처리하기 위해 취한 조치는 기관에서 적절히 검증한 다음에 종결한다. 필요한 경우, 업무에 필요한 지식과 기술을 보유한 관계 인물이 이렇게 적용한 보안 및 통제 수단의 효율성을 검증하는 데 관여한다.

5.9.7 중대한 사안 및 우려 사항은 기관 및 서비스 제공업체의 고위 경영진이나 기관의 이사회(필요한 경우)에 적시에 알려야 한다. 기관에서는 제기된 리스크가 기관의 리스크 허용 범위를 벗어나는 경우 해당 아웃소싱 계약을 검토하는 조치를 취해야 한다.

5.9.8 감사 보고서 사본은 기관이 MAS에 제출한다. 또한 기관은 MAS에 아웃소싱 계약과 관련한 기관 및 서비스 제공업체의 기타 보고서 또는 정보를 제공해야 한다(요청 시).

다. 재위탁 관리에 관한 사항

- 클라우드서비스 제공자가 일부 업무를 재위탁할 경우 재위탁 업무의 범위 및 수탁자 내역 등을 명확하게 제공할 것
  - 클라우드서비스 제공자는 업무 재위탁 시 수탁자가 원계약을 준수하도록 하고, 재위탁 계약서에 본 가이드의 계약서 명시사항 중 관련 부분을 포함할 것
- 재위탁 업무가 신규로 발생되거나 중요 변경 사항이 발생할 경우 금융회사에 사전 동의를 받아야 하며,
  - 금융회사는 이에 따른 보안리스크 등 서비스 영향을 고려하여 동의하지 않거나 계약을 해지할 수 있음
- 클라우드서비스 제공자는 정보기술부문의 정보보호와 관련된 업무를 위탁받은 경우, 해당업무를 제3자에게 재위탁할 수 없음(전자금융거래법 제40조제6항)

참고 주요국 금융권 지침 내 재위탁 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 - 4.7 재위탁

21) CEBS 지침의 가이드라인 10에 명시된 바와 같이, 금융회사는 위탁 서비스 제공 업체가 다른 공급업체에게 서비스 요소를 위탁하는 재위탁과 관련된 위험을 고려해야한다. 금융회사는 외주 업체가 금융회사와 위탁 서비스 제공 업체 간에 존재하는 의무를 완전히 준수 할 경우에만 재위탁에 동의해야한다. 또한 금융회사는 위탁 계약에 따라 위탁 서비스 제공 업체의 책임을 수행하는 능력에 중대한 영향을 미치는 재위탁 업무에 따른 어떤 약점이나 실패 위험을 해결하기 위해 적절한 조치를 취해야 한다.

22) 금융회사와 클라우드 서비스 공급자 간의 위탁 계약은 잠재적인 외주에서 제외되는 모든 유형의 활동을 지정 해야 하며, 클라우드 서비스 제공자가 외주 계약을 체결한 서비스에 대한 전적인 책임과 감독을 유지해야 함을 나타낸다.

23) 위탁 계약에는 클라우드 서비스 제공 업체가 하청 업체 또는 초기 계약서에 명시된 외주 서비스에 대한 계획된 중요한 변경 사항을 금융회사에 통보해야하는 의무가 포함되어야 한다. 이러한 변경에 대한 통지 기간은 외주 업체 또는 외주 서비스의 변경이 효력을 발생하기 전에 금융회사가 제안된 변경 사항의 영향에 대한 위험 평가를 수행 할 수 있도록 계약 상 사전 합의되어야 한다.

24) 클라우드 서비스 제공 업체가 합의된 서비스의 위험 평가에 악영향을 미칠 수 있는 외주 업체 또는 외주 업체의 변경을 계획하는 경우, 금융회사는 계약을 해지 할 수 있는 권리를 가져야한다.

25) 금융회사는 클라우드 서비스 제공자 또는 그 하청 업체에 의해 서비스가 제공되는지 여부에 관계없이 전체 서비스의 성능을 지속적으로 검토하고 모니터링 해야 한다.

2 (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 〈위탁 시 고려사항〉 中

[서비스 제공자 간의 관계]

위탁 공급망은 종종 복잡하다.
- 규제 대상 기업이 위탁 제공자와 직접 계약하지 않는 경우, 기업이 규제사항을 계속 준수할 수 있는지 여부를 결정하기 위해 규제 대상 업무와 관련된 재위탁 계약을 검토해야한다. 예를 들어, 기업은 보안 요구 사항과 데이터 및 사업장에 대한 효과적인 접근 방안을 고려해야한다. 규제 대상 기업은 위탁 제공자와 직접 계약하지 않더라도 이러한 규제 요구 사항을 준수할 수 있어야한다.
- 1999년 계약법(제3자의 권리)은 이러한 고려 사항과 관련 있을 수 있다.
- 규제 대상 기업은 서비스 제공자의 협력 방안을 고려해야한다. 예를 들어 기업 또는 서비스 제공자가 리드 시스템 통합(the lead systems integration) 역할을 담당하는가?
- 기업은 서비스 제공자의 서비스가 기업의 내부 시스템 또는 기타 제3자 시스템 (예: 대행 결제)과 쉽게 호환될 수 있는지 고려해야한다.

라. 서비스 중지 등 서비스 수준에 관한 사항

- 클라우드서비스 제공자가 시스템 업데이트 등 불가피한 사유로 일정기간 동안 서비스를 중지해야 할 경우 사전에 금융회사와 협의할 것
- 해킹, 천재지변 등 예상하지 못한 사유로 정상적인 서비스 제공이 중단되는 경우 지체 없이 금융회사에 통지할 것
  - 또한, 서비스 중단 등 장애가 10분 이상 지속된 경우, 진행 상황 파악 등을 위한 연락 담당자를 지정하고 정확한 장애원인 분석 및 재발방지 대책을 마련하여 금융회사에 제공할 것

※ 클라우드컴퓨팅법에서는 중단 기간을 지정하고 있으나, 금융회사 중요 서비스의 경우 기간과 무관하게 중단 발생 시 통지할 필요

▶ 클라우드컴퓨팅법 제25조제1항제3호 및 동법 시행령 제16조

클라우드컴퓨팅서비스 제공자는 사전예고 없이 다음 각 호의 어느 하나에 해당하는 기간(당사자 간 계약으로 기간을 정하였을 경우에는 그 기간을 말한다) 이상 서비스 중단이 발생한 때 지체 없이 그 사실을 해당 이용자에게 알려야 한다.

1. 클라우드컴퓨팅서비스의 중단 기간이 연속해서 10분 이상인 경우
2. 클라우드컴퓨팅서비스의 중단 사고가 발생한 때부터 24시간 이내에 클라우드컴퓨팅서비스가 2회 이상 중단된 경우로서 그 중단된 기간을 합하여 15분 이상인 경우

- 클라우드서비스 제공자는 장애·재해·파업·테러 등으로 서비스 지연 또는 중단이 발생할 경우 신속하게 복구하고 대응할 수 있는 절차 및 체계를 마련하여 금융회사에 통지하고, 이를 준수할 것
  - 특히, 중요정보를 클라우드서비스를 통하여 처리하는 경우, 장애, 보안사고 등 유사 시 신속한 대응을 위해 필요한 시스템 운영 관련 상주 인력을 국내에 확보하고, 원활한 사고 대응을 위해 해당 인력의 관리시스템 접근 권한 등을 확보할 것
  - 그 외, 클라우드서비스 가용성, 연속성, 성능 요건, 금융회사 지원 사항 등을 사전에 합의하여 명시할 것
- 계약의 파기 또는 종료, 기타 위탁업무의 원활한 이행이 어려운 경우 해당 위탁업무의 이전 및 반환 등에 관한 사항을 명시할 것(「3. 출구 전략 이행을 위한 명시사항」 참조)
- 클라우드서비스 제공자와 금융회사 간에 분쟁으로 소송이 제기되는 경우에는 민사소송법이 정한 법원을 관할 법원으로 하고, 당사자 일방이 외국 사업자인 경우에는 대한민국 법원이 국제재판관할권을 가짐
  - 계약의 성립, 효력, 해석 및 이행과 관련하여서는 대한민국법을 적용

2 보안 관련 명시사항

가. 데이터 관리 및 보호에 관한 사항

- 클라우드서비스 이용 관련 모든 정보(서비스 위탁 규모 등 포함)는 금융회사가 위탁한 업무 범위 내에서만 처리되어야 함
- 수사목적, 법적 분쟁 발생 등에 따른 해외 관계당국 또는 해외의 제3자에 대한 정보 제공 관련 법령에 대해서 사전에 파악*하여 금융당국 및 금융회사에 보고할 것(추가, 변경사항 포함)

  * 정보 제공 시 정보 주체 통지를 금지하는 조항이 있을 경우 해당 조항도 포함되어야 함 (해당 조항에 따라 실제로 정보제공이 요구되었으나 정보 주체 통지가 불가한 경우에는 금융당국에 별도 통지할 것)

  - 해당 법령에 따라 정보제공이 요구되는 경우 실제로 정보를 제공하기 전에 금융당국 및 금융회사에 통지하고, 관계국의 법령, 국가간 상호협정 등에서 정한 적법한 절차에 따라 처리할 것
    - 단, 원칙적으로 정보주체의 동의를 받도록 하는 「개인정보보호법」, 「신용정보의 이용 및 보호에 관한 법률」 등을 준수할 것
- 금융회사가 클라우드서비스를 이용하여 처리하는 모든 정보는 금융회사의 소유로서 금융회사는 이 정보에 대해 언제든지 조회, 수정, 삭제할 수 있는 권리를 가짐
- 클라우드서비스 제공자는 정보에 대한 어떠한 권리도 주장할 수 없으며, 모든 정보 전송 시 암호화 기술을 적용하여야 함
  - 그 밖에 클라우드서비스 제공자는 정보의 비인가 접근 및 유출 등을 방지하기 위해 충분한 보호수단을 구현하여야 함
- 금융회사에서 수립한 업무 연속성 계획 및 안전성 확보조치 방안의 이행을 위해 협조 및 지원할 것

나. 사고대응 및 취약점 분석·평가에 관한 사항

- 클라우드서비스 제공자는 재해 또는 사고 발생 시 신고 절차, 복구 및 대응 절차 등을 마련하고 주기적으로 훈련을 실시할 것
  - 관련 직원을 모두 포함한 비상 연락 체계를 마련하고, 복구목표시간 및 복구목표시점 요건을 사전에 합의하여 명시하며, 필요 시 공동 훈련을 실시할 것
- 사고 발생 시, 클라우드서비스 제공자는 이를 인지한 즉시 금융회사에 통지(침해사고의 경우 침해사고대응기관에도 통지)하고, 사고 조사 및 피해 복구에 적극 협조*할 것

  * 사고 원인분석을 위한 자료 보전 및 제출, 현장 조사, 인력 지원, 피해 확산·재발 방지 및 복구를 위해 필요한 조치 등

  ※ 금융회사는 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무 중단 또는 지연, 전산자료 또는 프로그램의 조작과 관련된 금융사고, 전자적 침해사고 등 관련 규정에서 정한 사고 발생 시 지체 없이 금융감독원에 보고하여야 하고(감독규정 제73조), 클라우드서비스 제공자는 침해사고 발생·이용자 정보 유출 시 지체 없이 그 사실을 해당 이용자에게 알려야 하며, 특히 이용자 정보 유출 시 과학기술정보통신부장관에게 보고하여야 함(클라우드컴퓨팅법 제25조)

- 클라우드서비스 제공자는 금융회사 및 침해사고대응기관이 감독규정 제24조, 제37조의3 및 제37조의4에 따라 수행하는 비상대응훈련, 재해복구전환훈련, 통합보안관제, 침해사고대응훈련, 취약점 분석·평가 등을 수행할 수 있도록 지원할 것
- 클라우드서비스 제공자는 제공자가 관리하는 영역(인프라 등)에 대해 주기적으로* 제3자로부터 취약점 분석·평가를 수행하고 조치하였음을 금융회사에 통지(금융당국 요청 시 세부 수행 결과를 제출)

  * 이용 대상의 중요도에 따라 매년, 중대 변경 시 등 금융회사에서 적정한 주기를 판단하여 구체적으로 명시

  - 또한, 금융회사는 관련 보안사고 발생 등 필요 시 클라우드서비스 제공자에 추가적인 점검 수행을 요구할 수 있음

다. 기타 보안요구사항

- 리스크 관리 등을 위해 필요한 보안 요구사항을 명시하고, 각자의 정보보호 역할과 책임 범위, 손해배상 및 계약해지 관련 사항을 명시할 것
  - 특히, 클라우드서비스 제공자는 장애사고 발생 방지 등 적절한 서비스 품질 수준 보장 및 정보보호 역할과 책임을 다하기 위해 최선의 노력을 기울일 것
- 금융회사는 클라우드서비스 제공자의 업무수행인력에 대하여 사전 신원조회를 실시(신원보증보험증권 징구로 갈음할 수 있음)하거나 대표자의 신원보증서를 징구할 수 있고,
  - 클라우드서비스 제공자는 업무수행인력 내역 및 인력변경 시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안을 제출할 것(감독규정 제60조 제1항제13호)
  - 또한, 클라우드서비스 제공자는 직원 보안 교육을 주기적으로 실시하고, 교육 계획 및 수행 결과를 금융회사에 제출할 것
    - 특히, 금융회사 관련 업무 수행에 따른 비밀유지 의무 준수 및 위반시 처벌내용 등에 대한 내용을 보안 교육에 포함할 것(감독규정 시행세칙 [별표 5의2])
- 클라우드서비스 제공자는 위탁 업무 관련 법규 및 자율규제를 준수하고, 금융회사의 위탁 업무 모니터링을 지원할 것
- 「[부록] 금융분야 클라우드컴퓨팅서비스 제공기준」 내 서비스 제공기준을 만족할 것

3 출구 전략 이행을 위한 명시사항

- 클라우드서비스 제공자는 금융회사의 클라우드서비스 전환 및 종료 관련 절차에 적극적으로 협조할 것
- 클라우드서비스 제공자는 클라우드서비스의 전환 및 종료 시 서비스 중단 없이 정보를 안전하게 금융회사에 반환하도록 데이터 이전을 지원할 것
  - 클라우드서비스 제공자는 금융회사에게 데이터 이전을 위한 충분한 시간을 제공하고, 데이터 삭제 이전에 금융회사에 서면으로 확인 받을 것
- 클라우드서비스 제공자는 데이터 이전이 완료된 후 금융회사의 정보를 복구 불가능한 방법으로 완전히 파기하고, 파기 확인서를 제출하여 정보의 파기 여부를 확인받을 것
  - 특히, 개인정보의 경우 「개인정보보호법」 제21조 등 관계 법령을 준수하여 파기할 수 있도록 지원할 것
  - 이 때, 재위탁된 정보, 관리 서비스 및 주변 솔루션 내 정보 등도 동일하게 처리할 것

▶ 개인정보보호법 제21조(개인정보의 파기)

① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.
④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

▶ 개인정보보호법 시행령 제16조(개인정보의 파기방법)

① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.
1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 행정안전부장관이 정하여 고시한다.

▶ 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)

① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.
1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

- 클라우드서비스 제공자의 사정에 의해 종료할 경우, 클라우드서비스 제공자는 다른 클라우드서비스 제공자로의 이전 등 대안을 마련할 것
- 금융회사는 클라우드서비스의 전환 및 종료 절차에 대한 모의훈련을 주기적으로 실시할 것을 요구할 수 있음

4 책임관계 명확화

가. 대외적 책임(금융소비자 피해 발생 시 손해배상 책임)

- 클라우드서비스 제공자의 관련 법령, 계약상 의무 위반 등으로 인해 금융소비자에게 손해가 발생하는 경우에는 금융회사가 클라우드서비스 제공자와 연대하여 배상책임을 부담
  - 클라우드서비스 제공자의 귀책사유로 금융회사가 금융소비자에게 손해를 배상한 경우에는 금융회사는 클라우드서비스 제공자에게 구상권을 행사할 수 있음

나. 계약 당사자간 책임관계(금융회사와 클라우드서비스 제공자간)

- **관련 법령 위반 등에 따른 손해배상 책임**
  - 전자금융거래법, 신용정보법, 개인정보보호법 등 관련 법령* 및 계약상 의무를 위반한 클라우드서비스 제공자의 귀책사유**로
    - 금융회사 또는 금융회사의 고객에게 손해를 끼친 경우 금융회사는 이용계약의 해제·해지 여부와 관계없이 클라우드서비스 제공자에게 손해배상을 청구할 수 있음

* 「전자금융거래법」, 「신용정보의 이용 및 보호에 관한 법률」, 「금융기관의 업무위탁 등에 관한 규정」, 「금융회사의 정보처리 업무 위탁에 관한 규정」 등 금융 관련 법령, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」,「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등

** 클라우드서비스 제공자가 전자금융거래 법령을 포함한 관계 법령 또는 이용 계약상의 의무를 미이행·위반한 경우에는 클라우드서비스 제공자의 고의 또는 과실이 있는 것으로 볼 수 있음

  - 금융회사가 청구할 수 있는 손해배상에는 서비스 중단 및 자료 유출 등으로 인한 직접적인 손해 외에 금융회사의 대외 신뢰도 저하에 따른 손해 등 간접적인 손해도 포함될 수 있음
  - 양 당사자간 서비스 계약의 해제·해지와 관련된 절차·사항을 계약상에 포함하되,

- 관련 법령 위반, 반복적인 계약상 의무 불이행, 중요 계약사항의 위반(감독당국의 조사·접근권 관련 의무 미이행 등) 등이 있는 경우 금융회사가 위약금 없이 계약을 해제·해지할 수 있도록 명시

서비스 장애·중단 및 품질 수준 저하로 인한 손해배상 책임

- 클라우드서비스 제공자의 귀책사유로 이용기관이 서비스를 일시 이용하지 못하거나,
  - 계약 당사자간 사전에 협의한 적절한 서비스 품질 수준을 유지·제공하지 못한 경우 클라우드서비스 제공자는 금융회사에게 그 손해를 배상하여야 함
- 금융회사는 관련 법령 및 본 가이드에서 제시하는 내용을 바탕으로 클라우드서비스 제공자와 사전 협의를 거쳐 적합한 서비스 수준 협약(SLA)*, 구체적 손해배상 규정** 등을 사전에 명확히 정하여야 함
  - 불가항력으로 인한 사고 등에 대한 클라우드서비스 제공자의 면책사유·범위 등을 명확히 할 것

* SLA(Service Level Agreement): 클라우드서비스 제공자가 금융회사 등 이용자에게 제공하는 서비스의 수준을 정량 기준 등을 통해 명확히 제시하고, 이에 미달하는 경우 손해를 배상토록 하여 서비스의 품질을 보장하기 위한 약정

** 클라우드서비스 제공자는 금융회사와 사전에 협의하여 정한 손해배상 규정에 따라 구체적인 손해를 산출하고, 금융회사에게 해당 손해액을 지급토록 함

재위탁 관련 손해배상 책임 등

- 클라우드서비스 제공자는 재위탁 관련 수탁자가 계약 내용을 준수하도록 관리·감독할 의무가 있음
  - 재위탁 시 발생한 금융회사 등의 손해에 대해서는 원위탁자(클라우드서비스 제공자)가 재위탁 받은 업체와 연대배상할 책임이 있음(재위탁 받은 업체의 고의·과실은 클라우드서비스 제공자의 고의·과실로 간주)

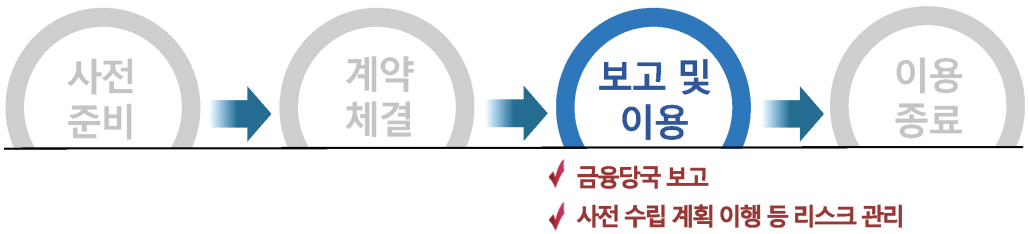
금융분야
클라우드컴퓨팅서비스
이용 가이드

제 7 장

보고 및 이용

1. 서류 구비 및 사전 보고
2. 서류 최신성 유지 및 수시 보고
3. 리스크 관리

제 7 장 보고 및 이용



1 서류 구비 및 사전 보고

금융회사는 제3장의 중요도 평가 결과와 무관하게 클라우드서비스 이용 전 다음 각 서류를 구비하여야 하고, 중요도 평가 결과 중요 업무의 경우, 클라우드서비스를 실제로 이용하려는 날의 7영업일 이전에 금융감독원에 이를 보고하여야 한다.

▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中

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 보고**하여야 한다. 이 경우 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 및 제2항에 따라 보고한 것으로 본다.

1. 고유식별정보 또는 개인신용정보를 처리하는 경우
2. 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 경우

④ 제3항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.

1. 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 각 호에 관한 서류
2. 제1항제1호에 따른 자체 중요도 평가 기준 및 결과
3. 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항
4. 제2항에 따른 정보보호위원회 심의·의결 결과

① 업무 위탁 관련 서류

※「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 각 호에 관한 서류

- 위탁계약서(안) 사본
- 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따라 금융기관이 마련하고 준수하여야 할 '업무위수탁 운영기준'(제4장 참조)
- 업무위탁 계약이 위탁 규정 등 관련법령에 위배되지 아니한다는 준법감시인(준법감시인이 없는 경우, 감사 등 이에 준하는 자)의 검토 의견 및 관련자료 사본
- 위탁의 필요성 및 기대효과
- 위탁에 따른 업무처리절차의 주요 변경내용
- 정보처리업무 운영에 대한 감독기관의 실질적 감독가능성을 확인할 수 있는 서류
- 위탁계약 상대방(재위탁 예정 시 재위탁계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)
- 전산사고 및 정보유출 등 발생 시 피해자 구제절차

② 자체 중요도 평가 기준 및 결과(제3장 참조)

③ 업무 연속성 계획 및 안전성 확보조치에 관한 사항(제4장 참조)

④ 정보보호위원회 심의·의결 결과(제5장 참조)

2 서류 최신성 유지 및 수시 보고

가. 서류 최신성 유지

▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**

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.

- 구비한 각 서류를 최신상태로 유지하고, 금융감독원장 요청 시 이를 지체 없이 제공할 것

※ 최신성 유지 및 요청 시 제공 의무는 중요도 평가 결과 및 사전 보고 여부와 관계없이 클라우드서비스를 이용하는 모든 금융회사가 부담하며, 고유식별정보·개인신용정보를 처리하지 않는 경우에도 해당

나. 수시 보고

▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**

⑥ 금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 변경사항이 발생한 날로부터 7영업일 이내에 발생 사유, 관련 자료 및 대응계획을 첨부하여 금융감독원장에게 보고하여야 한다.

1. 클라우드컴퓨팅서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등의 사유로 클라우드컴퓨팅서비스 이용계약에 중대한 변경사항이 발생한 경우
2. 클라우드컴퓨팅서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 아니한 경우
3. 제4항제2호 또는 제3호에 관한 중대한 변경사항이 발생한 경우

- 감독규정 제14조의2제3항에 따른 보고 대상 업무에 대해 다음 중 어느 하나에 해당하는 변경사항이 발생한 경우 7영업일 이내에 발생 사유, 관련 자료 및 대응 계획을 첨부하여 금융감독원장에게 보고할 것
  - 클라우드서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등의 사유로 이용 계약에 중대한 변경 사항이 발생한 경우

- 클라우드서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 않은 경우
- 중요도 평가, 업무 연속성 계획 및 안전성 확보조치에 중대한 변경 사항이 발생한 경우

참고 주요국 금융권 지침 내 감독당국 보고 관련 부분

1. (EU-EBA) 클라우드 아웃소싱 관련 권고 - 4.2 감독관에게 즉시 통보할 의무

2) 금융회사는 클라우드 서비스 제공자에게 위탁하는 중요 활동에 대해 관할당국에 적절하게 알릴 수 있어야 한다. 금융회사는 CEBS 가이드라인 4.3 항에 근거하여 이를 수행해야하며, 어떤 일이 있어도 관할 당국에 다음 정보를 제공해야한다.
   (a) 클라우드 서비스 제공자의 법인명과 모 회사명
   (b) 위탁하는 업무 및 데이터에 대한 설명
   (c) 클라우드 서비스가 수행되는 국가(데이터의 위치 포함)
   (d) 서비스 개시일
   (e) 최종 계약 갱신 일자(해당되는 경우)
   (f) 계약을 규율하는 관련 법
   (g) 서비스 만료일자 또는 차기 계약 갱신 일자(해당되는 경우)
3) 관할당국은 이전 단락에 따라 제공되는 정보에 더하여 위탁할 중요 활동에 대한 위험 분석에 대한 추가 정보를 금융회사에 요청할 수 있다.
   (a) 클라우드 서비스 제공자가 금융회사에 제공하는 서비스에 적합한 비즈니스 연속성 계획을 가지고 있는지 여부
   (b) 금융회사가 어느 당사자에 의한 종료 또는 클라우드 서비스 제공자에 의한 서비스 제공 중단의 경우 출구 전략을 가지고 있는지 여부
   (c) 금융회사가 위탁 활동을 적절하게 모니터링 하는데 필요한 기술과 자원을 유지하는지 여부.
4) 금융회사는 기관 및 그룹 차원의 클라우드 서비스 제공자로 위탁한 모든 중요 및 비중요업무에 대한 최신 정보 등록을 유지해야한다. 금융회사는 클라우드 서비스 제공자에게 위탁한 활동이 해당 기관에 의해 중요한 것으로 평가되었는지 여부와 상관없이 해당 등록 기관에 기록된 위탁 계약 및 관련 정보의 사본을 관할 당국의 요청 시 제공해야한다.
5) 중요 업무 해당 여부와 관계없이 제공해야하는 정보
   (a) 중요한 업무인 경우 통보해야하는 사항
   (b) 클라우드 위탁 유형(클라우드 서비스 모델과 클라우드 구현 모델, 퍼블릭/프라이빗/하이브리드/커뮤니티 클라우드)
   (c) 계약에 따라 클라우드 서비스를 제공받는 당사자
   (d) 경영진 또는 위임된 위원회가 업무 위탁을 승인한 증거
   (e) 해당되는 경우 재위탁한(subcontractors) 모든 업체명
   (f) 클라우드 제공자가 속한 국가
   (g) 위탁 업무가 중요한 업무로 평가되었는지 여부
   (h) 금융회사의 위탁 업무에 대한 최종 중요도 평가 일자
   (i) 클라우드 제공자가 무중단(time critical) 비즈니스 운영을 지원하는 여부

(j) 클라우드 제공자의 대체 가능성 평가(쉬움, 어려움, 또는 불가능함)
(k) 가능한 경우 대체 서비스 제공자 식별
(l) 업무 위탁 또는 재위탁에 대한 최종 위험평가 일자

2. (영국-FCA) 클라우드 및 제3자 아웃소싱 관련 지침 - 3.7

기업은 중요한 위탁 계약을 체결하거나 주요 변경사항이 있을 때 이를 통보해야 할 의무가 있음을 기억해야 한다. (SUP 15.3.8G (1) (e) 및 SYSC 8.1.12G(보험 회사 이외의 회사와 관련)에서 설명하는 의무를 따른다. MiFID 조직 규정에 대한 리사이틀 44를 참고한다.)

3. (싱가포르-MAS) 아웃소싱 가이드라인 - 4. 아웃소싱과 관련한 MAS의 관여

4.1 가이드라인 준수

4.1.1 기관은 MAS에 자사에서 본 가이드라인을 준수하고 있음을 입증할 준비가 되어 있어야 한다. 여기에는 적어도 1년에 한 번 또는 요청할 때마다 부칙 3에 명시된 템플릿에 자사 아웃소싱 등록부를 제출하는 것도 포함된다.

4.1.2 MAS가 기관의 가이드라인 준수 실태에 만족하지 못하는 경우, MAS에서 해당 기관에 지적된 결함을 시정하기 위해 추가 조치를 취할 것을 요구할 수 있다. 또한 MAS에서는 그와 같은 규정 위반을 기관 평가 시 감안할 수 있으며, 이 경우 아웃소싱이 기관 및 금융 시스템에 미치는 잠재적인 영향력, 지적된 결함의 심각성, 해당 기관의 내부 통제 및 리스크 관리 전적은 물론 해당 사안을 둘러싼 정황 등의 요인이 영향을 미칩니다. MAS에서는 기관의 국내 또는 소재국 규제 기관 및 기관의 서비스 제공업체와 직접 소통하여 해당 기관의 아웃소싱 리스크를 관리하는 데 있어 MAS와 협조할 역량 및 자발적인 의향 등을 알아볼 수 있다.

4.1.3 MAS에서는 다음과 같은 상황이 발생하는 경우 기관 측에 아웃소싱된 서비스를 변경, 대체할 다른 계약을 체결 또는 사내로 재통합하도록 요구할 수 있다.

(a) 기관이 아웃소싱 계약으로 인해 발생한 리스크의 특성과 정도를 만족스러운 수준으로 파악하고 있음을 입증하는 데 실패하거나 그럴 능력이 없는 경우
(b) 기관이 아웃소싱 계약으로 인해 발생하는 리스크를 해결할 적절한 수단을 만족스러운 수준으로, 적시에 실행하는 데 실패하거나 그럴 능력이 없는 경우
(c) 아웃소싱 계약으로 인해 기관에 타격을 입힐 수 있는 불리한 상황이 전개되는 경우
(d) MAS의 기관에 대한 감독관리 권한 및 해당 기관의 서비스에 관하여 MAS의 감독관리 역할을 수행할 역량이 저해되는 경우 또는
(e) 서비스 제공업체의 관리 환경이 변동되어 그로 인해 기관의 고객 정보 보안 및 기밀성이 저하된 경우 등이다.

4.2 불리한 상황 전개 통보

4.2.1 기관은 아웃소싱 계약으로 인해 기관에 타격을 입힐 가능성이 있는 각종 불리한 상황 전개에 관해 가급적 빠른 시일 내로 MAS에 알려야 한다. 그러한 불리한 상황 전개에는 아웃소싱 계약의 장기간 서비스 이행 불가 또는 중단으로 이어질 가능성이 있는 각종 사건사고 또는 기관의 고객 정보 보안 및 기밀성 침해 사례 등이 포함된다. 또한 기관은 기관의 그룹 내에서 그와 같이 불리한 상황이 전개된 경우에도 MAS에 그 사실을 알려야 한다.

3 리스크 관리

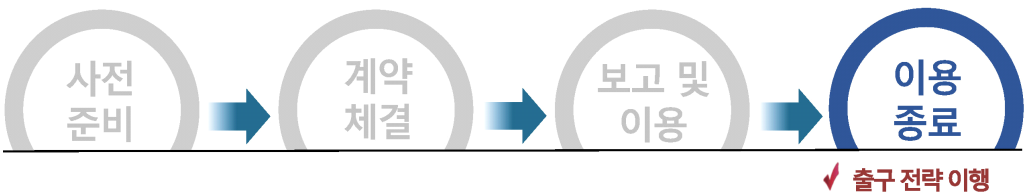
- 기 수립된 업무 연속성 계획(출구 전략 포함) 및 안전성 확보조치 방안을 준수하여 서비스 중단 및 보안 관련 리스크를 관리할 것
  - 리스크 관리를 위해 필요 시 침해사고대응기관에 협조를 요청할 수 있음
- 수립된 업무 연속성 계획 및 안전성 확보조치 방안 이행 등 규제 준수를 위해 클라우드서비스 제공자에게 협조를 요구할 것
  - 특히 금융당국의 조사·접근(현장방문 포함) 협조 의무, 통합보안관제·취약점 분석평가·비상대응훈련 등의 수행을 위한 협조 의무 등을 명확히 할 것
  - 다만, 불필요한 현장방문을 지양하고, 금융당국의 요구, 사고 발생, 제공자 평가 등 필요성이 있는 경우에 접근권을 행사하여야 함
- 클라우드서비스 제공자의 재위탁 현황을 관리하고, 재위탁 발생 및 변경 시 관련 보안리스크를 평가하고 관리할 것
- 특정 클라우드서비스 제공자에 서비스가 집중되지 않도록 관리하고, 특히 중요도가 높은 정보처리시스템에 대해서는 클라우드서비스 제공자에 대한 의존도가 과다하지 않도록 관리할 것

금융분야
클라우드컴퓨팅서비스
이용 가이드

제8장

이용 종료

제 8 장 이용 종료



금융회사는 클라우드서비스 제공자의 파산, 서비스 중단, 서비스 품질 저하, 규제 환경의 변화 또는 기타 금융회사의 필요에 따라 클라우드서비스를 전환 또는 종료할 경우 「제4장 계획 수립」에서 수립한 출구 전략에 의거하여 데이터 이전 및 파기 등을 실시하여야 한다.

첨부

1. 클라우드서비스 이용 관련 감독규정 주요 개정 내용
2. 해외 금융권 클라우드서비스 규제 사례
3. 전자금융감독규정 시행세칙의 망분리 대체 정보보호통제 수칙
4. 클라우드서비스 이용 가이드 관련 FAQ

첨부1 클라우드서비스 이용 관련 감독규정 주요 개정 내용

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
2. 〈별표 2의2〉의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가
3. 〈별표 2의3〉에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

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

④ 제3항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.

1. 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 각 호에 관한 서류
2. 제1항제1호에 따른 자체 중요도 평가 기준 및 결과
3. 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항
4. 제2항에 따른 정보보호위원회 심의·의결 결과

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 금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 변경사항이 발생한 날로부터 7영업일 이내에 발생 사유, 관련 자료 및 대응계획을 첨부하여 금융감독원장에게 보고하여야 한다.

1. 클라우드컴퓨팅서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등의 사유로 클라우드컴퓨팅서비스 이용계약에 중대한 변경사항이 발생한 경우
2. 클라우드컴퓨팅서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 아니한 경우
3. 제4항제2호 또는 제3호에 관한 중대한 변경사항이 발생한 경우

⑦ 금융감독원장은 제3항 또는 제6항에 따라 제출한 보고 서류가 누락되거나, 중요도 평가 또는 업무 연속성계획·안전성 확보조치 등이 충분하지 않다고 판단하는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

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 전자지급결제대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.

⑨ 그 밖에 금융회사 또는 전자금융업자의 클라우드컴퓨팅서비스 이용에 대해서는 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따른다.

제24조(비상대응훈련 실시)

④ 금융회사 또는 전자금융업자는 제1항 및 제2항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.

제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)

⑥ 금융회사 또는 전자금융업자는 제1항 또는 제3항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.

제60조(외부주문등에 대한 기준)

⑤ 금융회사 또는 전자금융업자는 제14조의2제1항제2호에 따른 평가를 위하여 제37조의4제1항 각 호의 어느 하나에 해당하는 기관에 지원을 요청할 수 있다.

첨부2 해외 금융권 클라우드서비스 규제 사례

국가	규제 사례
EU	• EBA(유럽은행청)은 클라우드 이용자 유의사항 등을 명시한 「클라우드 제공자 업무 위탁에 대한 권고」 발표('18.7월 발효) - 금융회사는 중요업무를 선별하고, 중요업무를 클라우드 제공자에 위탁 시 관할 당국에 통보하고 최신정보 유지 - 금융회사 및 위임된 제3자에게 위탁 업무 관련 접근권 및 현장감사권을 부여하도록 서면계약 체결 필요 - 정보 전송 시 정보보호 , 서비스 연속성 보장 등 보안 요구사항을 계약에 명시적 포함, 위탁 후 위험 관리 실시 - 클라우드 제공자가 위치하는 국가에서 요구하는 컴플라이언스 및 법적 위험성 평가를 통해 데이터처리 위치 고려
영국	• FCA(금융감독청)에서 금융회사의 클라우드 이용 명시적 허용 및 컴플라이언스를 명시한 「클라우드 및 제3자 IT 아웃소싱 관련 지침」 을 발표('16.7월) - (법적 요구사항) 중요 업무 아웃소싱 시 해당 결정의 근거가 되는 문서화된 명확한 비즈니스 사례 및 이유 보유 - (리스크 관리) 리스크 평가 실시 및 기록, 법적·운영리스크 파악, 제공자 파산 시, 데이터 유출 시 조치방법 등 고려 - (보안) 실사·감사 등 진행 시 ISO 등 국제 표준 준수, 제공자 자산 등에 대한 보안리스크 평가 진행 - (기타) 효과적인 데이터 접근, 제공자의 사업 관할지 접근 등
미국	• FFIEC(검사협의회)에서 금융권 클라우드 이용 시 주의사항을 명시한 「아웃소싱 클라우드 컴퓨팅」을 발표('12.7월) - 금융기관의 데이터 무결성, 기밀성 보호를 위한 통제사항 확인, 재해복구(DR), 업무연속성 계획(BCP) 적절성 확인 - 소비자 데이터가 국외에서 저장 또는 처리될 경우, 해당 국가의 관련 규정 확인 - 계약 시 금융기관의 프라이버시 관련 책임, 보안사고시 보안의무, 정보유출시 보고의무 등 법적 의무 명시
일본	• 당국의 지침 등은 없으나 자율규제기구인 FISC(금융정보시스템센터)의 시스템 안전대책 기준內 클라우드 통제항목 명시 - 클라우드 서비스 이용 시 다음의 안전대책 강구 · 클라우드 제공자 거점이 금융회사가 통제가능한 지역일 것 · 클라우드 이용 계약 시 금융회사의 감사권한 등 권리를 명기 · 클라우드 제공자에 대한 정기적 감사 및 클라우드 제공자의 책임범위를 명확히 설정
싱가포르	• MAS(통화국)는 클라우드서비스도 아웃소싱의 하나로 명시하고 「아웃소싱 가이드라인」 ('16.7월)을 준수토록 규정 - 금융회사는 클라우드 제공자에 대한 실사를 실시하고, 가이드에 명시된 아웃소싱 위험관리 수행 - 데이터 접근, 기밀성, 무결성 보장 등을 위한 금융회사의 적극적 조치, 클라우드 제공자가 적정한 통제를 통해 고객데이터를 명확히 분리하는지 확인 - 금융회사는 클라우드 제공자를 관리·감독하고 도입에 따른 궁극적 책임을 부담
호주	• APRA(금융감독청)은 아웃소싱 규정(CPS 231) 및 「공유 컴퓨팅 서비스(클라우드 포함) 관련 아웃소싱에 대한 정보 사항」('15.7월)을 통해 금융회사의 클라우드 이용 시 통지의무 등을 명시 - 중요 아웃소싱의 경우 국내는 APRA에 통지/국외 또는 내재된 위험이 높을 경우(퍼블릭 클라우드 사용 시 등) APRA와 사전 협의

첨부3 전자금융감독규정 시행세칙의 망분리 대체 정보보호통제 수칙

대 책	세부사항
내부망 보안 강화	• 업무망에 반입되는 전산자료 대상으로 악성코드 감염여부 진단·치료 대책 수립
외부망 보안 강화	• 지능형 해킹(APT)차단 대책 수립 • 외부망을 통해 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
메일 시스템 보안 강화	• 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립 • 메일을 통한 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
단말기 보안 강화	• PC 사용자의 관리자 권한 제거 • 승인된 프로그램만 설치·실행토록 대책 수립 • 단말기 전산 자료 암호화 저장
원격 접속 통제 수립	• 원격접속 기준 및 절차가 포함된 보안정책 수립 • 불법 원격접속을 방지하기 위한 사용자인증, 암호화 등의 보안대책을 수립 • 원격접속은 책임자의 승인을 받은 사전 등록자에 한하여 허용하며 원격접속 관리 기록부를 기록·보관 • 원격에서 접속하는 외부 단말기와 내부 업무용 시스템 구간의 암호화 통신 • 원격접속 사용자는 아이디·비밀번호 이외에 추가 인증수단을 적용 • 원격에서 접속하는 외부 단말기의 악성코드 감염 예방 대책 수립·적용 • 원격접속 가능한 내부 업무용 시스템의 접근 통제 수립·적용 • 원격으로 접속하여 수행한 모든 작업 내역 기록하고 매일 이상여부 점검 실시 및 책임자가 확인

첨부4 클라우드서비스 이용 가이드 관련 FAQ

1. 고유식별정보 또는 개인신용정보를 처리하는 경우, 해당 정보를 처리하는 모든 시스템을 국내에 설치하도록 하고 있는데, 클라우드서비스 제공자의 관리시스템도 포함되나요?

⇒ 관련 시스템의 국내 설치 의무 여부는 "**해당 정보**의 처리 여부"에 따라 구분됩니다. 클라우드서비스 제공자의 관리시스템에서 고유식별정보 또는 개인신용정보가 일시적으로라도 처리* 된다면, 국내에 설치하여야 합니다. (감독규정 제14조의2제8항)

* "처리"는 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말합니다. (개인정보보호법 제2조제2호)

2. 개발망이나 SaaS 구축의 경우 내부망 시스템 및 단말기와 연결은 어떻게 구성되나요?

⇒ 개발망이나 SaaS 구축의 경우에도 본 가이드의 원칙이 동일하게 적용되며, 기존 내부망에 구축하던 업무용 시스템은 클라우드서비스 제공자 구간 내에서 인터넷과 논리적으로 분리된 내부망에 위치해야하며, 기존 개발망에 구축하던 개발용 시스템은 클라우드서비스 제공자 구간 내에서 논리적으로 구분된 개발망에 위치해야합니다.

3. 지주사 클라우드 이용 시에도 적용되나요?

⇒ 지주사가 非상용 프라이빗 클라우드를 구축하여 그 계열사가 이용하는 경우에는(감독규정 제11조제11호 및 제12호, 제15조제1항제5호 준수) 감독규정 제14조의2에서 부여하고 있는 의무 적용 대상이 아닙니다.

4. SaaS 사업자가 인증받은 IaaS를 기반으로 하고 있을 때, 별도 인증 또는 평가가 필요한가요?

⇒ SaaS가 해당 IaaS와 동일 수준의 보안 조치를 했다고 보기 어려우므로 별도 인증 또는 평가가 필요합니다.

5. 금융권 추가보호조치 일부 항목이 기본보호조치 항목과 일부 중복되고 있는데 이 부분은 생략가능한가요?

⇒ 클라우드서비스 제공자가 금융권 추가보호조치를 준수하지 않을 경우 금융회사가 규정 위반을 하게 될 가능성이 있으므로, 금융권 추가보호조치 항목은 생략하지 않고 점검하여야 합니다.

6. 직원 교육프로그램 등을 위탁하고 있는데, 해당 업체가 클라우드서비스를 이용하는 경우 본 가이드의 적용 대상이 되나요?

⇒ 「금융기관의 업무위탁 등에 관한 규정」 제2조제2항 후단에서 후선업무와 관련한 단순 집행업무 등 금융업 영위와 직접적으로 관계되지 아니하는 위탁계약은 "업무위탁"의 범위에서 제외하고 있으며 동 규정 [별표 1]에 정의되어 있는 적용배제의 범위 中 "직원 연수 프로그램 운영, 교육 강의"에 대해 업무위탁규정 적용이 배제됨이 명시되어 있습니다.

이 경우 관련 업체가 클라우드서비스를 이용하는 경우에도 "업무위탁"의 범위에 포함되지 않으므로 금융회사가 클라우드서비스를 이용한다고 볼 수 없어, 본 가이드의 적용 대상이 아닙니다.

7. 업무 중요도 평가 결과 중요도가 낮은 업무에 대해 클라우드서비스를 이용하는 경우에도 본 가이드가 모두 적용되나요?

⇒ 가이드 각 장에서 중요도가 낮은 업무에 대해 구분 적용되는 부분을 별도로 명시하였으므로 이를 참고하시기 바랍니다.

금융분야
클라우드컴퓨팅서비스
이용 가이드

부록

금융분야 클라우드컴퓨팅 서비스 제공기준

1. 평가 대상
2. 평가 절차 및 방법
3. 평가항목 기준

제1장 평가 대상

- 「전자금융감독규정」 개정안은 「클라우드컴퓨팅법」에서 정한 클라우드서비스 제공자를 평가대상으로 규정하고 있는 바,
  - 금융회사가 제3자로부터 상용(商用)으로 제공받는 모든 유형*의 클라우드 서비스 제공자가 평가대상에 해당

    * IaaS, PaaS, SaaS

참고 「클라우드컴퓨팅법」의 클라우드서비스 정의

[법] 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. "클라우드컴퓨팅서비스"란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.

[시행령] 제3조(클라우드컴퓨팅서비스) 법 제2조 제3호에서 "대통령령으로 정하는 것"이란 다음 각 호의 어느 하나에 해당하는 서비스를 말한다.

1. 서버, 저장장치, 네트워크 등을 제공하는 서비스
2. 응용프로그램 등 소프트웨어를 제공하는 서비스
3. 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스
4. 그 밖에 제1호부터 제3호까지의 서비스를 둘 이상 복합하는 서비스

- 이에, 금융회사가 자체 구축·운영(非상용 Private)하거나 상용*이 아닌 클라우드서비스 제공자는 본 클라우드 규제 적용대상에 미 해당

  * '상용' 여부의 판단은 과기정통부에서 제공하는 「클라우드컴퓨팅법 해설서」의 '상용' 기준 내용 등을 참고

  - 다만, 이 경우 망분리 등 클라우드서비스 활용에 필요한 일부 규제의 예외를 인정받지 못할 수 있어 추진 시 고려 필요

참고 과기정통부 「클라우드컴퓨팅법 해설서」의 '상용' 기준 내용(발췌)

□ '상용'이란 무상·유상에 구애받지 않고 상업용으로 제공되는 것을 의미하므로 무상으로 제공되는 클라우드컴퓨팅서비스라도 상용으로 제공되고 있다면 포함될 수 있습니다. 무상으로 클라우드컴퓨팅서비스를 제공하더라도 광고를 통해서 수익을 올리고 있다면 상용에 해당합니다.

□ 반면, 전산시설등의 사용 수수료를 내더라도 상용(商用)으로 제공되는 클라우드컴퓨팅서비스가 아니라면 이 법에서 말하는 클라우드컴퓨팅서비스에 해당하지 아니합니다. 예컨대 협회, 단체 등이 전용으로 구축한 클라우드컴퓨팅서비스는 포함되지 않습니다.

제2장 평가 절차 및 방법

클라우드서비스 최초 이용 시 실시하는 **'종합 평가'**와 이용 中 **보안수준 유지여부 확인**을 위해 실시하는 **'정기 평가'**로 구분

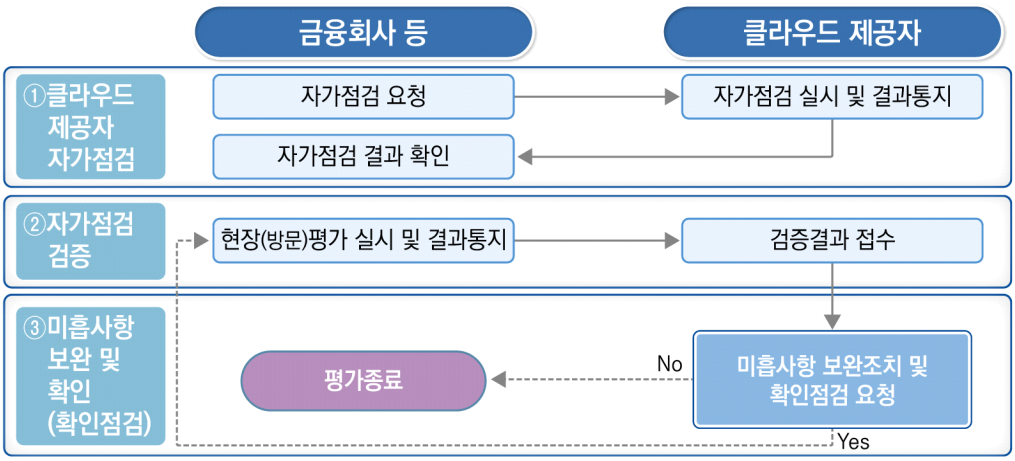
※ 업무 중요도 평가 결과 중요도가 낮은 업무의 처리만 위탁하는 경우에는 종합 평가 및 정기 평가를 서면(증적 포함)으로도 수행 가능

가. 종합 평가

- **(평가 시기)** 금융회사가 특정 클라우드서비스를 최초 이용 시 종합 평가 실시
  - 기존 이용 중인 클라우드서비스 제공자라도 아래와 같이 이용 서비스 유형이나 처리정보가 변경될 경우 종합 평가 실시 필요
    ① 이용 서비스 유형이 확대(예 : SaaS → SaaS, IaaS)된 경우
    ② 개정된 감독규정 시행('19.1.1.) 이전에 비중요정보의 처리를 위탁 중인 클라우드 서비스 제공자에게 개인신용정보 등의 처리를 추가로 위탁한 경우 등
- **(평가 절차)** ① 클라우드서비스 제공자 자가점검 → ② 금융회사의 자가점검 검증 → ③ 미흡사항* 보완 및 확인(필요시) 順으로 진행

  * 즉각적인 조치가 어려운 미흡사항은 보완조치 계획을 수립하고 조치 완료 내역을 실제 서비스 이용 전까지 금융회사가 확인

〈종합평가 업무 Flow〉



- **(평가 방법)** 클라우드서비스 제공자는 평가항목의 이행여부를 자가 점검하고, 증적*을 포함한 자가점검 결과를 금융회사에 제출

  * 동일한 평가항목에 대해서는 금융회사가 인정하는 보안인증의 결과를 제출할 경우 이를 증적 자료로 활용 가능

  - 금융회사는 클라우드서비스 제공자가 제출한 자가점검 결과를 '현장(방문) 평가'를 통해 검증

  ※ 사전 협의된 기관이나 금융회사가 지정한 제3자의 감사보고서 검토로 현장평가를 일부 대체할 수 있으며, 확인점검은 단순·경미사항에 한해 서면(증적 포함)으로도 수행 가능

나. 정기 평가

- **(평가 시기)** 클라우드서비스 제공자의 보안수준 유지 여부를 지속 검증하기 위해 종합 평가 종료 後 매 1년마다 정기 평가 실시

  ※ 업무 중요도 평가 결과 중요도가 낮은 업무의 처리만 위탁하는 경우에는 정기 평가 생략 가능

  - 평가항목의 대규모 변경 또는 클라우드서비스 제공자의 보안성에 중대한 변화* 등이 있는 경우 평가 주기와 무관하게 정기 평가 실시

  * 클라우드서비스 제공자의 보안사고 발생, 클라우드 IT인프라 전면 재구축 등

- **(평가 절차)** 종합 평가와 동일

- **(평가 방법)** 클라우드서비스 제공자의 자가점검 결과를 서면(증적 확인)으로 검증함을 원칙으로 하되,

  - 정기 평가 매 3년차* 또는 금융회사가 필요하다고 판단하는 경우 현장(방문)평가 실시

  * 과기정통부 주관 클라우드 보안인증제(CSAP)의 경우도 최초 인증 취득 後 3년이 경과하면 인증 갱신평가를 시행

  ※ 사전 협의된 기관이나 금융회사가 지정한 제3자의 감사보고서 검토로 현장평가를 일부 대체할 수 있음

다. 침해사고대응기관 평가 지원

클라우드서비스 제공자 평가는 기본적으로 **금융회사가 수행 주체**이며, 금융회사 요청 시 **침해사고대응기관이 안전성 평가 지원***(건전성 평가는 금융회사에서 직접 수행)

* 침해사고대응기관은 인력 및 예산 상황 등에 따라 지원 여부 및 일정 등 조정 가능하며, 참가기관 우선 지원을 원칙으로 함

- **(지원 대상)** 종합·정기 평가 시 '현장(방문)평가'를 지원하며, 지원 대상 기관은 전자금융거래법 적용 대상 금융회사로 한정

- **(지원 절차)** ① 평가지원 신청 → ② 평가 실시(확인점검 포함) → ③ 평가 결과 통지 → ④ 평가결과 공개(필요시) 順으로 진행

❶ **(평가지원 신청)** '종합 평가'와 '정기 평가'를 구분하여 아래의 방식으로 지원 신청

- 종합 평가: 클라우드서비스 개시 최소 3개월 前에 개별 신청
- 정기 평가: 침해사고대응기관이 매년 실시하는 평가 수요조사 시 신청

❷ **(평가 실시)** 침해사고대응기관이 클라우드서비스 제공자를 직접 방문하여 현장평가 실시

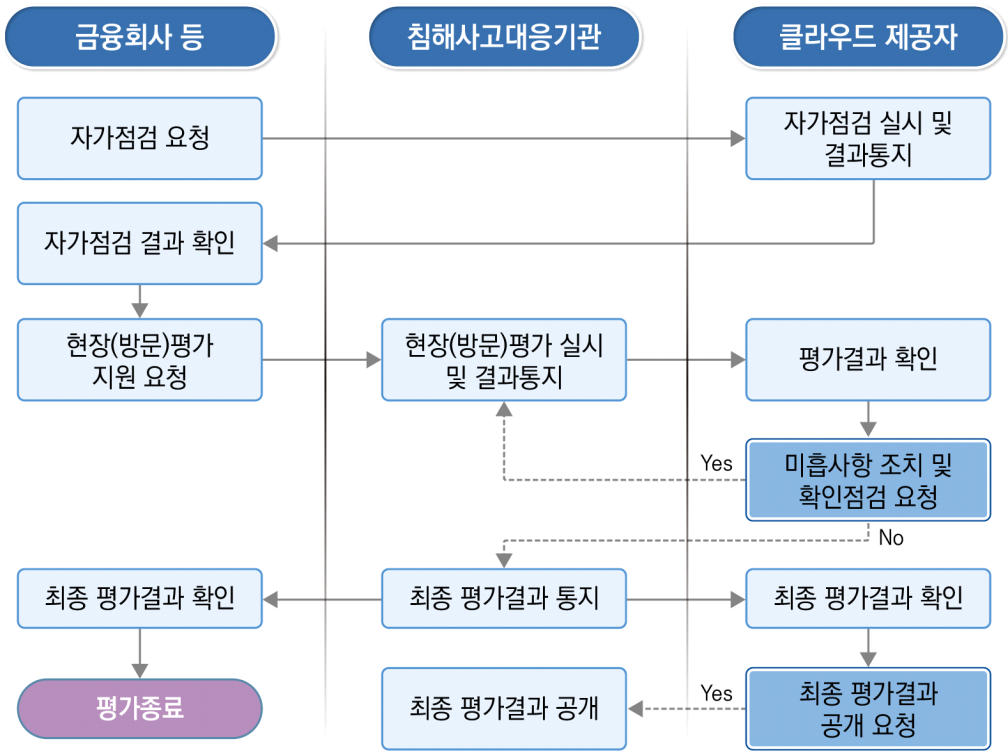
- 클라우드서비스 제공자가 평가결과 미흡사항을 조치하고 확인평가를 요청하는 경우 이를 지원

❸ **(평가결과 통지)** 침해사고대응기관이 실시한 현장평가 최종 결과를 클라우드서비스 제공자 및 금융회사 등에 각각 통지

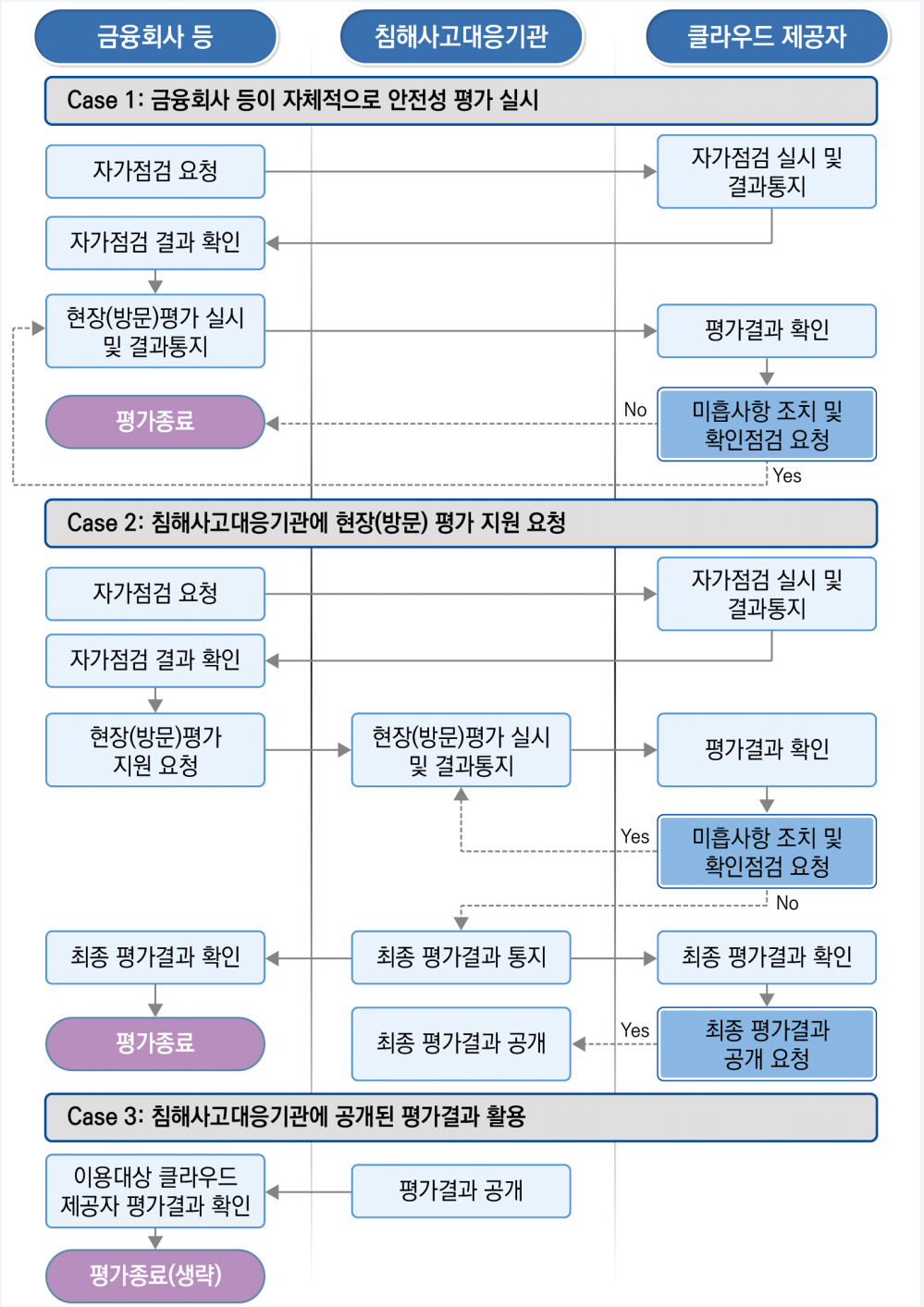
❹ **(평가결과 공유)** 동일 클라우드서비스 제공자에 대한 중복평가가 이행되지 않도록 클라우드서비스 제공자가 요청하는 금융회사에 대하여 침해사고대응기관이 평가결과를 공유

➜ 평가결과가 공유된 클라우드서비스 제공자에 대해서는 제공기준에 따른 안전성 평가 수행 시 기존 평가 결과 활용 가능(평가에 대한 부담 완화)

〈침해사고대응기관 평가 지원 흐름도〉



참고 클라우드서비스 제공기준 평가 절차 통합 Flow



제3장 평가항목 기준

클라우드서비스 제공자가 준수해야 할 일반적 보안 기준인 **'기본 보호조치'**와 금융분야 특화 기준인 **'금융부문 추가 보호조치'** 로 구분

가. 기본 보호조치 항목

- 과기정통부 주관 클라우드서비스 보안인증제(CSAP)의 일반적 평가·인증 통제항목* 준용(IaaS, SaaS)

  * 전체 14개 카테고리 中 공공부문 추가 보안요구사항은 제외

참고 CSAP의 평가·인증 통제항목

통제분야	통제항목수	
	IaaS	SaaS
1. 정보보호 정책 및 조직	5개	5개
2. 인적보안	12개	5개
3. 자산관리	10개	3개
4. 서비스 공급망 관리	4개	3개
5. 침해사고 관리	7개	7개
6. 서비스 연속성 관리	7개	6개
7. 준거성	4개	3개
8. 물리적 보안	12개	-
9. 가상화 보안	10개	6개
10. 접근통제	10개	10개
11. 네트워크 보안	6개	5개
12. 데이터 보호 및 암호화	10개	8개
13. 시스템 개발 및 도입 보안	12개	10개
합계	**109개**	**71개**

- 클라우드서비스 中 PaaS의 경우는 상기 IaaS, SaaS 통제항목에 준하여 보호조치 수행*

  * 추후 필요시 PaaS에 특화된 통제항목을 개발할 계획

  ※ 「[첨부1] 기본 보호조치 세부 평가항목」 참조

나. 금융부문 추가 보호조치

※ 「[첨부2] 금융부문 추가 보호조치」 참조

다. 평가항목 일부 적용 예외

- 국내·외 클라우드 보안인증을 취득·유지하고 있는 클라우드서비스 제공자의 해당 서비스에 대해서는 '기본 보호조치' 항목 평가 생략 가능

※ 단, 금융회사가 사용 예정인 서비스 및 데이터센터 등 이용 영역이 인증 대상에 반드시 포함되어 있어야 하며, 인증기관으로부터 확인 받은 서류에 해당 영역이 명시되어 있어야 함

- 다만, 신뢰도가 낮은 보안인증 취득 우려를 해소할 수 있도록 아래 기준에 부합하는 보안인증제에 한해 평가 생략이 가능

① 국가기관 또는 관련 분야 공신력 있는 전문 기관이 주관(총괄)

② 다수 국내·외 사업자(서비스)가 해당 인증을 취득

③ 평가항목이 본 제공기준의 평가항목과 상당수가 부합 또는 일치

➜ 국내·외 클라우드 보안인증제에 대해 상기 기준 부합여부를 검토 결과 아래 4개 보안인증 취득 시 '기본 보호조치' 평가 생략 가능

구분	인증제도명	평가생략 근거
국내	클라우드 서비스 보안인증제(CSAP)	• 과기정통부 주관, KISA가 평가·인증 • 국내 주요 클라우드 사업자가 인증 취득 • 평가항목수가 최대 120여개
해외	FedRAMP(High) (미국)	• 정부(FedRAMP 관리국) 주관 • 평가항목 수가 최대 400여개
	CSA STAR Certification(Gold) (Global)	• 400여개의 클라우드 사업자가 회원인 글로벌 클라우드 보안협회(CSA*) 주관 * CSA : Cloud Security Alliance • 평가항목 수가 최대 300여개
	MTCS(Level 3) (싱가포르)	• 정보통신미디어개발청(IMDA) 주관

※ 위 리스트는 상기 기준에 부합하여 평가 생략이 가능한 인증 제도를 열거한 것이며, 동 기준에 부합하는 국내·외 클라우드 보안인증제가 추가로 확인되는 경우, 지속 업데이트할 계획

첨부1 기본 보호조치 세부 평가항목(IaaS, SaaS)

1. 관리적 보호조치

구 분			세부 조치사항	IaaS	SaaS
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	1.1.1 정보보호 정책 수립	정보보호 정책을 문서화하고, 정보보호 최고책임자의 승인 후 정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 제공하여야 한다.	O	O
		1.1.2 정보보호 정책 검토 및 변경	정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하고, 관련 법규 변경 및 내·외부 보안사고 발생 등 중대한 사유가 발생할 경우에는 추가로 검토하고 변경하여야 한다.	O	O
		1.1.3 정보보호 정책문서 관리	정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하여야 한다.	O	O
	1.2 정보보호 조직	1.2.1. 조직 구성	정보보호 활동을 계획, 실행, 검토하는 정보보호 전담 조직을 구성하고 정보보호최고책임자를 임명하여야 한다.	O	O
		1.2.2. 역할 및 책임 부여	정보자산과 보안에 관련된 모든 임직원 및 외부업무 관련자의 정보보호 역할과 책임을 명확하게 정의하여야 한다. 또한 서비스 이용자의 정보보호 역할과 책임도 서비스 수준 협약 등을 통해 명확히 정의하여야 한다.	O	O
2. 인적보안	2.1 내부인력 보안	2.1.1 고용계약	고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 포함시키고, 새로 채용하거나 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자원, 자산에 접근이 허용되기 이전에 서명을 받아야 한다.	O	O
		2.1.2 주요 직무자 지정 및 감독	클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경우 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하여야 한다.	O	O
		2.1.3 직무 분리	권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무분리 기준을 수립하고 적용하여야 한다.	O	O
		2.1.4 비밀유지 서약서	정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기적으로 갱신하여야 한다.	O	O
		2.1.5 상벌규정	정보보호 정책을 위반한 임직원에 대한 징계 규정을 수립하고, 위반 사항이 발생 시 규정에 명시된 대로 징계 조치를 취하여야 한다. 또한 정보보호 정책을 충실히 이행한 임직원에 대한 보상 방안도 마련하여야 한다.	O	X
		2.1.6 퇴직 및 직무변경	임직원의 퇴직 또는 직무변경에 관한 책임을 명시적으로 정의하고 수행하여야 한다. 또한 이에 대한 접근권한도 제거하여야 한다.	O	X

구 분			세부 조치사항	IaaS	SaaS
	2.2 외부인력 보안	2.2.1 외부인력 계약	외부인력(외부유지보수직원, 외부 용역자 포함)에 의한 정보자산 접근등과 관련된 보안요구사항을 계약에 반영하여야 한다.	O	X
		2.2.2 외부인력 보안이행 관리	계약서에 명시한 보안요구사항 준수여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하여야 한다.	O	X
		2.2.3 계약 만료시 보안	외부 인력과의 계약 만료 시 자산 반납, 접근권한의 회수, 중요정보 파기, 업무 수행 시 알게 된 정보에 대한 비밀유지서약 등을 확인하여야 한다.	O	X
2. 인적보안	2.3 정보보호 교육	2.3.1 교육 프로그램 수립	모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하여야 한다.	O	X
		2.3.2 교육 시행	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하여야 한다.	O	O
		2.3.3 평가 및 개선	정보보호 교육 시행에 대한 기록을 남기고 결과를 평가하여 개선하여야 한다.	O	X
3. 자산관리	3.1 자산 식별 및 분류	3.1.1 자산 식별	클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준을 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한다.	O	O
		3.1.2 자산별 책임할당	식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.	O	X
		3.1.3 보안등급 및 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 보안등급을 부여하고, 보안 등급별 취급절차에 따라 관리하여야 한다.	O	X
	3.2 자산 변경관리	3.2.1 변경관리	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 평가를 통해 변경 사항을 관리하여야 한다. 또한 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지를 하여야 한다.	O	O
		3.2.2 변경 탐지 및 모니터링	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하여야 한다.	O	X
		3.2.3 변경 후 작업검증	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업 검증을 수행하여야 한다.	O	X
	3.3 위험관리	3.3.1 위험관리 계획수립	관리적, 기술적, 물리적, 법적 분야 등 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하여야 한다.	O	X

구 분			세부 조치사항	IaaS	SaaS
		3.3.2 취약점 점검	취약점 점검 정책에 따라 주기적으로 기술적 취약점(예:유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하여야 한다.	O	O
		3.3.3. 위험분석 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 수용 가능한 위험 수준을 설정하여 관리하여야 한다.	O	X
		3.3.4 위험처리	법규 및 계약관련 요구사항과 위험수용 수준을 고려하여 위험평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하여야 한다.	O	X
4. 서비스 공급망 관리	4.1 공급망 관리정책	4.1.1 공급망 관리 정책 수립	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하여야 한다.	O	O
		4.1.2 공급망 계약	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약 시 책임을 개별 계약서에 각각 명시해야하며, 해당 서비스에 관련된 모든 이해관계자에게 적용하여야 한다.	O	O
4. 서비스 공급망 관리	4.2 공급망 변경관리	4.2.1 공급망 변경관리	정보보호정책, 절차 및 통제에 대한 수정 및 개선이 필요하다고 판단될 경우 서비스 공급망상에 발생할 수 있는 위험에 대한 검토를 통해 안전성을 확보 후 계약서 내용 변경 방안을 제시하여야 한다.	O	O
		4.2.2 공급망 모니터링 및 검토	클라우드컴퓨팅서비스 공급망상에서 발생하는 기록 및 보고서는 정기적으로 모니터링 및 검토하여야 한다.	O	X
5. 침해사고 관리	5.1 침해사고 대응절차 및 체계	5.1.1 침해사고 대응 절차 수립	침해사고에 대한 효율적이고 효과적인 대응을 위해 신고 절차, 유출 금지 대상, 사고 처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다. 침해사고 대응절차는 이용자와 제공자의 책임과 절차가 포함되어야 한다.	O	O
		5.1.2 침해사고 대응 체계 구축	침해사고 정보를 수집·분석·대응할 수 있는 보안관제 시스템 및 조직을 구성·운영하고, 침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하여야 한다.	O	O
		5.1.3 침해사고 대응 훈련 및 점검	침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련시켜야 하고, 주기적으로 침해사고 대응 능력을 점검하여야 한다.	O	O
	5.2 침해사고 대응	5.2.1 침해사고 보고	침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치현황 등을 신속하게 알려야 한다.	O	O
		5.2.2 침해사고 처리 및 복구	침해사고 발생 시 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.	O	O

구 분			세부 조치사항	IaaS	SaaS
	5.3 사후관리	5.3.1 침해사고 분석 및 공유	침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알려야 한다. 또한 유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하여야 한다.	O	O
		5.3.2 재발방지	침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 침해사고 재발방지 대책을 수립하고, 필요한 경우 침해사고 대응체계도 변경하여야 한다.	O	O
6. 서비스 연속성 관리	6.1 장애대응	6.1.1 장애 대응절차 수립	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응절차를 마련하여야 한다.	O	O
		6.1.2 장애 보고	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응절차에 따라 법적 통지 및 신고의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.	O	O
		6.1.3 장애 처리 및 복구	클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.	O	O
		6.1.4 재발방지	장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하여야 한다.	O	O
	6.2 서비스 가용성	6.2.1 성능 및 용량관리	클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.	O	O
6. 서비스 연속성 관리	6.2 서비스 가용성	6.2.2 이중화 및 백업	정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속회선 등)의 장애로 서비스가 중단되지 않도록 정보처리설비를 이중화하고, 장애발생시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.	O	O
		6.2.3 서비스 가용성 점검	서비스 가용성에 대한 영향평가를 주기적으로 점검하여야 한다.	O	X
7. 준거성	7.1 법 및 정책 준수	7.1.1 법적요구 사항 준수	정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다.	O	O
		7.1.2 정보보호 정책 준수	정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하며 이용자가 요구하는 경우 관련 증거를 제공하여야 한다.	O	X
	7.2 보안감사	7.2.1 독립적 보안감사	법적 요구사항 및 정보보호 정책 준수여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하여야 한다.	O	O

구 분			세부 조치사항	IaaS	SaaS
		7.2.2 감사기록 및 모니터링	보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가 된 접근 및 변조로부터 보호되어야 한다.	O	O

2. 물리적 보호조치

구 분			세부 조치사항	IaaS	SaaS
8. 물리적 보안	8.1 물리적 보호구역	8.1.1 물리적 보호구역 지정	중요정보 및 정보처리시설을 보호하기 위한 물리적 보안 구역(예 : 주요 정보처리 설비 및 시스템 구역, 사무실, 외부인 접견실 등)을 지정하고, 각 보안구역에 대한 보안 대책을 마련하여야 한다.	O	X
		8.1.2 물리적 출입통제	물리적 보안 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 시설(예 : 경비원, 출입통제시스템 등)을 갖추어야 하고, 출입 및 접근 이력을 주기적으로 검토하여야 한다.	O	X
		8.1.3 물리적 보호구역 내 작업	유지보수 등 주요 정보처리 설비 및 시스템이 위치한 보호구역 내에서 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.	O	X
		8.1.4 사무실 및 설비 공간 보호	사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하여야 한다.	O	X
		8.1.5 공공장소 및 운송·하역구역 보호	공공장소 및 운송·하역을 위한 구역은 내부 정보처리 시설로부터 분리 및 통제하여야 한다.	O	X
		8.1.6 모바일기기 반·출입	노트북 등 모바일기기 미승인 반출·입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부인력 모바일 기기 반출입 통제 절차를 수립하고 기록·관리하여야 한다.	O	X
8. 물리적 보안	8.2 정보처리 시설 및 장비보호	8.2.1 정보처리 시설의 배치	물리적 및 환경적 위험으로부터 잠재적 손상을 최소화하고 비인가 된 접근 가능성을 최소화하기 위하여, 정보처리시설 내 장비의 위치를 파악하고 배치하여야 한다.	O	X
		8.2.2 보호설비	각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재 감지기, 소화설비, 누수 감지기, 항온 항습기, 무정전 전원장치(UPS), 이중 전원선 등의 설비를 갖추어야 한다.	O	X
		8.2.3 케이블 보호	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상이나 도청으로부터 보호하여야 한다.	O	X
		8.2.4 시설 및 장비 유지보수	정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수하여야 한다.	O	X

구 분			세부 조치사항	IaaS	SaaS
		8.2.5 장비 반·출입	장비의 미승인 반출·입을 통한 중요 정보 유출, 악성코드 감염 등의 침해사고 예방을 위하여 보안구역 내 직원 및 외부업무 관련자에 의한 장비 반출·입 절차를 수립하고 기록 및 관리하여야 한다.	O	X
		8.2.6 장비폐기 및 재사용	정보처리시설 내의 저장 매체를 포함하여 모든 장비를 파악하고, 민감한 데이터가 저장된 장비를 폐기하는 경우 복구 불가능하도록 하여야 한다. 또한 재사용하는 경우에도 복구 불가능 상태에서 재사용하여야 한다.	O	X

3. 기술적 보호조치

구 분			세부 조치사항	IaaS	SaaS
9. 가상화 보안	9.1 가상화 인프라	9.1.1 가상자원 관리	가상자원(가상머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하여야 한다.	O	O
		9.1.2 가상자원 회수	이용자와의 계약 종료 시 가상자원 회수 절차에 따라 백업을 포함한 모든 클라우드 시스템에서 삭제하여야 한다.	O	X
		9.1.3 가상자원 모니터링	가상자원에 대한 무결성을 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 하여야 한다. 또한, 가상자원에 손상이 발생한 경우 이를 이용자에게 알려주어야 한다.	O	X
		9.1.4 하이퍼바이저 보안	가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근통제방안을 마련하여야 한다. 또한 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하여야 한다.	O	X
		9.1.5 공개서버 보안	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.	O	O
		9.1.6 상호운용성 및 이식성	클라우드컴퓨팅서비스 제공자는 표준화된 가상화 포맷, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅서비스 간의 상호 운영성 및 이식성을 높여야 한다.	O	X
9. 가상화 보안	9.2 가상환경	9.2.1 악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하여야 한다. 또한 이상 징후 발견 시 이용자에게 통지하고 사용중지 및 격리 조치를 수행하여야 한다.	O	O
		9.2.2 인터페이스 및 API보안	가상환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하여야 한다.	O	O

구 분			세부 조치사항	IaaS	SaaS
		9.2.3 데이터 이전	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하여야 한다.	O	O
		9.2.4 가상 소프트웨어 보안	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작사가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.	O	O
10. 접근통제	10.1 접근통제 정책	10.1.1 접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.	O	O
		10.1.2 접근기록 관리	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다.	O	O
	10.2 접근권한 관리	10.2.1 사용자 등록 및 권한부여	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.	O	O
		10.2.2 관리자 및 특수 권한 관리	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.	O	O
		10.2.3 접근권한 검토	클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴식, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.	O	O
	10.3 사용자 식별 및 인증	10.3.1 사용자 식별	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.	O	O
		10.3.2 사용자 인증	클라우드 시스템에 대한 접근을 사용자인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.	O	O
		10.3.3 강화된 인증수단 제공	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.	O	O
		10.3.4 사용자 패스워드 관리	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경 주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.	O	O

구 분			세부 조치사항	IaaS	SaaS
		10.3.5 이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 클라우드 시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고, 관련 내용을 공지하여야 한다.	O	O
11. 네트워크 보안	11.1 네트워크 보안	11.1.1 네트워크 보안 정책 수립	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안정책과 절차를 수립하여야 한다.	O	O
		11.1.2 네트워크 모니터링 및 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.	O	O
		11.1.3 네트워크 정보보호 시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.	O	O
		11.1.4 네트워크 암호화	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다.	O	O
		11.1.5 네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.	O	O
		11.1.6 무선 접근통제	클라우드 시스템은 무선망과 분리하고, 무선접속에 대한 접근을 통제하여야 한다. 무선접속을 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인을 받아야 한다.	O	X
12. 데이터 보호 및 암호화	12.1 데이터 보호	12.1.1 데이터 분류	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.	O	O
		12.1.2 데이터 소유권	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하여야 한다.	O	O
		12.1.3 데이터 무결성	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.	O	O
		12.1.4 데이터 보호	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.	O	O
		12.1.5 데이터 추적성	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.	O	O
		12.1.6 데이터 폐기	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다.	O	O
	12.2 매체 보안	12.2.1 저장매체 관리	중요정보를 담고 있는 하드디스크, 스토리지 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.	O	X

구 분			세부 조치사항	IaaS	SaaS
		12.2.2 이동매체 관리	중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 이동매체 취급, 보완, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.	O	X
	12.3 암호화	12.3.1 암호 정책 수립	클라우드컴퓨팅서비스에 저장 도는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 절책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.	O	O
		12.3.2 암호키 관리	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.	O	O
13. 시스템 개발 및 도입 보안	13.1 시스템 분석 및 설계	13.1.1 보안요구 사항 정의	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안 취약점, 정보보호 기본요소(기밀성, 무결성, 가용성)등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.	O	O
		13.1.2 인증 및 암호화 기능	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요 정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.	O	O
		13.1.3 보안로그 기능	클라우드 시스템 설계 시 사용자의 인증, 권한변경, 중요정보 이용 및 유출 등에 대한 감사 증적을 확보할 수 있도록 하여야 한다.	O	O
		13.1.4 접근권한 기능	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.	O	O
		13.1.5 시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화하여야 한다. 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여야 한다.	O	O
	13.2 구현 및 시범	13.2.1 구현 및 시험	안전한 코딩방법에 따라 클라우드 시스템을 구현하고, 분석 및 설계과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다.	O	O
		13.2.2 개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.	O	O
		13.2.3 시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.	O	O

구 분			세부 조치사항	IaaS	SaaS
		13.2.4 소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운연환경에 보관하지 않는 것을 원칙으로 한다.	O	O
	13.3 외주개발 보안	13.3.1 외주개발 보안	클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.	O	O
	13.4 시스템 도입 보안	13.4.1 시스템 도입 계획	클라우드 시스템의 처리속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립하여야 한다.	O	X
		13.4.2 시스템 인수	새로 도입되는 시스템에 대한 인수 기준이 수립되어야 하며, 인수 전에 테스트가 수행되어야 한다.	O	X

첨부2 금융부문 추가 보호조치

국내·외 클라우드 보안인증제를 취득하여 평가 생략이 가능한 **기본 보호조치 항목과 별도**로, 금융회사가 전자금융감독규정 등 **법규 준수를 위해 꼭 필요한 사항**을 **지원 및 협조** 받을 수 있는지를 평가한다.

1. 클라우드서비스 제공자의 건전성에 관한 사항

전자금융보조업자 재무건전성 평가(감독규정 제60조제1항제10호)에 준하여 실시

제60조(외부주문등에 대한 기준) ① 10. 전자금융보조업자에 대한 재무건전성을 연1회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시

2. 금융회사의 의무 준수를 위해 클라우드서비스 제공자의 지원 및 협조가 필수적인 사항

금융부문 추가 보호조치 항목	세부 조치사항	감독규정 관련 조문
2.1 사고 보고 및 분석 수행 절차 확보	사고보고 및 분석을 위해 사고조사 지원, 훈련 지원 등 금융위원회, 금융감독원, 침해사고대응기관의 협조 요청에 대응할 수 있도록 체계가 마련되어 있는가?	제37조의4(침해사고대응기관 지정 및 업무범위 등), 제73조(정보기술부문 및 전자금융 사고보고)
	전산장애, 전자적 침해행위 등 발생 시 금융회사 및 침해사고대응기관에 즉시 알리고 적절히 대처할 수 있는 방안이 마련되어 있는가?	
2.2 금융권 통합보안관제 수행 체계 지원	금융권 통합 보안관제수행을 위한 관리적·물리적·기술적 지원 체계가 마련되어 있는가?	
2.3 취약점 분석·평가 수행 체계 지원	관계 법규에 따라 금융회사가 취약점 분석·평가를 수행할 수 있도록 지원 체계가 마련되어 있는가?	제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)
	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?	
2.4 합동비상대응훈련 지원	금융회사가 수립한 비상대책에 따른 비상대응훈련 및 재해복구전환훈련 실시에 대해 협조 및 지원하도록 체계가 마련되어 있는가?	제24조(비상대응훈련 실시)
	필요한 경우 금융위원회가 실시하는 금융분야 합동비상대응훈련에 참여하고 지원하도록 체계가 마련되어 있는가?	

금융부문 추가 보호조치 항목	세부 조치사항	감독규정 관련 조문
2.5 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?	제9조(건물에 관한 사항), 제10조(전원, 공조 등 설비에 관한 사항), 제11조(전산실 등에 관한 사항)
	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?	
2.6 전산자료 보호	사용자계정과 비밀번호를 개인별로 부여하고, 관리하기 위한 기능을 제공하는가?	제13조(전산자료 보호대책)
	전산자료를 정기적으로 백업하고 검증할 수 있도록 지원 체계가 마련되어 있는가?	
	정보처리시스템 관리자의 주요 업무 관련 행위를 책임자 또는 금융회사가 이중확인 및 모니터링 할 수 있는 기능을 제공하는가?	
	정보처리시스템의 가동기록을 1년 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 접근 권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제 장치를 마련·운용하는가?	
2.7 이중화 및 백업체계 구축	(주요 전산장비의 경우) 금융회사가 이중화 또는 예비장치를 확보할 수 있도록 협조 및 지원 체계가 마련되어 있는가?	제23조(비상대책 등의 수립·운용)
	금융회사가 각 업무별로 지정한 복구목표시간을 준수할 수 있도록 협조 및 지원 체계가 마련되어 있는가?	
	장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 상황별 대응절차, 재해복구계획, 비상대응조직의 구성 및 운용, 모의훈련, 비상연락체계, 파업 시 비상지원인력, 업무매뉴얼 등을 포함한 업무지속성 확보방안을 수립·준수하고 주기적으로 점검하는가?	
2.8 해킹 등 방지대책	시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업을 실시하고 있는가?	제15조(해킹 등 방지대책)
	내부 업무용시스템 설치 시 인터넷 등 외부통신망과 분리·차단 및 접속을 금지(물리적 또는 논리적) 할 수 있도록 기능을 제공하고 지원하도록 체계가 마련되어 있는가?	

금융부문 추가 보호조치 항목	세부 조치사항	감독규정 관련 조문
	패치 수행 등을 위해 중앙에서 파일을 배포할 경우 무결성 검증을 수행하는가?	
	클라우드서비스 제공자 내에서 클라우드 시스템 관리를 목적으로 클라우드 시스템에 직접 접속하는 단말기에 대해서는 인터넷 등 외부 통신망으로부터 분리(물리적 또는 논리적) 하는가?	
	금융회사가 클라우드서비스 이용 정보처리시스템 및 정보통신망에 대해 정보보호시스템을 설치·운영할 수 있도록 지원 체계가 마련되어 있는가?	
	해킹 등 전자적 침해행위로 인한 사고를 방지하기 위해 적절한 정보보호시스템을 설치하여 안전하게(이력보관, 접근통제 등) 운영하고 있는가?	
2.9 기타	금융회사가 재무건전성 평가 등 주요 경영활동에 대해 상시 모니터링을 실시할 수 있도록 지원 체계가 마련되어 있는가?	제60조(외부주문등에 대한 기준)
	금융회사가 서비스 품질수준을 평가할 수 있도록 지원 체계가 마련되어 있는가?	
	금융회사의 정보처리업무 위탁과 관련한 계약서, 계약서 부속자료 및 그 밖의 전자금융업무와 관련한 자료 등을 금융감독원의 요구를 수용하도록 체계가 마련되어 있는가?	제61조(전자금융보조업자 자료제출 기준)
	금융회사가 개인(신용)정보 관련 규제 등 기타 금융관련 법령을 준수하는데 필요한 사항을 지원 및 협조하도록 체계가 마련되어 있는가?	-

별첨

금융분야 클라우드컴퓨팅 서비스 이용 관련 참고자료

1. 전자금융감독규정 개정·시행 보도자료 (금융위원회, '19.12.7.)
2. 관련 규정

[1] 전자금융감독규정 개정·시행 보도자료

(금융위원회, `19.12.7.)

금융위원회	보 도 자 료				
	보도	2018.12.7.(금) 11:00	배포	2018.12.7.(금)	

책 임 자	금융위 전자금융과장 주 홍 민(02-2100-2970)	담 당 자	김 영 진 사무관 (02-2100-2973)
	금감원 IT.핀테크전략국장 전 길 수(02-3145-7420)		정 기 영 팀장 (02-3145-7415)

제 목 : 「전자금융감독규정」 개정·시행(2019년 1월 1일)

- 금융회사가 클라우드를 자율적으로 안전하게 활용할 수 있게 됩니다.

1. 개정 배경

□ 금융위원회는 '18.12.5(水) 제21차 정례회의를 개최하여, 「**전자금융감독규정 개정안**」을 **심의 · 의결**하고 '19.1.1일 시행할 예정

○ 지난 '16년부터 금융권은 개인신용정보가 아닌 '비중요 정보'에 한해 클라우드를 허용하였으나,

- 최근 **금융분야 디지털화(digitalization)가 폭넓게 확산**됨에 따라 클라우드 이용 확대와 관련한 추가 규제완화 필요성이 지속 제기

* 클라우드 규제완화 건의, 전문가 의견 수렴(핀테크 간담회(4.11), 클라우드 간담회(4.17))

○ 이에 금번 개정안은 클라우드 활용 범위를 **개인신용정보까지 확대**하되, **금융권 보안수준 및 관리·감독체계를 강화**하도록 함

2. 주요 내용

1 금융권 클라우드 이용범위 확대 (§14조의2 제1항·제8항)

○ **(현행)** 금융회사 · 전자금융업자는 중요정보(개인신용정보 · 고유식별정보)를 포함하지 않은 **非중요정보만 클라우드**에서 이용 가능

○ **(개선) 개인신용정보 · 고유식별정보도 클라우드에서 이용** 가능

2 금융권 클라우드서비스 안전성 기준 제시 (§14조의2 제1항, 별표2의2)

○ **(현행)** 금융회사 등이 비중요정보만을 이용할 수 있고, **별도의 클라우드 서비스의 안전성 기준이 없음**

○ **(개선) 금융분야 특수성을 반영한 안전성 확보조치** 등 금융권 클라우드 이용·제공 기준을 제시

< 금융 클라우드 안전성 기준 >

데이터 보호	금융권 통합보안관제 지원, **전산자료 접근통제, 정보시스템 가동기록 보존**, 중요정보 **암호화 등 데이터 보호**, 개인(신용)정보법 등 금융관련 법령 준수
서비스장애 예방/대응	클라우드 이용시에도 주요 전산장비 **이중화 및 백업체계를 구축**, 서비스 **연속성 보장, 장애 발생시 비상 대응조치·통지 의무**

3 클라우드에 대한 내부통제 강화 (§14조의2 제1항·제2항 등)

○ **(현행)** 개인신용정보·고유식별정보를 포함하지 않은 **비중요 정보 시스템**에 대해서 **별도의 안전성 평가없이**도 지정·운영

○ **(개선)** 금융회사가 클라우드 서비스의 **안전성을 평가**하고, **자체 정보보호위원회 심의·의결**을 거치도록 함

4 클라우드 이용 관련 보고의무 등 감독 강화 (§14조의2 제3항~제6항)

○ **(현행)** 비중요정보 처리시스템 운영현황에 대해서만 보고

○ **(개선)** 정보의 중요도에 따라 클라우드 이용 현황을 **감독당국에 보고**하고, **법적책임, 감독·검사 의무** 등을 계약서에 명확화

5 국내 소재 클라우드 운영 (§14조의2 제8항)

○ 사고 발생시 법적 분쟁, 소비자 보호, 감독 관할 등을 고려해 **개인신용정보 처리**는 **국내 소재 클라우드**에 한해 **우선 허용**

6 기타 : 허가·등록의 **물적요건 정비 등**

3. 향후 운영방안

1 클라우드 운영원칙 : 이용 촉진, 자율보안·감독 강화

❶ 금융회사가 인공지능(AI) 상담, 상품개발, 데이터 분석 등을 위해 클라우드에서 **개인신용정보도 이용**하되, **자체 보안 수준을 강화**

* 클라우드 이용시 금융회사가 중요정보를 직접 통제·관리하고, 안전성 확보방안을 수립

❷ 클라우드 이용의 안전성을 위해 **보고의무를 강화**하고, **금융회사와 감독당국의 조사·접근권**(현장방문 포함)을 확보

2 금융회사 내부통제 절차 마련

❶ **(중요도 평가)** 금융회사는 클라우드 이용 업무에 대해 **정보의 중요도를 평가**하고, **개인신용정보 처리 여부** 등을 **사전확인**

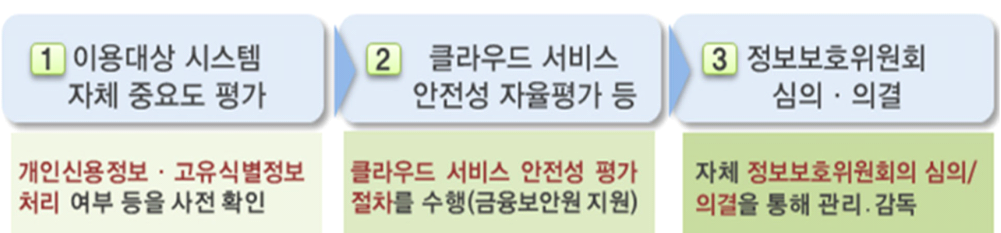
❷ **(안전성 평가)** 클라우드의 기술적·관리적 보호조치 등 안전성을 자체 평가하여 **안전성이 확보된 클라우드를 이용**

→ **금융보안원**이 금융회사의 클라우드 **안전성 평가를 지원**

❸ **(정보보호위원회 심의·의결)** 금융회사內 **자체 정보보호위원회***에서 안전성 평가결과와 클라우드 위수탁 운영기준 등을 **심의·의결**하여 관리·감독하고, 의결사항을 감독당국에 보고

* 금융회사의 정보보호최고책임자를 위원장으로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성

<금융권 클라우드 서비스 안전이용 절차>



3 금융회사·클라우드 제공자간 법적 책임 명확화

❶ **(사고예방)** 클라우드 제공자는 금융회사에 데이터의 물리적 위치(중요정보는 국내 한정)를 알리고, 정보보호 의무와 **서비스 장애 방지대책** 등 **클라우드 관리·보안요구사항**을 이행

❷ **(사고대응)** 사고 발생시 비상대응을 위해 국내 전산센터內 **필수 운영인력**이 **상주***하고, **장애 발생 사실을 신속 통지·대응****

- 특히, **신속한 장애 대응 및 복구**가 가능토록 개인신용정보를 처리하는 모든 시스템**(관리시스템 포함)**을 **국내에 설치**

* 전자금융감독규정 제23조 : 비상 상황시 신속 원상복구를 위한 비상지원인력을 확보

** 장애 발생시 이를 지체없이 통보하고, 진행상황 파악 등을 위한 컨택 포인트를 지정한 후 장애원인 분석 및 재발방지 대책을 금융회사에 제공

❸ **(손해배상) 손해배상, 재판관할 사항** 등을 계약서에 명시하여 금융회사·클라우드 제공자간 **법적 책임관계를 명확화**

- **고객 손해 :** 고객 피해 발생시 **금융회사가** 이용자에 대해 직접 **손해를 배상하고,** 클라우드 제공자는 연대 배상책임을 부담

- **금융회사 손해 :** 고의·과실로 인한 서비스 품질 저하·장애 등 발생시 **클라우드 제공자가** 금융회사의 **손해를 배상**

4 클라우드 이용 감독 강화

❶ 클라우드 이용시 금융회사가 **안전성 확보조치, 계약 내용 등**을 **감독당국에 보고**토록 하여 **모니터링**을 **강화**

❷ **금융회사·감독당국 조사·접근권**(현장방문 포함)을 **계약서**에 명시*

- 또한, 클라우드 이용계약 **시정·보완 요구권**(전자금융거래법 제40조제2항), 클라우드 사업자(전자금융보조업자)에 대한 **자료제출 요구권**을 통해 관리·감독(전자금융거래법 제40조제3항,4항,5항)

* EU·영국 등과 같이 클라우드 이용 계약서에 금융회사와 감독당국의 조사·접근권을 명시

※ 국내외 클라우드 운영 상황, 해외 사례 분석 등을 토대로 클라우드 제공자(전자금융보조업자)에 대한 감독당국의 **감독·조사권을 보다 강화**(법개정 사항)하는 방안을 추진

5 클라우드 이용 관련 데이터 보호장치 마련

❶ **전자금융거래법 · 신용정보법** 등에서 규정한 안전성 확보조치에 따른 **보호장치**를 마련

- **외부 통신망과 분리 · 차단***되도록 하고 사고 발생시 원인 파악을 위해 **정보시스템 기록을 보존**

* 클라우드 서비스를 이용하는 금융회사의 정보처리시스템에 대해 동일 클라우드를 이용하는 외부기관의 통신망과 분리·차단하고 접속을 금지

- **중요정보는 암호화 처리**하고, 클라우드 제공자 등 접근권한이 없는 자의 **열람은 불가**

❷ 범죄 수사를 위한 외국 정부의 정보제공 요청시 **국내법 위반 소지가 있을 경우 거부가 가능**

- 클라우드 제공자는 해당국의 **관계 법령을 사전 보고**하고, 요청이 있을 경우 **금융당국 · 금융회사에 사전 통지**하여 **동의** 받도록 함

※ **국내 클라우드** 시스템에 대해서는 미국 해외 정보 이용법(CLOUD법)*에 따른 **미국정부의 데이터 제공 요청에 반드시 따라야 하는 것은 아님**

* Clarifying Lawful Overseas Use of Data Act

○ 동 법은 **범죄 조사**에 필요한 해외 소재 데이터 확보 및 안보 유지를 위해 제정한 것으로, **외국 정부의 법령을 고려하여 데이터를 요청**할 수 있도록 함

* ① 고객 또는 가입자가 미국인이 아니며 미국에 거주하지 않고, ② 요구된 데이터 공개로 인해 사업자가 자격 있는 외국 정부의 법을 위반할 중대한 위험이 있는 경우, 사업자는 미국 정부의 데이터 요구에 대한 각하 · 변경을 법원에 청구할 수 있음 (Clarifying Lawful Overseas Use of Data Act §2703)

4. 향후 일정

□ 개정규정 : **'19.1.1일 시행** 예정

□ 「**금융권 클라우드 서비스 가이드라인**」 개정안 마련(12월중)

※ 별첨 : 금융권 클라우드 이용 확대 관련 Q&A

[참고자료] 금융권 클라우드 이용 확대 관련 Q&A (금융위원회 `18.12.)

1. 중요정보의 클라우드 허용에 따른 보안성 저하 우려에 대한 대책은?

□ 개인신용정보와 같은 중요정보도 클라우드로 이용하는 만큼, 금융회사 스스로 **엄격한 내부통제·보안 방안을 갖출 필요**

○ 금융회사는 **자체 정보보호위원회***에서 **클라우드 제공자의 건전성·안전성을 평가**하여 이용

* 금융회사의 정보보호최고책임자를 위원장으로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성

□ 아울러, 클라우드 제공자는 **전자금융거래법·신용정보법** 등에 따른 **암호화, 데이터 위·변조 방지 등** 보호조치를 준수해야 함

2. 해외 소재 클라우드의 허용 계획은?

□ 클라우드 이용 확대를 추진하면서, **금융보안의 중대성,** 사고 발생시 **소비자 보호·감독 관할 등은** 충분히 고려되어야 함

○ 이에 해외 소재 클라우드 허용은 **국내 소재 클라우드 운영** 이후 성과, 문제점 등을 고려하여 **점진적으로 검토**할 예정

○ 다만, 금융회사는 **국내 클라우드 사업자** 뿐만 아니라, **이미 국내에 전산센터***를 둔 **해외 클라우드 사업자의 서비스도 이용 가능**

* 국내센터 마련: 아마존(AWS), MS, IBM 등 / 구축 검토 : 구글, 오라클 등

□ 개인신용정보를 포함하지 않은 **비중요정보, 비식별 조치된 데이터**는 종전대로 **해외 소재 클라우드도 이용 가능**

3. 클라우드 이용시 클라우드서비스 제공자의 개인정보 열람 등 정보 유출의 위험이 있는 것은 아닌지?

□ 클라우드를 이용하는 경우에도 고객의 **개인정보**는 개인정보보호법·신용정보법에 따라 **암호화**하여 **전송***되며,

○ **클라우드서비스 제공자** 등 접근권한이 없는 자는 **열람이 불가**

* 개인정보보호법, 신용정보법에 따라 **고유식별정보, 개인신용정보**는 정보처리

위탁시 (클라우드 이용) 정보보호를 위한 **암호화 조치**를 하여야 함

※ **데이터의 '암호화 조치'란?**

- **원본 데이터(평문)**를 권한없는 제3자가 알아볼 수 없는 **형태로 치환(암호문)**하여 **전송·저장하는 조치로** 정보 유출시에도 **데이터 보호가 가능**

  * 권한있는 이용자는 **원래의 정보를** 복호화 처리(자신이 소유한 키값을 이용해 암호화된 데이터를 원문 상태로 복원)하면 **이용 가능**하다는 점에서 **원래의 데이터가 재식별되지 않는 개인정보의 비식별 조치**와는 구분됨

4. 최근 클라우드 장애 사고 처럼 주요 클라우드 사업자의 서비스 장애 발생할 경우 금융권 주요 서비스가 마비될 가능성이 있지 않은지? 이에 대한 대책은?

□ 사고 발생시 신속한 대응을 위해 국내 전산센터內 **필수 운영인력**이 **상주***하고, **장애 발생 사실을 지체없이 통지·대응****

○ **관리시스템을 포함**하여 개인신용정보를 처리하는 모든 시스템을 **국내에 설치**토록 하여 **신속한 장애 대응·복구**가 가능토록 함

* 전자금융감독규정 제23조 제2항 제2호 : 비상사태 발생 시 신속한 원상복구를 위한 비상지원인력 확보 등을 명시

** 장애 발생시 이를 지체없이 통보하고, 진행상황 파악 등을 위한 컨택 포인트를 지정한 후 장애원인 분석 및 재발방지 대책을 금융회사에 제공

※ 클라우드 관련 장애·재해가 발생해도 금융서비스가 중단되지 않도록 **중요 전산장비를 이중화하고 백업체계를 구축토록 함**

< 금융 클라우드 안전성 기준 >

데이터 보호	금융권 통합보안관제 지원, **전산자료 접근통제 및 정보시스템 가동기록 보존**, 중요정보 **암호화 등 데이터 보호**, 개인(신용)정보법 등 금융관련 법령 준수
서비스장애 예방/대응	클라우드 이용시에도 주요 전산장비 **이중화 및 백업체계를 구축**, 서비스 **연속성 보장, 장애 발생시 비상 대응조치·통지 의무**

5. 클라우드 이용과 관련한 사고 발생시 금융회사와 클라우드 서비스 제공자간 법적 책임의 범위는?

□ 클라우드 이용 관련 소비자 피해 발생시 **금융회사, 클라우드 제공자**가 고객에게 **연대배상 책임**을 부담함으로써 **두텁게 보호**

* 클라우드 이용시 위탁자인 금융회사는 수탁자인 클라우드 제공자와 연대하여 손해배상책임을 부담(업무위탁 규정 제3조 제5항, 전금법 제11조 제1항 등)

○ 또한, **손해배상·계약해지, 재판관할 사항** 등을 명시토록해 금융회사·클라우드 제공자간 **법적 책임관계를 명확화**

구분	고객 손해발생시 책임 (이용자→금융회사.클라우드제공자)	클라우드제공자 책임범위 명시 (금융회사.클라우드제공자)
책임 관계	사고발생시 **금융회사**가 **1차적 손해배상 책임**의 **주체**이며, **클라우드 제공자**는 수탁자로서 **연대배상책임을 부담**	고의.과실로 **서비스 품질 저하, .장애** 등 발생시 **클라우드제공자의 책임범위, 재판관할 등을 사전에 명시해** 분쟁을 예방

6. 美정부가 CLOUD법에 따라 미국 클라우드 서비스업체에 저장되는 우리 국민의 정보에 접근할 수 있다는데?

□ **국내 클라우드** 시스템은 미국 해외 정보 이용법(CLOUD법)*에 따른 美**정부의 데이터 제공 요청에 반드시 따라야 하는 것은 아님**

* Clarifying Lawful Overseas Use of Data Act

○ 동 법은 **범죄조사**에 필요한 해외 소재 데이터 확보·안보 유지를 위해 제정한 것으로, **외국 정부 법령을 고려하여 데이터를 요청**할 수 있도록 함

* ① 고객 또는 가입자가 미국인이 아니며 미국에 거주하지 않고, ② 요구된 데이터 공개로 인해 사업자가 자격 있는 외국 정부의 법을 위반할 중대한 위험이 있는 경우, 사업자는 미국 정부의 데이터 요구에 대한 각하 또는 변경을 법원에 청구할 수 있음

(Clarifying Lawful Overseas Use of Data Act §2703)

※ 범죄 수사를 위한 외국 정부의 정보제공 요청시 **국내법 위반 소지가 있을 경우 거부가 가능**

- 클라우드 제공자는 해당국의 **관계 법령을 사전 보고**하고, 정보제공 요청이 있을 경우 **금융당국·금융회사에 사전 통지하여 동의 받도**록 함

* 미국 CLOUD법은 미국정부의 범죄 조사를 위한 것으로, 정보 접근에 있어 외국인에 대해서는 예외가 인정되고 있음

7. 외국계 클라우드 사업자는 국내 개인정보보호 관련 법규를 따르지 않아 개인정보 보호에 취약한 것 아닌지?

□ 외국계 클라우드 사업자도 **국내 개인정보보호 법령을 준수**해야 함

○ 따라서, **중요정보 암호화, 접속기록 위·변조 방지, 시스템 접근 통제** 등 개인정보 보호 관련 제반 보호조치 사항을 준수해야 함

<참고 : 개인정보보호법·신용정보법상 안전성 확보 장치>

(**신용정보법 제17조 등**) 신용정보 위탁 제공시 암호화 등 보호조치 준수, 위탁 업무범위를 초과한 이용금지, 수탁자 교육, 재위탁 금지 등

(**개인정보보호법 제26조**) 제3자 업무 위탁시 목적외 개인정보처리 금지, 기술적·관리적 보호조치 준수, 수탁자 관리·감독 의무 등

(**개인정보보호법 제24조 및 제24조의2**) 암호화 등 안전성 확보조치 준수

8. 개정안은 클라우드서비스 제공자의 관리시스템을 국내에 설치하여야 하는지 여부가 불명확한데?

□ 현재 전자금융감독규정은 국내에 본점을 둔 금융회사의 **전산실 및 재해복구센터**를 **국내에 설치**토록 하고있음(제11조 제11호)

○ 전산실은 전산장비, 통신·보안장비, 전산자료가 보관된 장소를 의미하므로 **정보처리시스템을 포함**하고 있음(제2조 제1호)

□ 또한, **개인신용정보**를 처리하는 업무의 **정보처리시스템을 국내에 설치하도록 명시**(개정안 제14조의2 제8항)

○ 관련 법령 정의상 **클라우드 관리시스템**도 **'정보처리시스템'***에 해당하므로 개인신용정보를 처리하는 경우 이를 **국내에 두어야 함**

* 전자금융감독규정 제2조제3호 : "정보처리시스템"이라 함은 **전자금융업무를 포함하여 정보기술부문에 사용되는 하드웨어와 소프트웨어**를 말하며 **관련 장비를 포함한다**

9. 외국계 클라우드 서비스 업체에 대하여 감독·조사권이 실질적으로 확보될 수 있는 것인지?

□ 금융회사·클라우드 제공자간 계약 체결시 현장방문을 포함한 **클라우드 제공자의 감독·검사 의무**를 **계약서에 명시**토록 함

○ 감독당국은 사고 발생, 예방·점검 등 필요시 **자료제출 요구, 현장점검**을 통해 **관리·감독**할 수 있으며,

* EU, 영국 등 해외 사례와 같이 클라우드 이용 계약서에 금융회사와 감독당국의 조사·접근권을 명시토록 함

○ 관리시스템을 포함한 **개인신용정보를 처리하는 모든 시스템을 국내에 두도록 해** 감독당국의 **신속한 현장 감독·조사**가 가능

□ 국내외 클라우드 운영 상황, 해외 사례 분석 등을 토대로 클라우드 제공자(전자금융보조업자)에 대한 감독당국의 **감독·조사권을 보다 강화**(법개정 사항)하는 방안을 추진

10. 클라우드 보안 수준과 관련해 국내외 클라우드 업체간 규제 형평성의 차이는 발생하지 않는지?

□ 금융 클라우드 서비스 제공 관련 보호조치 기준에서 제시하는 안전성 확보조치 사항은 **국내외 클라우드 사업자 모두에게 동일**

○ 클라우드 안전성 확보조치 평가·검증과 관련하여 국내의 경우 **클라우드 서비스 보안인증(CSAP)**이 있으며

○ 해외의 경우 **FedRAMP(미국), CSA STAR(글로벌 협회), MTCS(싱가포르)** 등 국내 기준에 부합하는 일정한 인증을 받은 경우 이에 상응하는 보호조치를 갖춘 것으로 간주

* 관련 인증은 기본 보호조치에 관한 사항을 포함하고 있으며, **금융부문 추가 보호조치 사항은 평가를 생략할 수 없음**

○ 다만, 이경우에도 운영과정에서 미비점이 발견될 경우 금융회사·감독당국의 관리·감독을 통해 **보완 등 조치가 가능함**

- **FedRAMP :** 미국 정부 주관의 클라우드 보안인증 기준으로, 미국 정부에서 클라우드 이용 시 필수로 요구됨
- **CSA STAR :** 클라우드 보안협회 주도의 ISO 표준 기반의 인증 제도로, 민간 클라우드 인증 중 국제적으로 가장 인정받고 있음
- **MTCS :** 싱가포르 공공기관에서 운영 중인 인증 제도로, 싱가포르 공공기관 뿐만아니라 금융기관에서 클라우드 이용 시 필수로 요구됨

11. 해외 클라우드 사업자가 국내외 클라우드 보안인증을 취득하기만 하면 운영관리나 물리적 보호조치에 대한 관리·감독을 건너뛸 수 있게 되는 것 아닌지?

□ **국내·외 유효한 클라우드 관련 보안인증***을 취득·유지하고 있는 클라우드 서비스에 대해서는

* 금융 클라우드 이용 가이드에서 **적합한 인증범위 · 등급을 명시**할 계획

○ **인증기준이** 현행법상 클라우드가 갖추어야 할 **기술적 · 관리적 · 물리적 보호조치 기준을 이미 포함**하고 있어 이를 평가한 것으로 봄

* 관련 인증은 기본 보호조치에 관한 사항을 포함하고 있으며, **금융부문 추가 보호조치 사항은 평가를 생략할 수 없음**

○ 클라우드 **보안인증 외에도** 금융회사가 수행하는 클라우드서비스 제공자에 대한 **안전성 평가를 금융보안원이 지원**하여 안전성이 확보된 클라우드만을 이용할 수 있도록 내부 통제를 강화

○ 한편, 실제 운영과정에서 미비점이 발견될 경우 금융회사 또는 감독당국의 관리 · 감독을 통해 **보완 등 조치가 가능함**

[2] 관련 규정

전자금융감독규정

제1장 총칙

제1조(목적) 이 규정은 「전자금융거래법」(이하 "법"이라 한다) 및 동법 시행령(이하 "시행령"이라 한다)에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항 및 다른 법령에 따라 금융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "전산실"이라 함은 전산장비, 통신 및 보안장비, 전산자료 보관 및 출력장비가 설치된 장소를 말한다.
2. "전산자료"라 함은 전산장비에 의해 입력·보관·출력되어 있는 자료를 말하며 그 자료가 입력·출력되어 있는 자기테이프, 디스크, 디스켓, 콤팩트디스크(CD) 등 보조기억매체를 포함한다.
3. "정보처리시스템"이라 함은 전자금융업무를 포함하여 정보기술부문에 사용되는 하드웨어(hardware)와 소프트웨어(software)를 말하며 관련 장비를 포함한다.
4. "정보기술부문"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 정보를 수집·가공·저장·검색·송신 또는 수신을 행하는 금융회사 또는 전자금융업자의 업무, 인력, 시설 및 조직을 말한다.
5. "정보보호" 또는 "정보보안"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 수집·가공·저장·검색·송신 또는 수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 기술적·물리적·관리적 수단을 강구하는 일체의 행위를 말하며 사이버안전을 포함한다.
6. "정보보호시스템"이라 함은 정보처리시스템내 정보를 유출·위변조·훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램을 말한다.
7. "해킹"이라 함은 접근을 허가받지 아니하고 전자금융기반시설에 불법적으로 침투하거나 허가받지 아니한 권한을 불법적으로 갖는 행위 또는 전자금융기반시설을 공격하거나 해를 끼치는 행위를 말한다.
8. "컴퓨터악성코드"(이하 "악성코드"라 한다)라 함은 컴퓨터에서 이용자의 허락없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 이용자에게 피해를 주는 프로그램을 말한다.
9. "공개용 웹서버"라 함은 인터넷 이용자들이 웹페이지를 자유롭게 보고 웹서비스(월드 와이드 웹을 이용한 서비스를 말한다)를 이용할 수 있게 해주는 프로그램이 실행되는 장치를 말한다.
10. "정보통신망"(이하 "통신망"이라 한다)이라 함은 유·무선, 광선 등 정보통신수단에 의하여 부호·문자·음향·영상 등을 처리·저장 및 송·수신할 수 있는 정보통신 조직형태를 말한다.
11. 삭제

제3조(전자금융보조업자의 범위) 법 제2조제5호에서 "금융위원회가 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 정보처리시스템을 통하여 「여신전문금융업법」 상 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산에 관한 업무를 지원하는 사업자
2. 정보처리시스템을 통하여 은행업을 영위하는 자의 자금인출업무, 환업무 및 그 밖의 업무를 지원하는 사업자
3. 전자금융업무와 관련된 정보처리시스템을 해당 금융회사 또는 전자금융업자를 위하여 운영하는 사업자
4. 제1호 부터 제3호의 사업자와 제휴, 위탁 또는 외부주문(이하 "외부주문등"이라 한다)에 관한 계약을 체결하고 정보처리시스템을 운영하는 사업자

제2장 전자금융거래 당사자의 권리와 의무

제4조(확인에 필요한 구체적인 거래내용) 시행령 제7조제4항제6호에서 "금융위원회가 정하여 고시하는 사항"이란 다음 각 호를 말한다.

1. 법 제8조에 따른 오류정정 요구사실 및 처리결과에 관한 사항
2. 전자금융거래 신청, 조건변경에 관한 내용

제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준) ① 금융회사 또는 전자금융업자가 법 제9조제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다.

1. 「금융위원회의 설치 등에 관한 법률」 제38조제1호(다만, 「은행법」에 의한 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다) 및 제7호의 회사, 「전자금융거래법 시행령」 제2조제2호의 회사 : 20억원
2. 「금융위원회의 설치 등에 관한 법률」 제38조제8호의 회사, 「전자금융거래법」제2조제3호나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조제1호의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점 : 10억원
3. 「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원
4. 제1호 부터 제3호 이외의 금융회사 : 1억원. 다만, 제1호 부터 제3호 이외의 금융회사들이 관련 법령에 의해 당해 금융회사를 구성원으로 하는 금융회사를 통해 전자금융거래 관련 정보기술부문의 주요부분을 공동으로 이용하는 경우, 정보기술부문의 주요부문을 제공하는 금융회사가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제2호의 금액(시행령 제2조제5호의 금융회사는 제1호의 금액) 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의 보험 또는 공제에 가입한 것으로 본다.
5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원
6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원
7. 제5호, 제6호 이외의 전자금융업자 : 1억원 <종전의 제6호에서 이동>

② 금융회사 또는 전자금융업자가 전자금융사고 책임이행을 위한 준비금을 적립하는 경우에는 제1항 각 호에서 정한 금액 이상의 금액을 보유하고 책임이행이 신속

히 이루어질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야 한다.
③ 금융회사 또는 전자금융업자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우 보험 또는 공제의 보상한도는 제1항에서 정한 금액에서 준비금 적립액을 차감한 금액 이상으로 한다.
④ 제1항 부터 제3항의 규정은 전자금융업무를 취급하지 않는 금융회사에 대하여는 적용하지 아니한다.

제6조(추심이체 출금 동의의 방법 등) ① 시행령 제10조제1호에서 "금융위원회가 정하여 고시하는 전자문서"라 함은 다음 각 전자문서을 말한다.
1. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서
   가. 전자서명을 생성하기 위하여 이용하는 전자적 정보(이하 "전자서명생성정보" 라함)가 본인에게 유일하게 속할 것
   나. 전자서명 당시 본인이 전자서명생성정보를 지배·관리하고 있을 것
   다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것
   라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것
2. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서
   가. 서명 전 실명증표를 통해 본인확인
   나. 전자문서가 생성된 이후 서명자가 지급인 본인임을 확인 가능
   다. 전자서명 및 전자문서에 대한 위변조 여부 확인이 가능
   라. 전자문서를 고객에게 전송한 이후 고객이 취소할 수 있는 충분한 기간 부여
3. 삭제

② 시행령 제10조제1호 및 제2호에서 "금융위원회가 정하는 방법"이라 함은 다음 각 호의 방법을 말한다.
1. 전화 녹취
2. 음성응답 시스템(Audio Response System : ARS)

③ 지급인(출금계좌의 실지명의인을 포함한다)이 출금의 동의를 해지하는 경우에도 제1항 및 제2항의 규정을 준용한다.
④ 금융회사·전자금융업자 또는 수취인은 제1항 각 호의 출금 동의의 방법을 운용함에 있어 다음 각 호의 어느 하나에 해당하는 사실을 확인하여야 한다.
1. 지급인과 추심이체 출금계좌 실지명의인이 동일인인 사실
2. 지급인과 추심이체 출금계좌 실지명의인이 동일인이 아닐 경우에는 지급인이 당해 계좌에서 출금할 수 있는 권한을 보유하고 있는 사실

제6조의2(정보보호최고책임자의 지정대상) ① 시행령 제11조의3제1항 후단에서 "금융위원회가 정하여 고시하는 상시 종업원 수의 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.
② 시행령 <별표 1>의제3호나목 단서에서 "금융위원회가 정하여 고시하는 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.

제3장 전자금융거래의 안전성 확보 및 이용자 보호

제1절 통칙

제7조(전자금융거래 종류별 안전성 기준) 법 제21조제2항의 "금융위원회가 정하는 기준"이라 함은 다음 각 호의 내용에 관하여 제8조 부터 제37조에서 정하는 기준을 말한다.
1. 인력, 조직 및 예산 부문
2. 건물, 설비, 전산실 등 시설 부문
3. 단말기, 전산자료, 정보처리시스템 및 정보통신망 등 정보기술부문
4. 그 밖에 전자금융업무의 안전성 확보를 위하여 필요한 사항

제2절 인력, 조직 및 예산 부문

제8조(인력, 조직 및 예산) ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다.
1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것
2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것
3. 전산인력의 자질향상 및 예비요원 양성을 위한 교육 및 연수프로그램을 운영할 것
4. 정보보호최고책임자는 임직원이 정보보안 관련법규가 준수되고 있는지 정기적으로 점검하고 그 점검결과를 최고경영자에게 보고할 것
5. 최고경영자는 임직원이 정보보안 관련법규를 위반할 경우 그 제재에 관한 세부기준 및 절차를 마련하여 운영할 것

② 금융회사 또는 전자금융업자는 인력 및 예산에 관하여 다음 각 호의 사항을 준수하도록 노력하여야 한다.
1. 정보기술부문 인력은 총 임직원수의 100분의 5 이상, 정보보호인력은 정보기술부문 인력의 100분의 5 이상이 되도록 할 것
2. 정보보호예산을 정보기술부문 예산의 100분의 7 이상이 되도록 할 것

③ 제2항 각 호의 사항을 이행하지 못하는 금융회사 또는 전자금융업자는 그 사유 및 이용자 보호에 미치는 영향 등을 설명한 자료를 해당 금융회사 또는 전자금융업자가 운영하는 홈페이지 등을 통해 매 사업연도 종료 후 1개월 이내에 공시하여야 한다. 다만, 허가, 등록 또는 인가를 마친 후 1년이 지나지 않은 금융회사 또는 전자금융업자는 공시하지 아니할 수 있다.
④ 제2항제1호의 인력에 관한 기준은 <별표 1>과 같으며, 제2항제2호의 예산에 관한 기준은 <별표 2>와 같다.

제8조의2(정보보호위원회 운영) ① 금융회사 또는 전자금융업자는 중요 정보보호에 관한 사항을 심의·의결하는 정보보호위원회를 설치 운영하여야 한다.
② 정보보호위원회의 장은 정보보호최고책임자로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성한다.
③ 정보보호위원회는 다음 각 호의 사항을 심의·의결한다.
1. 법 제21조제4항에 따른 정보기술부문 계획서에 관한 사항
2. 법 제21조의2제4항제1호에 관한 사항
3. 법 제21조의3에서 정한 취약점 분석·평가 결과 및 보완조치의 이행계획에 관

한 사항
4. 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항
5. 기타 정보보호위원회의 장이 정보보안업무 수행에 필요하다고 정한 사항
④ 정보보호최고책임자는 정보보호위원회 심의·의결사항을 최고경영자에게 보고하여야 한다.
⑤ 최고경영자는 특별한 사정이 없는 한 정보보호위원회의 심의·의결사항을 준수하여야 한다.

제3절 시설부문

제9조(건물에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다.
1. 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것
2. 비상시 대피를 위한 비상계단 및 정전대비 유도등을 설치할 것
3. 번개, 과전류 등 고전압으로 인한 전산장비 및 통신장비 등의 피해 예방을 위하여 피뢰설비를 갖출 것
4. 서버, 스토리지(Storage) 등 전산장비 및 통신장비 등의 중량을 감안한 적재하중 안전대책을 수립·운용할 것
5. 화재발생 시 조기진압을 위한 소화기 및 자동소화설비 등을 갖추고, 화재전파방지를 위한 배연설비설치 등 화재예방 안전대책을 수립·운용할 것
6. 화재발생 위험이 높은 지역, 상습 침수지역 및 진동피해 발생지역 등 외부환경에 의하여 전산장비 등이 영향을 받을 수 있는 지역은 제외할 것

제10조(전원, 공조 등 설비에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다.
1. 전원실, 공조실 등 주요 설비시설에 자물쇠 등 출입통제장치를 설치할 것
2. 전원, 공조, 방재 및 방범 설비에 대한 적절한 감시제어시스템을 갖출 것
3. 전산실의 전력공급 중단에 대비하여 자가발전설비를 갖출 것
4. 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전전원장치(Uninterruptible Power Supply : UPS)를 갖출 것
5. 과전류, 누전에 의한 장애 방지를 위하여 과전류차단기, 누전경보기 등을 설치하고 일정한 전압 및 주파수 유지를 위한 정전압정주파수장치(Constant Voltage Constant Frequency : CVCF)를 갖출 것
6. 전산실에 공급되는 전원 및 공조 설비는 부하가 큰 설비부분과 분리하여 설치하고 공조 설비 상태 점검을 위한 압력계, 온도계 등을 갖출 것
7. 전산실에 24시간 동안 적정한 온도 및 습도를 유지하기 위해서 자동제어 항온·항습기를 갖출 것

제11조(전산실 등에 관한 사항) 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다.
1. 화재·수해 등의 재해 및 외부 위해(危害) 방지대책을 수립·운용할 것
2. 상시 출입문은 한 곳으로 정하며 상시 출입은 업무와 직접 관련이 있는 사전 등록자에 한하여 허용하고, 그 밖의 출입자에 대하여는 책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부를 기록·보관할 것
3. 상시 출입이 허용된 자 이외의 출입자의 출입사항에 대하여는 전산실의 규모 및 설치장소 등을 감안하여 무인감시카메라 또는 출입자동기록시스템 설치 등 적절한 조치를 취하여 사후 확인이 가능하도록 할 것
4. 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치할 것
5. 천정·바닥·벽의 침수로 인한 정보처리시스템의 장애가 발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등 방안을 강구할 것
6. 적정수준의 온도·습도를 유지하기 위하여 온도·습도 자료 자동기록장치 및 경보장치 설치 등 적절한 조치를 취할 것
7. 케이블이 안전하게 유지되도록 전용 통로관 설치 등 적절한 보호조치를 강구할 것
8. 정전에 대비하여 조명설비 및 휴대용손전등을 비치할 것
9. 집적정보통신시설(Internet Data Center : IDC) 등과 같이 다수의 기관이 공동으로 이용하는 장소에 정보처리시스템을 설치하는 경우에는 미승인자가 접근하지 못하도록 적절한 접근통제 대책을 마련할 것
10. 다음 각 목의 중요 시설 및 지역을 보호구역으로 설정 관리할 것
가. 전산센터 및 재해복구센터
나. 전산자료 보관실
다. 정보보호시스템 설치장소
라. 그 밖에 보안관리가 필요하다고 인정되는 정보처리시스템 설치장소
11. 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치할 것
12. 무선통신망을 설치하지 아니할 것

제4절 정보기술부문

제12조(단말기 보호대책) 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다.
1. 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것
2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것
3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것
4. 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것
5. 삭제

제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.
1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로

관리할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
3. 전산자료의 보유현황을 관리하고 책임자를 지정 · 운영할 것
4. 전산자료의 입력 · 출력 · 열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
5. 전산자료 및 전산장비의 반출 · 반입을 통제할 것
6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립 · 운용할 것
7. 정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것
8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록 · 관리할 것
9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것
10. 이용자 정보의 조회 · 출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)
11. 정보처리시스템의 가동기록은 1년 이상 보존할 것
12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것
13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)
14. 사용자가 전출 · 퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것

② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록 · 관리하여야 한다.

③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경 · 조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.

④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록 · 유지되어야 한다.
1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록

⑤ 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련 · 운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중 확인 및 모니터링을 하여야 한다.

제14조(정보처리시스템 보호대책) 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립 · 운용하여야 한다.
1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것
2. 데이터베이스관리시스템(Database Management System : DBMS) · 운영체제 · 웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성 · 보관할 것
3. 정보처리시스템의 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성 · 보관할 것
4. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링시스템을 갖출 것
5. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것
6. 정보처리시스템의 책임자를 지정 · 운영할 것
7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할 것
8. 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록 · 관리할 것
9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것
10. 정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것

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
2. <별표 2의2>의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가
3. <별표 2의3>에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의 · 의결을 거쳐야 한다.

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

④ 제3항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.
1. 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 각 호에 관한 서류
2. 제1항제1호에 따른 자체 중요도 평가 기준 및 결과
3. 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항
4. 제2항에 따른 정보보호위원회 심의·의결 결과
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 금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 변경사항이 발생한 날로부터 7영업일 이내에 발생 사유, 관련 자료 및 대응계획을 첨부하여 금융감독원장에게 보고하여야 한다.
1. 클라우드컴퓨팅서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등의 사유로 클라우드컴퓨팅서비스 이용계약에 중대한 변경사항이 발생한 경우
2. 클라우드컴퓨팅서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 아니한 경우
3. 제4항제2호 또는 제3호에 관한 중대한 변경사항이 발생한 경우
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.
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 전자지급결제대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.
⑨ 그 밖에 금융회사 또는 전자금융업자의 클라우드컴퓨팅서비스 이용에 대해서는 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따른다.

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.
1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)
4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것
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.)
② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.
1. 삭제
2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것
4. 정보보호시스템 원격관리를 금지할 것. 다만, 원격관리가 불가피한 경우 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것
5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것
6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것 <종전의 제5호에서 이동>
③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.
④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.
⑤ 삭제
⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.
1. 무선통신망 이용 업무는 최소한으로 국한하고 법 제21조의2에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것
4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것

제16조(악성코드 감염 방지대책) ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.
1. 응용프로그램을 사용할 때에는 악성코드 검색프로그램 등으로 진단 및 치료 후 사용할 것
2. 악성코드 검색 및 치료프로그램은 최신상태로 유지할 것
3. 악성코드 감염에 대비하여 복구 절차를 마련할 것

4. 제12조제3호에 따른 중요 단말기는 악성코드 감염여부를 매일 점검할 것

② 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다.

제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것
2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

1. 게시자료에 대한 사전 내부통제 실시
2. 무기명 또는 가명에 의한 게시 금지
3. 홈페이지에 자료를 게시하는 담당자의 지정·운용
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

③ 삭제

④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다.

⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

제18조(IP주소 관리대책) 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다.

1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며 내부 IP주소체계의 외부유출을 금지할 것
2. 개인별로 내부 IP주소를 부여하여 유지·관리할 것
3. 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것
4. 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP주소를 사용할 것. 다만, 외부직원 등과의 공동작업 수행 등 네트워크의 분리가 어렵다고 금융감독원장이 정하는 경우에는 업무특성별로 접근권한을 분리하여 IP주소를 사용할 수 있다.
5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용할 것

제5절 정보기술부문 내부통제

제19조(정보기술부문 계획서 제출 절차 등) ① 시행령 제11조의2에 따라 금융위원회에 정보기술부문 계획서를 제출해야 하는 금융회사 또는 전자금융업자는 현실적이고 실현 가능한 장·단기 정보기술부문 계획을 매년 수립·운용하여야 한다.

② 금융위원장은 금융감독원장으로 하여금 정보기술부문 계획서의 적정성 등을 평가한 후 관련보고서를 제출하게 할 수 있다.

제19조의2(정보보호 교육계획의 수립 시행) ① 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 다음 각 호의 기준에 따라 매년 교육계획을 수립·시행하여야 한다.

1. 임원 : 3시간 이상(단, 정보보호최고책임자는 6시간 이상)
2. 일반직원 : 6시간 이상
3. 정보기술부문업무 담당 직원 : 9시간 이상
4. 정보보호업무 담당 직원 : 12시간 이상

② 최고경영자는 정보보호교육을 실시한 이후 대상 임직원에 대해 평가를 실시하여야 한다.

③ 제1항의 교육프로그램 개발과 정보보호교육은 정보보호 전문 교육기관에 위탁할 수 있다.

제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진) 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다.

1. 조직에 미치는 영향이 크거나 내부직무전결기준에 따라 부서장 전결 금액 이상의 사업 추진 시에는 사전에 충분한 타당성 검토를 실시할 것
2. 정보처리시스템의 신규 사업 및 통합·전환·재개발 등과 같은 주요 추진사업에 대하여 비용 대비 효과분석을 실시할 것
3. 타당성 검토와 비용 대비 효과분석 결과는 전산운영위원회 등 독립적인 조직의 승인을 받을 것
4. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 분석·설계 단계부터 보안대책을 강구할 것

제21조(정보처리시스템 구축 및 전자금융거래 관련 계약) 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다.

1. 적합한 업체를 공정하게 선정하기 위하여 객관적인 업체 선정 기준 및 절차를 마련·운용할 것
2. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 제1호에 따른 기준 및 절차의 내용에는 정보보안 관련 사항을 포함할 것
3. 공정하고 합리적인 예정가격 산출 기준을 수립·적용할 것
4. 계약금액, 구축완료일자, 납품방법 및 대금지급방법 등 계약이행에 필요한 내용을 포함한 계약서 작성 기준을 수립·운용할 것
5. 구매 또는 개발한 제품의 소유권, 저작권 및 지적재산권 등의 귀속관계를 명확

히 하여 사후 분쟁이 발생하지 않도록 할 것
6. 납품 또는 개발이 완료된 소프트웨어 등에 대하여 공급업체 파산 등 비상사태에 대비한 대책을 마련·운용할 것
7. 검수는 개발자, 계약자 등 이해당사자를 배제하여 공정하게 실시할 것
8. 계약조항을 이행하지 못하는 사유가 발생하였거나 계약조항을 변경할 경우에는 검사부서의 승인을 받을 것
9. 내부감사규정에 따라 감사가 정한 금액 이상의 계약에 대하여는 자체 감사를 실시하거나 검사부서의 승인을 받을 것

제22조(정보처리시스템 감리) 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여 다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야 한다.
1. 목적 및 대상, 시스템 감리인, 감리시기 및 계획 등 일반기준
2. 기획, 개발 및 운용의 감리 실시 기준
3. 지적사항 및 개선사항 등 감리 후 보고 기준
4. 전자금융업무와 관련된 외부주문등에 대한 감리 기준

제23조(비상대책 등의 수립·운용) ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립·준수하여야 한다.
1. 상황별 대응절차
2. 백업 또는 재해복구센터를 활용한 재해복구계획
3. 비상대응조직의 구성 및 운용
4. 입력대행, 수작업 등의 조건 및 절차
5. 모의훈련의 실시
6. 유관기관 및 관련업체와의 비상연락체제 구축
7. 보고 및 대외통보의 범위와 절차 등

② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다.
1. 파업 시 핵심전산업무 종사자의 근무지 이탈에 따른 정보처리시스템의 마비를 방지하기 위하여 비상지원인력을 확보·운영할 것
2. 비상사태 발생 시에도 정보처리시스템의 마비를 방지하고 신속히 원상복구가 될 수 있도록 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문업체를 활용하는 방안을 수립·운영할 것
3. 비상지원인력이 사용법을 충분히 이해하고 업무운용이 가능한 수준으로 전산시스템 운영지침서, 사용자매뉴얼 등을 쉽고 자세하게 작성하고 최신상태로 유지할 것
4. 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시할 것

③ 금융회사 또는 전자금융업자는 제1항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하여야 한다.
④ 「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의 「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립·준수하고 이를 금융위원회에 알려야 한다.
⑤ 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운영하여야 한다.
⑥ 제4항에 따른 행동매뉴얼 또는 제5항에 따른 비상대책에는 제1항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.
⑦ 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다.
⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다.
1.「은행법」에 의해 인가를 받아 설립된 은행(다만,「은행법」제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다)
2.「한국산업은행법」에 의한 한국산업은행, 「중소기업은행법」에 의한 중소기업은행, 「농업협동조합법」에 의한 농협은행, 「수산업협동조합법」에 의한 수산업협동조합중앙회의 신용사업부문
3.「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자(다만, 「자본시장과 금융투자업에 관한 법률」 제12조에 의해 인가를 받은 외국투자매매업자·투자중개업자의 지점 등은 제외한다)
4.「자본시장과 금융투자업에 관한 법률」에 의한 증권금융회사 및 한국예탁결제원
5.「자본시장과 금융투자업에 관한 법률」에 의한 거래소
6.「여신전문금융업법」에 의한 신용카드업자(다만, 법인신용카드 회원에 한하여 신용카드업을 영위하는 자는 제외한다)
7.「보험업법」에 의한 보험요율산출기관
8.「상호저축은행법」에 의한 상호저축은행중앙회
9.「신용협동조합법」에 의한 신용협동조합중앙회
10.「보험업법」에 의한 보험회사

⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24시간 이내로 한다.
⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다.
[제9항에서 이동 <2015. 6. 24.>]

제24조(비상대응훈련 실시) ① 금융회사 또는 전자금융업자는 제23조제4항에 따른 행동매뉴얼 또는 같은 조 제5항에 따른 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다.
② 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다.

③ 금융위원회는 제2항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다.
1.「정부조직법」 제15조에 따른 "국가정보원(국가사이버안전센터)"
2.「경찰법」 제2조에 따른 "경찰청(사이버테러대응센터)"
3. 침해사고대응기관
4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관
④ 금융회사 또는 전자금융업자는 제1항 및 제2항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.

제25조(정보처리시스템의 성능관리) 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.

제26조(직무의 분리) 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다.
1. 프로그래머와 오퍼레이터
2. 응용프로그래머와 시스템프로그래머
3. 시스템보안관리자와 시스템프로그래머
4. 전산자료관리자(librarian)와 그 밖의 업무 담당자
5. 업무운영자와 내부감사자
6. 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력
7. 정보기술부문인력과 정보보호인력
8. 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우

제27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용하여야 한다.
② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.
③ 금융회사 또는 전자금융업자는 대차대조표 등 중요 자료의 계상액과 각종 보조부·거래기록·전산원장파일의 계상액에 대한 상호일치 여부를 전산시스템을 통하여 주기적으로 확인하여야 한다.
④ 금융회사 또는 전자금융업자는 제3항에 따른 확인 결과 불일치가 발견된 때에는 그 원인 및 조치 내용을 전산자료의 형태로 5년간 보존하여야 한다.
⑤ 금융회사 또는 전자금융업자는 이용자 중요원장에 직접 접근하여 중요원장을 조회·수정·삭제·삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존하여야 한다.

제28조(거래통제 등) ① 금융회사 또는 전자금융업자는 사고위험도가 높은 거래에 대하여는 책임자 승인거래로 처리토록 하는 등 전산시스템에 의한 이중확인이 가능하도록 하여야 한다.
② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다.

제29조(프로그램 통제) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다.
1. 적용대상 프로그램 종류 및 등록·변경·폐기 방법을 마련할 것
2. 프로그램 변경 전후 내용을 기록·관리할 것
3. 프로그램 등록·변경·폐기내용의 정당성에 대해 제3자의 검증을 받을 것
4. 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정할 것
5. 프로그램에 대한 접근은 업무담당자에 한정할 것
6. 운영시스템 적용은 처리하는 정보의 기밀성·무결성·가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 실시할 것
7. 프로그램 반출, 실행프로그램의 생성 및 운영시스템 등록은 전산자료 관리자 등 해당프로그램 담당자 이외의 자가 수행할 것
8. 운영체제, 데이터베이스관리프로그램 등의 시스템 프로그램도 응용프로그램과 동일한 수준으로 관리할 것
9. 프로그램 설명서, 입·출력 레코드 설명서, 프로그램 목록 및 사용자·운영자지침서 등 프로그램 유지보수에 필요한 문서를 작성·관리할 것
10. 전자 금융거래에 사용되는 전산프로그램은 실제 업무를 처리하는 정보처리시스템에 설치하기 전에 자체 보안성 검증을 실시할 것

제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다.
1. 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행할 것
2. 일괄작업은 최대한 자동화하여 오류를 최소화할 것
3. 일괄작업 수행 과정에서 오류가 발생하였을 경우 반드시 책임자의 확인을 받을 것
4. 모든 일괄작업의 작업내용을 기록·관리할 것
5. 책임자는 일괄작업 수행자의 주요업무 관련 행위를 모니터링할 것

제31조(암호프로그램 및 키 관리 통제) ① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다.
② 금융회사 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.

제32조(내부사용자 비밀번호 관리) 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.
1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설

정하고 분기별 1회 이상 변경
나. 비밀번호 보관 시 암호화
다. 시스템마다 관리자 비밀번호를 다르게 부여
3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인 절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

제33조(이용자 비밀번호 관리) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유 · 내용 등을 기록 · 관리하여야 한다.
② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.
1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
2. 통신용 비밀번호와 계좌원장 비밀번호를 구분해서 사용
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)
4. 금융회사가 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것
5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록 · 사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것

제6절 전자금융업무

제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.
1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)
2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것.
4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것
5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위 · 변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

② 삭제

제35조(이용자 유의사항 공지) 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다.
1. 비밀번호 유출위험 및 관리에 관한 사항
2. 금융기관 또는 전자금융업자가 제공하고 있는 이용자 보호제도에 관한 사항
3. 해킹 · 피싱 등 전자적 침해 방지에 관한 사항
4. 본인확인 절차를 거쳐 비밀번호 변경이 가능하도록 정보처리시스템을 구축하고 비밀번호 변경 시 같은 번호를 재사용하지 않도록 할 것

제36조(자체 보안성심의) ① 금융회사 또는 전자금융업자는 다음 각 호의 행위를 하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다.
1. 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행
2. 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정
② 금융회사 또는 전자금융업자는 제1항에 따른 심의(이하 "자체 보안성심의"라 한다)를 마친 후 제1항 각 호의 행위를 수행한 날로부터 7일 이내에 금융감독원장이 정하는 자체 보안성심의 결과보고서를 금융감독원에 제출하여야 한다. 다만, 제1항제1호에 따른 보안성심의의 경우 신규 전자금융업무가 제공 또는 시행된 날을 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 기관으로서 금융감독원장이 정하는 기준에 해당하는 금융회사 또는 전자금융업자는 그러하지 아니하다.
③ 금융감독원장은 제2항에 따라 제출받은 자체 보안성심의 결과보고서를 검토한 결과, 보안수준이 충분하지 않다고 인정되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선 · 보완을 요구할 수 있다.
④ 제2항 및 제3항에도 불구하고 다음 각 호의 기관은 제1항제1호에 따른 자체 보안성심의 결과보고서의 제출을 하지 아니할 수 있다.
1. 「우체국예금 · 보험에 관한 법률」에 의한 체신관서
2. 「새마을금고법」에 의한 새마을금고 및 새마을금고중앙회
3. 「한국수출입은행법」에 따른 한국수출입은행
4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관

제37조(인증방법 사용기준) 금융회사 또는 전자금융업자는 전자금융거래의 종류 · 성격 · 위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.

제37조의2(전자금융기반시설의 취약점 분석 · 평가 주기, 내용 등) ① 전자금융기반시설의 취약점 분석 · 평가는 총자산이 2조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다.
② 금융회사 및 전자금융업자는 취약점 분석 · 평가를 위하여 정보보호최고책임자

(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100분의 30 이상은 「정보보호산업의 진흥에 관한 법률 시행규칙」 제8조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제37조의3제1항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다.

③ 제1항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석·평가의 내용은 금융감독원장이 정한다.

④ 금융회사 및 전자금융업자는 해당 주기 내에 평가 대상 시설과 평가기간을 나누어 평가할 수 있다.

⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다.

1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행
2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것
3. 이행계획의 시행 결과는 최고경영자에게 보고할 것

⑥ 금융회사 또는 전자금융업자는 제1항 또는 제3항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.

제37조의3(전자금융기반시설의 취약점 분석·평가 전문기관의 지정 등) ① 전자금융기반시설의 취약점 분석·평가를 위한 평가전문기관은 다음 각 호의 자로 한다.

1. 「정보통신기반 보호법」 제16조에 따라 금융분야 정보공유·분석센터로 지정된 자
2. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호전문서비스 기업
3. 침해사고대응기관
4. 금융위원장이 지정하는 자

② 금융회사 및 전자금융업자는 시행령 제11조의5제3항에 따른 전자금융기반시설의 취약점 분석·평가 결과보고서를 금융위원장에게 제출하여야 하며, 금융감독원장은 결과보고서를 분석하여 매분기 1개월 이내에 금융위원장에게 보고하여야 한다.

③ 금융위원장은 취약점 분석·평가 결과보고서에 근거하여 필요시 금융회사 및 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

제37조의4(침해사고대응기관 지정 및 업무범위 등) ① 침해사고에 대응하기 위한 침해사고대응기관은 다음 각 호의 자로 한다.

1. 금융보안원
2. 삭제
3. 금융위원장이 지정한 자

② 침해사고대응기관은 다음 각 호의 업무를 수행한다.

1. 침해사고에 관한 정보의 수집·전파를 위한 정보공유체계의 구축
2. 침해사고의 예보·경보 발령내용의 전파
3. 침해사고의 원인분석과 신속한 대응 및 피해 확산방지를 위해 필요한 조치
4. 금융회사 및 전자금융업자와 관련된 해킹 등 전자적 침해행위 정보를 탐지·분석하여 즉시 대응 조치를 하기 위한 기구(이하 "금융권 통합 보안관제센터"라 한다)의 운영
5. 금융회사 및 전자금융업자의 침해사고 예방, 대응을 위한 자율기준의 마련 및 운영

③ 금융위원장은 침해사고대응기관을 포함하여 침해사고조사단을 구성할 수 있다.

④ 금융위원장은 제2항에 따른 침해사고 긴급대응을 위한 침해사고대응기관의 업무 수행 또는 제3항에 따른 침해사고 원인분석 및 긴급조치를 위하여 금융회사 및 전자금융업자, 전자금융보조업자에 협조를 요청할 수 있다.

⑤ 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 연 1회 이상 침해사고 대응 및 복구훈련 계획을 수립·시행하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게 제출하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다.

1. 법 제2조제3호가목의 금융회사 중 신용협동조합
2. 법 제2조제3호다목·라목의 금융회사
3. 시행령 제2조제4호부터 제6호까지의 조합
4. 시행령 제5조제2항의 요건을 충족한 금융회사

⑥ 금융위원장은 침해사고대응기관의 장으로 하여금 침해사고 대응·복구 및 훈련 결과를 점검하고 보완이 필요하다고 판단되는 경우 개선·보완을 요구할 수 있다.

⑦ 금융위원장은 침해사고대응기관의 장으로 하여금 시행령 제11조의6제1항제4호에 따른 보안취약점 통보를 위하여 금융회사 및 전자금융업자가 사용하고 있는 소프트웨어에 대한 조사·분석을 실시하게 할 수 있다.

제37조의5(정보보호최고책임자의 업무) 정보보호최고책임자는 정보보안점검의 날을 지정하고, 임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고, 그 점검 결과 및 보완 계획을 최고경영자에게 보고하여야 한다.

제38조(금융위원회가 정하는 보관자료 및 거래기록 등) 시행령 제12조제1항제2호다목에서 "금융위원회가 정하여 고시하는 거래기록"이라 함은 제4조제1호의 기록을 말한다.

제39조(전자지급수단의 이용한도) 시행령 제13조제2항 부터 제4항에 따라 금융위원회가 정하는 전자지급수단의 구체적인 이용한도는 <별표 3>과 같다.

제40조(약관교부 방법 등) ① 전자금융업무를 수행하는 금융회사 및 전자금융업자는 전자금융거래와 관련한 약관(이하 "약관"이라 한다)을 별도로 마련하여야 한다.

② 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자의 요청이 있는 경우 전자문서의 전송(전자우편을 이용한 전송을 포함한다), 모사전송, 우편 또는 직접 교부의 방식으로 전자금융거래 약관의 사본을 이용자에게 교부하여야 한다.

③ 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자가 약관의 내용에 대한 설명을 요청하는 경우 다음 각 호의 어느 하나의 방법으로 이용자에게 약관의 중요내용을 설명하여야 한다.

1. 약관의 중요내용을 이용자에게 직접 설명
2. 약관의 중요내용에 대한 설명을 전자적 장치를 통하여 이용자가 알기 쉽게 표시하고 이용자로부터 해당 내용을 충분히 인지하였다는 의사표시를 전자적 장치를 통하여 수령

④ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 그 시행일 1월 전에 변경되는 약관을 해당 전자금융거래를 수행하는 전자적 장치(해당 전자적 장치에 게시하기 어려울 경우에는 이용자가 접근하기 용이한 전자적 장치로서 당해 금융회사 등이 지정하는 대체장치를 포함한다. 이하 이 조에서 같다)에 게시하고 이용자에게 통지하여야 한다. 다만, 이용자가 이의를 제기할 경우 금융회사 또는 전자금융업자는 이용자에게 적절한 방법으로 약관 변경내용을 통지하였음을 확인해 주어야 한다.

⑤ 금융회사 또는 전자금융업자가 법령의 개정으로 인하여 긴급하게 약관을 변경한 때에는 변경된 약관을 전자적 장치에 최소 1월 이상 게시하고 이용자에게 통지하여야 한다.

제41조(약관 제정 또는 변경에 따른 보고 등) ① 법 제25조제1항 단서에서 "금융위원회가 정하는 경우"란 다음 각 호와 같다.

1. 이용자의 권익을 확대하거나 의무를 축소하기 위한 약관의 변경
2. 금융감독원장에게 보고된 약관의 내용과 동일하거나 유사한 약관의 제정 또는 변경
3. 그 밖에 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융감독원장이 정하는 약관의 제정 또는 변경

② 금융회사 또는 전자금융업자가 전자금융거래 약관을 제정 또는 변경하고자 하는 경우에는 해당 약관 및 약관내용을 이해하는데 필요한 관련서류를 시행예정일 45일 전까지 금융감독원장에게 제출하여야 한다. 이 경우 약관 및 관련서류는 전자문서로 제출할 수 있다.

③ 금융감독원장은 제2항의 규정에 따라 제출받은 약관을 심사하고 건전한 금융거래질서의 유지를 위하여 약관내용의 변경이 필요하다고 인정하는 경우 해당 금융회사 또는 전자금융업자에 대하여 약관의 변경을 권고할 수 있다.

④ 제3항의 규정에 따라 변경권고를 받은 금융회사 또는 전자금융업자는 권고의 수락여부를 금융감독원장에게 보고하여야 한다.

제4장 전자금융업의 허가와 등록 및 업무
제1절 허가 및 등록의 대상과 절차

제42조(총발행잔액의 산정방법 등) ① 시행령 제15조제5항에 따른 선불전자지급수단 발행 시 총발행잔액은 등록신청일이 속하는 사업연도의 직전 사업연도 1분기(직전 사업연도 1분기말 이후에 사업을 개시한 경우에는 사업개시한 날이 속하는 분기를 말한다)부터 등록신청일 직전 분기까지 각 분기말 미상환 발행잔액의 단순평균으로 한다. 다만, 사업기간이 3월 미만인 경우에는 등록신청일 직전 월말 미상환 발행잔액으로 한다.

② 법 제28조제3항제1호다목에 따라 금융위원회에 등록하지 아니하고 선불전자지급수단을 발행하는 자는 매분기말 기준으로 선불전자지급수단의 미상환잔액을 평가하여 이를 시행령 제15조제6항에 따른 지급보증, 상환보증보험 또는 공제에 반영하여야 한다.

제42조의2(거래금액 기준) ① 법 제30조제3항제1호에서 "금융위원회가 정하는 기준"이라 함은 당해 전자금융업에 대한 분기별 결제대행금액(이용자가 지급한 재화 및 용역의 매출총액), 결제대금예치금액 또는 전자고지결제금액이 30억원 이하에 해당하는 경우를 말한다.

② 법 제30조제4항에서 "금융위원회가 정하는 기한"이라 함은 신고한 때로부터 6월 이내를 말한다.

③ 등록 자본금 초과시 신고와 관련한 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.

제43조(허가등 절차의 구분) 다음 각 호의 허가 또는 인가(이하 "허가등"이라 한다)의 절차는 허가등 사항에 대한 사전심사 및 확실한 실행을 위하여 허가등의 이전에 예비적으로 행하는 의사표시(이하 "예비허가등"이라 한다)와 허가등으로 구분한다.

1. 법 제28조제1항의 규정에 의한 전자화폐의 발행 및 관리 업무의 허가
2. 법 제45조에 의한 합병 등의 인가

제44조(예비허가등) ① 예비허가등을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 <별지 제3호 서식>에 따른 관련 신청서 및 첨부서류를 금융위원회에 제출하여야 한다.

② 금융위원회는 예비허가등의 심사를 위하여 필요하다고 인정하는 때에는 예비허가등의 신청에 대하여 이해관계인의 의견을 요청할 수 있고, 금융시장에 중대한 영향을 미칠 우려가 있다고 판단되는 경우 공청회를 개최할 수 있다.

③ 금융위원회는 제2항의 규정에 의하여 접수된 의견 중 신청인에게 불리한 의견에 대하여는 신청인에게 소명하도록 기한을 정하여 통보할 수 있다.

④ 금융감독원장은 예비허가등의 신청내용에 대한 진위여부를 확인하고 이해관계인, 일반인 및 관계기관 등으로부터 제시된 의견을 감안하여 신청내용이 관련 법령과 이 장 제2절에서 규정하는 허가등 세부기준에 부합되는지 여부를 심사하여야 한다.

⑤ 금융감독원장은 사업계획의 타당성을 평가하기 위하여 평가위원회를 구성·운영할 수 있으며 신청내용의 확인, 발기인 및 경영진과의 면담 등을 위하여 실지조사를 실시할 수 있다.

⑥ 금융위원회는 예비허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준을 감안하여 예비허가등의 여부를 결정한다.

⑦ 금융위원회는 예비허가등 시에 조건을 붙일 수 있으며 예비허가등을 거부하는 경우 이를 서면으로 신청인에게 통보하여야 한다.

⑧ 금융위원회는 합병, 영업양도 등 구조조정 및 이용자보호 등을 위하여 신속한 처리가 필요하거나 예비허가등의 신청 시 허가등의 요건을 갖추었다고 판단되는 때에는 예비허가등의 절차를 생략할 수 있다.

제45조(허가등) ① 신청인은 예비허가등의 내용 및 조건을 이행한 후 금융감독원장이 정하는 바에 따라 <별지 제4호 서식>에 따른 관련 신청서 및 첨부서류를 금융

위원회에 제출하여야 한다.
② 금융위원회는 허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준에 따라 심사하여 허가여부를 결정한다.
③ 허가등에는 조건을 붙일 수 있으며 허가를 거부하는 경우에는 이를 서면으로 신청인에게 통보하여야 한다.
④ 금융위원회는 예비허가등의 내용 및 조건의 이행여부를 확인하기 위하여 실지조사를 실시할 수 있으며, 신청인은 이에 적극 협조하여야 한다.
⑤ 신청인은 예비허가등 또는 허가등 시에 부과된 조건이 있는 경우 그 이행상황을 이행기일 경과 후 지체 없이 금융위원회에 보고하여야 한다.

제46조(보완서류 등의 제출) 금융위원회는 예비허가등 또는 허가등의 심사 시 보완서류 등의 추가자료가 필요한 경우 신청인에게 기한을 정하여 그 자료의 제출을 요구할 수 있다.

제47조(허가등 사실의 공고) 금융위원회는 허가등의 신청을 승인한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

제48조(등록) ① 법 제28조 및 제29조에 따라 등록을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 <별지 제5호 서식>에 따른 등록신청서를 금융감독원에 제출하여야 하며 금융감독원장은 등록신청일로부터 20일 이내에 서면으로 등록여부를 통지한다. 다만, 제3항의 실지조사에 걸린 기간은 통지기간에 산입하지 아니한다.
② 금융감독원장은 신청인의 등록 신청에 대하여 이 장 제2절의 심사기준에 따라 등록 여부를 결정한다.
③ 금융감독원장은 등록의 내용 및 조건의 이행여부를 확인하기 위한 실지조사를 실시할 수 있다.
④ 금융감독원장은 등록 신청을 수리한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

제49조(기재가 생략되는 출자자의 범위) 시행령 제20조제1항제3호에서 "금융위원회가 정하여 고시하는 소액출자자"라 함은 허가 또는 등록대상 전자금융업자가 되고자 하는 법인의 의결권 있는 발행주식총수의 100분의 1 이하의 주식을 소유하는 자를 말한다.

제2절 허가 및 등록의 세부요건

제50조(인력 및 물적 시설 세부요건) ① 법 제28조 및 제29조에 따라 허가를 받거나 등록을 하고자 하는 자는 인력과 물적 시설에 대한 다음 각 호의 요건을 모두 갖추어야 한다.
1. 신청 당시 전산업무 종사 경력이 2년 이상인 임직원을 5명 이상 확보하고 있거나 허가·등록 시점에 확보 가능할 것
2. 전자금융업을 원활히 영위하는데 필요한 전산기기를 갖출 것
3. 전산장애 발생 시 전산자료 손실에 대비한 백업(backup)장치를 구비할 것
4. 전자금융업의 원활한 영위를 위한 각종 프로그램을 갖출 것
5. 전산자료 보호 등을 위한 적절한 정보처리시스템 관리방안을 확보하고 정보보호시스템 등 감시운영체제를 구축할 것
6. 전산실 등의 구조 및 내장, 설비 등의 안전성을 확보하고 적절한 보안대책을 수립할 것

② 국외에서 주로 영업하는 국외 사이버몰("국외 사이버몰"이란 컴퓨터 등과 정보통신설비를 이용하여 재화 등을 거래할 수 있도록 설정된 가상의 영업장으로서 운용자의 사무소가 국외에 있는 경우를 말한다. 이하 같다)에서의 상거래에 수반한 전자지급결제대행업을 영위할 목적으로 전자금융업을 등록하고자 하는 자는 제50조제1항의 규정에도 불구하고 다음 각 호의 요건을 모두 충족한 경우 등록할 수 있다.
1. 국외에 소재한 계열사(「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제2조제3항의 "계열사"를 말한다. 이하 같다)와 이용계약을 체결하였고, 계열사의 인력 및 물적 시설이 제50조제1항 각 호의 세부요건을 충족할 것
2. 제1호의 규정에도 불구하고 전자금융업을 등록하고자 하는 자는 신청 당시 법령 준수업무와 이용자 민원처리업무를 담당할 3명 이상의 임직원(전산업무 종사 경력이 2년 이상인 임직원 1명을 포함하여야 한다)은 직접 확보하고 있거나 등록시점에 확보 가능할 것
3. 신청 당시 계열사의 인력 또는 물적시설을 통해 5개국 이상의 국가에서 전자지급결제대행업무가 수행되고 있을 것

③ 제2항에 따라 등록을 하려는 자가 계열사의 인력 또는 물적시설의 이용계약을 체결하는 경우에는 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」을 적용한다. 다만, 동 규정의 제7조는 적용하지 아니한다.

제50조의2(국외 사이버몰을 위한 전자지급결제대행업) ① 제50조제2항에 따라 등록하고자 하는 경우 시행령 제20조제2항제8호에 따라 다음 각 호의 서류를 제출하여야 한다.
1. 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제7조제1항 각 호의 서류
2. 등록신청자 및 계열사의 수탁업무 수행 과정에서의 법·시행령 및 이 규정 등 준수에 대한 확약서
3. 신청 시점에 전자지급결제대행업무를 수행하고자 하는 국외 사이버몰에 대한 다음 각 목의 사항(해당 국가의 법령 등에서 이와 유사한 것으로 인정되는 사항을 포함한다)을 기재한 서류
   가. 「전자상거래 등에서의 소비자보호에 관한 법률」 제10조제1항 각 호의 서류
   나. 신청일 직전연도에 사이버몰에서 체결된 전자상거래 중 국내에 소재한 소비자와 사업자 간 거래의 비중

② 제50조제2항에 따라 등록을 한 자는 국외에서 주로 영업하는 국외 사이버몰을 통한 상거래에 대해서만 전자지급결제대행업을 영위하여야 한다.
③ 금융감독원장은 국외에서 주로 영업하는 국외 사이버몰의 판단기준 등 필요한 사항을 정할 수 있다.

제51조(재무건전성 세부기준 및 계산방법 등) ① 시행령 제18조제1항 및 제2항에

따라 금융위원회가 정하는 재무건전성 기준은 다음 각 호와 같다.
1. 시행령 제18조제1항의 규정에 따른 기관 중 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사에 해당하는 기관은 그 기관의 설립·운영 등에 관한 법령상 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 재무기준에 해당하지 아니할 것
2. 제1호 이외의 경우에는 다음 각 목의 요건을 충족할 것
   가. 시행령 제18조제1항의 규정에 따른 금융회사 중 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사에 해당하지 않는 기관은 자기자본 대비 부채총액의 비율이 100분의 200 이내일 것. 다만, 금융회사 업무의 성격 및 재무 구조 등을 감안할 때 부채비율 기준을 적용하지 아니하고, 「금융산업의 구조 개선에 관한 법률」 제2조제1호 각 목 중 어느 하나의 금융회사(이하 "기준 금융회사"라 한다)의 재무건전성 기준을 적용하는 것이 적절하다고 금융위원회가 승인하는 경우에는, 기준 금융회사의 설립, 운영 등에 관한 법령에 따라 산출한 재무 비율이 같은 법령상의 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 기준에 해당하지 아니할 것
   나. 법 제28조제1항에 따른 허가대상 전자금융업일 경우에는 자기자본 대비 부채총액의 비율이 100분의 180 이내일 것
   다. 법 제28조제2항 및 제29조에 따른 등록대상 전자금융업일 경우에는 자기자본·출자총액 또는 기본재산 대비 부채총액의 비율이 100분의 200 이내일 것

② 제1항제2호의 부채비율은 신청일이 속하는 사업연도의 직전 사업연도말 대차대조표(최근 대차대조표를 사용하고자 하는 경우에는 신청일 최근 분기말 대차대조표 또는 회계법인의 확인을 받은 신청일 최근 월말 대차대조표) 상의 자기자본 및 부채총액을 이용하여 산출한다. 이 경우 전자화폐·선불전자지급수단의 미상환잔액 및 전자자금이체·전자지급결제대행·결제대금예치·전자고지결제·「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스 등의 업무를 영위하는 자가 이용자와의 거래 관계에서 일시 보관하는 금액(이하 "미정산 잔액"이라 한다)은 부채총액에서 차감한다.

③ 제1항에도 불구하고 다음 각 호의 요건을 갖춘 신청인의 재무건전성 기준은 자기자본 대비 부채총액의 비율이 100분의 1500 이내일 것으로 한다.
1. 정부등이 자본금·출자총액 또는 기본재산의 100분의 10 이상을 소유하고 있거나 출자하고 있을 것
2. 신청인의 사업 수행이 곤란하게 되는 경우 정부등이 해당 사업을 인수할 것을 확약하는 등 그 사업의 연속성에 대하여 정부등이 보장하고 있을 것
3. 사업 개시 후 5년 이내 제1항의 재무건전성 기준을 충족하는 것을 내용으로 하는 실현가능한 재무구조개선계획을 수립하여 관련서류와 함께 제출할 것

제52조(사업계획에 관한 요건) 법 제28조에 따라 허가를 받고자 하는 자의 사업계획은 다음 각 호의 요건을 모두 갖추어야 한다.
1. 영업개시 후 3년간 추정재무제표 및 수익전망이 전자화폐 내지 선불전자지급수단 발행업계의 과거 수익상황 등에 비추어 타당성이 있고 그 내용이 해당 신청회사의 영업계획에 부합할 것
2. 전자화폐 발행업을 원활히 영위하는데 필요한 이용자 확보계획이 구체적이고 타당하며 실현가능성이 있을 것
3. 영위하고자 하는 영업의 내용이 법령에 위반되지 아니하고 투자자보호나 건전한 금융질서를 저해할 우려가 없을 것

제53조(주요출자자에 관한 요건) 주요출자자(시행령 제18조제3항에 따른 주요출자자를 말한다)는 <별표 4>에서 정한 요건을 충족하여야 한다.

제54조(허가 및 등록신청 결격자) 법 제32조제4호의 규정에서 "금융위원회가 정하는 자"라 함은「신용정보의 이용 및 보호에 관한 법률」제25조 제2항 제1호의 종합신용정보집중기관에 다음 각호 중 어느하나의 신용정보가 등록된 자를 말한다.
1. 어음·수표 거래정지처분 또는 부도거래정보
2. 대출금 등의 용도 외 유용 사실
3. 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실

제55조(신청에 따른 등록말소 및 이용자 보호조치) ① 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 <별지 제6호 서식>에 따른 등록말소신청서를 금융위원회에 제출하여야 한다.

② 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 신청 이전에 이용자 보호조치 계획을 금융위원회에 제출하여야 한다.

③ 금융위원회는 제1항의 전자금융업자가 제출한 계획이 이용자 보호에 충분하지 않은 경우에 그 보완을 요구할 수 있다.

제3절 전자금융업의 업무

제56조(전자화폐 발행업자의 겸업가능 업무) 시행령 제22조제1항제3호에서 "금융위원회가 정하여 고시하는 업무"란 다음 각 호의 어느 하나에 해당하는 업무를 말한다.
1. 전자화폐 발행 및 관리를 위한 가맹점의 모집
2. 전자화폐 발행 및 관리를 위한 인터넷 홈페이지의 운영 및 이를 통한 통신판매 중개

제57조(수수료 및 준수사항 등의 고지방법) 법 제38조제3항 각 호의 사항은 다음 각 호의 방법 중 제1호의 방법을 포함한 둘 이상의 방법으로 가맹점에게 알려야 한다.
1. 가맹점에의 개별 통보
2. 전국적으로 보급되는 일간신문에의 공고
3. 해당 금융회사 또는 전자금융업자 영업장 및 인터넷 홈페이지에의 게시

제5장 전자금융업무의 감독

제58조(금융회사의 정보기술부문 실태평가 등) ① 금융감독원장은 금융회사의 정보기술부문의 건전성 여부를 감독하여야 한다.

② 금융감독원장은 업무의 성격 및 규모, 정보기술부문에 대한 의존도 등을 감안하여 <별표 5>에 규정된 금융회사(이하 이 조에서 '은행등'이라 한다)에 대하여 검사를 통해 정보기술부문 운영 실태를 평가하고 그 결과를 경영실태평가 등 감독 및 검사업무에 반영하여야 한다.

③ 제2항에 의한 실태평가는 1등급(우수), 2등급(양호), 3등급(보통), 4등급(취

약), 5등급(위험)의 5단계 등급으로 구분한다.
④ 금융감독원장은 제2항에 따른 정보기술부문 실태평가 결과 종합등급이 4등급인 경우에는 해당 은행등에게 이의 개선을 위한 확약서 제출을 요구할 수 있으며, 종합등급이 5등급이거나 직전 정보기술부문 실태평가 결과에 비해 평가등급이 2등급 이상 하향된 경우에는 취약점 개선대책의 수립·이행을 내용으로 하는 양해각서를 체결할 수 있다.
⑤ 제4항의 확약서는 대표자의 승인을 받아 제출하고, 양해각서는 해당 은행등의 이사회 재적이사 전원의 서명을 받아 체결한다.
⑥ 금융감독원장은 확약서 또는 양해각서의 이행상황을 점검하여 그 이행이 미흡하다고 판단되는 경우에는 확약서를 다시 제출받거나 양해각서를 다시 체결할 수 있다.
⑦ 확약서 또는 양해각서의 효력발생일자, 이행시한 및 이행상황 점검주기는 각 확약서 또는 양해각서에서 정한다. 다만, 이행상황 점검주기를 따로 정하지 않은 경우 은행등은 매분기 익월말까지 분기별 이행상황을 금융감독원장에게 보고하여야 한다.
⑧ 제2항에 따른 정보기술부문 실태평가 결과는 경영실태평가 세부 평가항목 중 경영관리 또는 위험관리 항목의 평가비중에서 최소 100분의 20 이상 반영되어야 하며, 금융감독원장은 정보기술부문 실태평가 결과가 4등급 이하인 은행등에 대해 경영실태평가 2등급 이상으로 평가할 수 없다.
⑨ 제2항에 의한 정보기술부문의 실태평가를 위한 세부 사항은 금융감독원장이 정한다.

제59조(검사결과의 보고방법) 금융감독원장은 법 제39조제5항에 따른 결과보고를 하는 경우 「금융기관 검사 및 제재에 관한 규정」 제3장부터 제4장을 준용한다.

제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.
1. 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영
2. 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지
3. 계좌번호, 비밀번호 등 이용자 금융정보 무단보관 및 유출 금지
4. 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립
5. 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용
6. 정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립
7. 외부주문등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것
8. 업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립
9. 정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립·운용하고, 통제는 제8조제1항제2호의 조직에서 수행
10. 전자금융보조업자에 대한 재무건전성을 연1회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시
11. 전자금융보조업자가 제공하는 서비스의 품질수준을 연1회 이상 평가할 것
12. 전자금융보조업자가 사전 동의 없이 다시 외부주문등 계약을 체결하거나 계약업체를 변경하지 못하도록 하고, 사전 동의시 해당 계약서에 제7호의 사항을 기재하도록 통제
13. 업무수행인력에 대하여 사전 신원조회 실시(이 경우 신원보증보험 증권 징구로 갈음할 수 있다) 또는 대표자의 신원보증서 징구, 인력변경시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안 수립
14. 외부주문등은 자체 보안성검토 및 정기(금융감독원장이 정하는 중요 점검사항에 대해서는 매일) 보안점검 실시
② 금융회사 또는 전자금융업자는 제1항제10호 및 제11호의 평가결과를 금융감독원장에게 보고하여야 한다.
③ 금융감독원장은 제2항의 규정에 따른 평가결과 보고를 접수하고, 그 평가실시 여부를 제58조제2항의 규정에 따른 정보기술부문 실태평가에 반영할 수 있다.
④ 법 제40조제6항 단서에서 "금융위원회가 인정하는 경우"란 전자금융거래정보의 보호와 관련된 전산장비·소프트웨어에 대한 개발·운영 및 유지관리 업무를 재위탁하는 경우로서 다음 각 호의 사항을 준수하는 경우를 말한다.
1. 재수탁업자가 재위탁된 업무를 처리함에 있어 금융거래 정보의 변경이 필요한 경우에는 위탁회사 또는 원수탁업자의 개별적 지시에 따라야 하며, 위탁회사 또는 원수탁업자는 변경된 정보가 지시 내용에 부합하는지 여부를 확인하여야 함
2. 위탁업무와 관련된 이용자의 금융거래정보는 위탁회사의 전산실 내에 두어야 함. 다만, 재수탁업자가 이용자의 이용자 정보를 어떠한 경우에도 알지 못하도록 위탁회사 또는 원수탁업자가 금융거래정보를 처리하여 제공한 경우에는 위탁회사의 관리·통제 하에 재수탁회사 등 제3의 장소로 이전 가능함
⑤ 금융회사 또는 전자금융업자는 제14조의2제1항제2호에 따른 평가를 위하여 제37조의4제1항 각 호의 어느 하나에 해당하는 기관에 지원을 요청할 수 있다.

제61조(전자금융보조업자 자료제출 기준) ① 금융감독원장은 전자금융보조업자에 대해 외부주문등과 관련한 계약서, 계약서 부속자료 및 그 밖의 전자금융업무와 관련한 자료 등을 직접 요구할 수 있다.
② 제1항에 따른 자료제출 요구시 전자금융보조업자는 특별한 이유가 없는 한 자료제출에 응하여야 한다.

제62조(업무보고서의 제출) ① 법 제42조에 따라 금융회사 및 전자금융업자는 금융감독원장이 정하는 바에 따라 업무보고서를 금융감독원장에게 제출하여야 한다. 다만, 법 제2조제1호에 따른 전자금융업무를 하지 아니하는 금융회사는 그러하지 아니하다.
② 제1항에 따른 업무보고서 제출은 정보통신망(「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 제2조의 규정에 의한 정보통신망을 말한다)을 이용한 전자문서의 방법에 의할 수 있다.
③ 제1항의 업무보고서 제출에 관한 세부적인 절차, 양식 등에 관해서는 금융감독원장이 별도로 정한다.

제63조(전자금융업자 경영지도기준) ① 법 제42조제2항에 따른 구체적인 경영지도기준은 다음과 같다.
1. 법 제30조 및 시행령 제17조에 따른 허가나 등록요건 상 최소자본금·출자총액 또는 기본재산 기준을 항상 충족할 것
2. 총자산에서 총부채를 감한 자기자본이 항상 0을 초과할 것
3. 미상환잔액 대비 자기자본 비율은 100분의 20 이상일 것(전자화폐 및 선불전자지급수단 발행자에 한한다)
4. 총자산 대비 투자위험성이 낮은 자산의 비율은 100분의 10 이상으로 유지하거나 미정산 잔액 대비 투자위험성이 낮은 자산의 비율을 100분의 100 이상으로 유지할 것. 단, 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 및 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자는 제외한다. 이 때 투자위험성이 낮은 자산은 <별표 6>와 같다.
5. 유동성 비율은 다음 각 목과 같이 유지할 것
   가. 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 : 100분의 60 이상
   나. 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자 : 100분의 50 이상
   다. 그 밖의 등록대상 전자금융업자 : 100분의 40 이상

② 제1항에서 정하는 비율의 구체적 산정기준은 금융감독원장이 정한다.
③ 금융감독원장은 제1항의 경영지도비율이 악화될 우려가 있거나 경영상 취약부문이 있다고 판단되는 전자금융업자에 대하여 이의 개선을 위한 계획 또는 약정서를 제출토록 하거나 해당 전자금융업자와 경영개선협약을 체결할 수 있다. 다만, 제64조 부터 제66조까지의 규정에 의한 경영개선권고, 경영개선요구 또는 경영개선명령을 받고 있는 전자금융업자의 경우에는 그러하지 아니하다.

제64조(경영개선권고) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 권고하여야 한다.
1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 20 미만인 경우
2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.
1. 인력 및 조직운영의 개선
2. 경비절감
3. 고정자산투자, 신규업무영역에의 진출 및 신규출자의 제한
4. 부실자산의 처분
5. 자본금의 증액 또는 감액
6. 이익배당의 제한
7. 특별대손충당금의 설정

③ 금융위원회는 제1항에 의한 권고를 하는 경우 해당 전자금융업자 및 관련 임원에 대하여 주의 또는 경고조치를 취할 수 있다.

제65조(경영개선요구) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 요구하여야 한다.
1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 10 미만인 경우
2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우
3. 제64조제1항의 규정에 의해 경영개선권고를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.
1. 조직의 축소
2. 위험자산의 보유제한 및 처분
3. 자회사의 정리
4. 임원진 교체 요구
5. 영업의 일부정지
6. 합병, 제3자 인수, 영업의 전부 또는 일부 양도계획의 수립
7. 제64조제2항에서 정하는 사항

제66조(경영개선명령) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당하는 경우에는 해당 전자금융업자에 대해 필요한 조치를 이행하도록 명령하여야 한다.
1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 5 미만인 경우
2. 제65조제1항의 규정에 의해 경영개선요구를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하거나 이행이 곤란하여 정상적인 경영이 어려울 것으로 인정되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다. 다만, 영업의 전부정지, 영업의 전부양도, 계약의 전부이전 또는 주식의 전부소각의 조치는 제1항제1호의 기준에 미달하고 건전한 전자금융거래질서나 이용자의 권익을 해할 우려가 현저하다고 인정되는 경우에 한한다.
1. 주식의 전부 또는 일부 소각
2. 임원의 직무집행 정지 및 관리인의 선임
3. 6월 이내의 영업의 정지
4. 계약의 전부 또는 일부의 이전
5. 제65조제2항에서 정하는 사항

제67조(이유제시 등) 제64조 부터 제66조의 조치를 하는 경우 금융위원회는 해당 전자금융업자에게 그 근거와 이유를 제시하여야 한다.

제68조(적기시정조치의 유예) 제64조제1항, 제65조제1항 및 제66조제1항 각 호의 어느 하나에 해당하는 전자금융업자가 자본의 확충 또는 자산의 매각 등을 통하여 단기간 내에 그 기준에 해당되지 않을 수 있다고 판단되는 경우 또는 이에 준하는 사유가 있다고 인정되는 경우에는 금융위원회는 일정기간동안 조치를 유예할 수

있다.

제69조(경영개선계획 제출 및 평가 등) ① 제64조 부터 제66조에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자는 동 조치를 받은 후 2월의 범위 내에서 금융위원회가 정하는 기한 내에 해당 조치의 내용이 반영된 계획(이하 "경영개선계획"이라 한다)을 금융감독원장에게 제출하여야 한다.
② 금융위원회는 제64조 부터 제66조에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자가 제1항에 의해 제출한 계획에 대하여 1월 이내에 승인여부를 결정하여야 한다. 다만, 제3항의 규정에 의한 경영평가위원회의 심의가 지연되는 경우에는 15일 이내에서 그 기한을 초과할 수 있다.
③ 금융감독원장은 제2항의 금융위원회의 승인여부 결정 이전에 해당 계획에 대하여 외부 전문가로 구성된 경영평가위원회의 심의를 거치도록 하여야 한다. 다만, 긴급을 요하거나 심의의 실익이 크지 아니하다고 금융감독원장이 인정하는 경우에는 그러하지 아니하다.
④ 제3항에 의해 경영평가위원회가 사전심의를 하는 경우에는 해당 전자금융업자를 출석시켜 의견을 청취할 수 있다.
⑤ 금융위원회는 제64조에 의해 경영개선권고를 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인하고, 제65조제2항 각 호의 일부 또는 전부에 해당하는 조치를 요구하며, 동 조치내용이 반영된 계획을 일정기간 내에 제출하도록 하여 승인여부를 결정한다.
⑥ 금융위원회는 제5항의 규정에 의해 제출한 계획 또는 제65조에 의해 경영개선요구를 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인한다. 이 경우 금융위원회는 제65조제2항 각 호의 일부 또는 전부에 해당하는 조치를 요구하고, 동 조치내용이 반영된 계획을 일정기간 내에 제출토록 하여야 하며 동 계획의 타당성이 인정되지 않을 경우에는 제66조제2항에서 규정한 조치의 일부 또는 전부를 이행하도록 명령하여야 한다.
⑦ 금융위원회는 제6항의 규정에 의해 제출된 계획 또는 제66조에 의해 경영개선명령을 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인한다. 이 경우 금융위원회는 제71조 각 호의 일부 또는 전부에 해당하는 조치를 할 수 있다.
⑧ 제2항의 규정에 따라 경영개선계획을 승인받은 전자금융업자는 매분기말 익월 10일까지 동 계획의 분기별 이행실적을 금융감독원장에게 제출하여야 하며, 금융감독원장은 그 이행실적이 미흡하거나 관련제도의 변경 등 여건변화로 인하여 이행이 곤란하다고 판단되는 경우에는 경영개선계획의 수정요구, 일정기간 내 이행촉구 등 필요한 조치를 취할 수 있다.
⑨ 제8항의 규정에 따라 금융감독원장이 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자의 경영개선계획의 주요사항을 수정 요구하거나 일정기간 내 이를 이행토록 촉구하는 경우에는 그 내용을 금융위원회에 사전 보고하여야 한다.
⑩ 제8항의 규정에 따라 전자금융업자가 경영개선계획의 주요사항을 수정하여 제출한 경우에는 제2항부터 제7항을 준용할 수 있다.
⑪ 제3항의 경영평가위원회의 구성 · 운영과 관련된 세부사항은 금융감독원장이 정한다.

제70조(경영개선계획 이행기간 등) ① 제64조에 의하여 경영개선권고를 받은 전자금융업자의 경영개선계획 이행기간은 승인일로부터 6월 이내로 한다.
② 제65조에 의하여 경영개선요구를 받은 전자금융업자의 경영개선계획 이행기간은 승인일로부터 1년 이내로 한다. 이 경우 제64조에 의하여 경영개선권고를 받은 전자금융업자가 경영개선계획 이행 중 경영개선요구를 받은 경우의 이행기간은 경영개선권고에 따른 경영개선계획의 승인일로부터 1년 이내로 한다.
③ 제69조제8항에 의하여 금융감독원장으로부터 경영개선계획의 수정요구 또는 일정기간 내 이행촉구를 받은 경우에는 제1항과 제2항의 기간을 초과할 수 있다. 다만, 그 초과기간은 제1항 또는 제2항에서 정하는 기간 이내이어야 한다.
④ 제66조에 의하여 경영개선명령을 받은 전자금융업자의 경영개선계획의 이행기간은 금융위원회가 정한다.
⑤ 제64조 부터 제66조까지의 규정에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자가 자본 확충 또는 부실채권정리 등 경영개선계획의 주요사항을 조기에 달성하여 경영상태가 현저히 개선된 경우에는 금융위원회는 권고, 요구 또는 명령한 조치의 내용을 완화하거나 그 이행을 면제할 수 있다.
⑥ 제64조 부터 제66조까지의 규정에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자의 경영개선계획 이행기간이 만료되어 경영상태가 충분히 개선되었다고 인정되는 경우에는 금융위원회는 당초의 조치가 종료되었음을 통지하여야 하며, 경영상태가 제64조제1항, 제65조제1항 또는 제66조제1항에 해당하는 경우에는 동 조항에 따라 별도의 경영개선권고, 경영개선요구 또는 경영개선명령을 하여야 한다.

제71조(경영개선계획의 불이행에 따른 조치) 금융위원회는 제66조에 의하여 경영개선명령을 받은 전자금융업자가 제70조에 의한 이행기한 내에 경영개선계획의 주요사항을 이행하지 아니하여 경영정상화가 이루어지지 아니하였다고 판단되는 경우 해당 전자금융업자에 대하여 다음 각 호의 일부 또는 전부에 해당하는 조치를 할 수 있다.
1. 제66조제2항에서 정한 조치
2. 허가의 취소
3. 임원의 해임 권고
4. 그 밖에 이용자 보호를 위하여 필요한 조치

제72조(과징금 수납기관 및 납부서식 등) ① 시행령 제27조제1항의 규정에 의하여 금융위원회가 과징금의 납부를 통지하는 경우에는 <별지 제2호 서식>에 따른다.
② 시행령 제27조제2항에 따른 수납기관은 은행법에 의한 금융회사와 우체국으로 한다.

제72조의2(과징금 과오납에 따른 환급가산금 이율) 금융위원장은 「은행법」제8조에 따라 은행업 인가를 받은 국내은행의 1년 만기 정기예금 이자율을 감안하여 환급가산금 이자율을 정하여야 한다.

제6장 보칙

제73조(정보기술부문 및 전자금융 사고보고) ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고

하여야 한다.
1. 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연된 경우
2. 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우
3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우
4. 법 제9조제1항의 규정에서 정하는 사고

② 금융회사 및 전자금융업자는 제1항에 따른 사고보고를 고의로 지연하거나 숨긴 자에 대하여 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다.

③ 금융감독원장은 제1항에 따라 보고 받은 내용을 지체 없이 금융위원장에게 보고하여야 하며, 제1항제3호에 따른 사고 발생시에는 제37조의4제1항 각 호에 따른 침해사고대응기관에도 알려야 한다.

④ 제1항의 사고보고와 관련하여 사고보고 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.

제74조(위탁업무의 처리 결과 보고) 금융감독원장은 시행령 제30조의 규정에 따라 금융위원회로부터 위탁받은 업무의 처리 결과를 매분기 금융위원회에 보고하여야 한다.

제75조(규제의 존속기한 및 재검토) 제75조(규제의 존속기한 및 재검토) ① 금융위원회는 행정규제기본법 제8조·제19조의2 및 훈령·예규 등의 발령 및 관리에 관한 규정(대통령훈령 제248호)에 따라 이 고시에 대하여 2019년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

② 제8조제2항은 2020년 1월 1일까지 효력을 가진다.

부칙

제1조(시행일) 이 규정은 2019년 1월 1일부터 시행한다.

제2조(클라우드컴퓨팅서비스 이용절차 등에 관한 적용례) 제14조의2의 개정규정은 이 규정 시행 이후 클라우드컴퓨팅서비스를 이용하고자 하는 금융회사 또는 전자금융업자부터 적용한다.

[별표 2의2]

금융분야 클라우드컴퓨팅서비스 제공기준(제14조의2 관련)

금융회사 또는 전자금융업자는 아래의 항목을 포함하여 클라우드서비스 제공자의 건전성 및 안전성을 평가하되, 클라우드서비스 제공자가 국내·외의 클라우드서비스 관련 보안인증 등을 취득하여 유지 중임을 확인한 경우 제1호의 기본 보호조치에 관한 평가는 생략할 수 있다.

1. 기본 보호조치

가. 관리적 보호조치
- ㅇ 정보보호 정책 및 법규 준수 등에 관한 사항
- ㅇ 인적보안에 관한 사항
- ㅇ 위험평가 및 관리에 관한 사항
- ㅇ 서비스 공급망 관리에 관한 사항
- ㅇ 업무연속성 계획 및 재해복구에 관한 사항
- ㅇ 침해사고 대응 및 관리에 관한 사항

나. 기술적 보호조치
- ㅇ 사용자 인증 및 접근통제에 관한 사항
- ㅇ 가상화 및 인프라 보안에 관한 사항
- ㅇ 개발 및 운영보안에 관한 사항
- ㅇ 암호화 및 데이터 보호에 관한 사항

다. 물리적 보호조치
- ㅇ 물리적 보안에 관한 사항

2. 금융부문 추가 보호조치

가. 클라우드 서비스 제공자의 건전성에 관한 사항

나. 금융회사 및 전자금융업자가 다음의 의무를 준수하기 위하여 클라우드서비스 제공자의 지원 및 협조가 필수적인 사항
- ㅇ 이 규정 제3장(전자금융거래의 안전성 확보 및 이용자 보호에 관한 사항)에 관한 사항
- ㅇ 이 규정 제60조(외부주문등에 대한 기준), 제61조(전자금융보조업자 자료제출 기준) 및 제73조(정보기술부문 및 전자금융사고보고)에 관한 사항

다. 개인(신용)정보 관련 규제 준수에 관한 사항

라. 기타 금융관련 법령 준수에 관한 사항

[별표 2의3]

업무위탁 운영기준 보완사항(제14조의2 관련)

금융회사 및 전자금융업자가 클라우드컴퓨팅서비스 제공자에게 규정 제14조의2 제3항 각호에 해당하는 정보처리 업무의 위탁을 추진하는 경우 「자본시장과 금융투자업에 관한 법률」 제42조제7항에 따른 업무위탁 운영기준 또는 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따른 자체 업무위수탁 운영기준에 다음 각 호의 사항을 반영하고 이를 준수하여야 한다.

1. 위수탁계약의 결정 · 해지 절차 및 재위탁에 관한 사항
- 위탁업무에 대한 자체 중요도 평가 실시에 관한 사항
- 재위탁 및 재위탁의 변경 시 동의에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항 통보에 관한 사항

2. 위탁업무의 모니터링에 관한 사항
- 정보처리의 물리적 위치에 관한 사항
- 클라우드서비스 제공자의 보안관리 수준 등에 관한 사항
- 유 · 무형의 위탁업무 처리에 관한 최신 정보 등록 · 관리, 위탁업무의 품질 또는 서비스수준 등에 관한 사항

3. 비상대책 등에 관한 사항
- 합병·분할, 계약상 지위의 양도, 재위탁 등 중요 상황 발생시 대책(업무 연속성 계획 포함)에 관한 사항
- 위탁업무를 다른 수탁자 또는 클라우드컴퓨팅 업무를 위탁한 금융회사 및 전자금융업자에 이전시키는 경우 업무 장애 · 서비스지연, 이전을 지원할 의무 등 전환계획에 관한 사항
- 위탁계약의 종료, 중단, 변경 시 데이터 반환·파기에 관한 사항

4. 위탁업무 관련 조사 · 접근권 확보에 관한 사항
- 감독당국 또는 내외부 감사인의 조사 · 접근권(현장방문 포함) 확보에 관한 사항

5. 위수탁 계약서 주요 기재사항
- 클라우드컴퓨팅서비스가 제공되는 물리적 위치
- 재위탁 또는 재위탁의 변경 등 금융회사 또는 전자금융업자의 동의가 필요한 사항
- 위탁하는 업무, 데이터에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 등 금융회사 또는 전자금융업자에 대한 통보가 필요한 사항
- 감독당국 또는 내외부 감사인의 조사 · 접근(현장방문 포함) 수용 의무
- 계약의 파기 또는 종료, 기타 위탁업무의 원활한 이행이 어려운 경우 해당 위탁업무의 이전 및 반환 등에 관한 사항
- 위탁 및 위탁업무 관련 준거법 준수의무 및 자율규제에 대한 협조
- 비상대응훈련(재해복구전환훈련 포함), 취약점 분석 · 평가, 침해사고대응훈련 등의 협조에 관한 사항
- 위탁업무 모니터링 지원에 관한 사항
- 전송 정보에 대한 정보보호 의무 및 서비스 연속성 보장 등의 보안 요구사항
- 재위탁 관련 클라우드서비스 제공자의 관리 · 감독 의무에 관한 사항
- 재위탁 또는 재위탁 변경에 따른 보안리스크 증가 등 서비스에 악영향을 미칠 수 있는 경우 원위탁자의 계약해지 권한 보유에 관한 사항

금융기관의 업무위탁 등에 관한 규정

제1조(목적) 이 규정은 금융기관이 「금융위원회의 설치 등에 관한 법률」 제17조제3호에 따라 인가·허가 또는 등록 등(이하 "인가등"이라 한다)의 업무를 수행함에 있어 그 업무의 위탁 등에 관한 사항을 정함을 목적으로 한다.

제2조(정의) ① 이 규정에서 "금융기관"이라 함은 다음 각 호와 같다. <개정 2017. 11. 14.>

1. 「은행법」에 의해 설립된 금융기관
2. 「농업협동조합법」에 의한 농협은행, 농협손해보험, 농협생명보험
3. 「수산업협동조합법」에 의한 수협은행
4. 「중소기업은행법」에 의한 중소기업은행
5. <삭제 2017. 11. 14.>
6. <삭제 2017. 11. 14.>
7. 「상호저축은행법」에 의한 상호저축은행 및 그 중앙회
8. <삭제 2017. 11. 14.>
9. 「여신전문금융업법」에 의한 여신전문금융회사
10. 「보험업법」에 의한 보험회사
11. <삭제 2017. 11. 14.>
12. <삭제 2017. 11. 14.>
13. 「신용협동조합법」에 의한 신용협동조합 및 그 중앙회, 같은 법 제95조의 규정에 의한 각 조합 및 그 중앙회의 상호금융부문
14. 「한국산업은행법」에 의한 한국산업은행
15. 기타 금융업 또는 금융관련업무를 영위하는 자로서 금융감독원장(이하 "감독원장"이라 한다)이 정하는 자

② 이 규정에서 "업무위탁"이라 함은 금융기관이 인가등을 받은 금융업을 영위하기 위하여 제3자(개인을 포함한다)의 용역 또는 시설 등을 계속적으로 활용하는 행위를 말한다. 다만, 후선업무와 관련한 단순 집행업무 등 금융업 영위와 직접적으로 관계되지 아니하는 위탁계약은 제외한다.

③ 제2항의 "후선업무와 관련한 단순 집행업무"의 범위는 <별표 1>과 같다.

④ 이 규정에서 "업무수탁"이라 함은 금융기관이 제3자가 영위하는 업무를 위탁받아 계속적으로 처리하는 행위를 말한다.

⑤ 제2항 및 제3항의 규정에 불구하고 외국 금융기관 국내지점의 국내외 본지점간의 용역 또는 시설 등의 공급계약은 이 규정에 의한 업무위탁 또는 수탁으로 간주한다.

⑥ 이 규정에서 "금융관련법령"이란 「금융회사의 지배구조에 관한 법률」 제2조제7호에 따른 "금융관계법령"을 말한다.

제3조(업무위탁 등) ① 금융기관은 인가등을 받은 업무를 영위함에 있어 제3자에게 업무를 위탁하거나 제3자의 업무를 수탁할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 사항은 그러하지 아니하다.

1. 인가 등을 받은 금융업 또는 다른 금융업의 본질적 요소를 포함하는 업무를 위탁하는 경우. 다만, 다음 각 목의 어느 하나에 해당하는 업무의 경우에는 위탁할 수 있다.
   가. 위탁하고자 하는 업무가 해당 금융업의 본질적 요소가 아니라 다른 금융업의 본질적 요소인 경우로서 법령에서 해당 업무수행을 허용하고 있는 자에 대하여 위탁하는 경우
   나. 인가등을 받은 업무를 효율적으로 수행하는 데 필요한 경우로서 해당 업무를 위탁하더라도 금융기관의 건전성 또는 신인도를 저해하거나 금융질서의 문란 또는 금융이용자 피해를 발생시킬 우려가 낮은 것으로 금융위원회가 인정하는 경우
2. 관련 법령에서 금융기관이 수행하도록 의무를 부여하고 있는 경우
3. 업무의 위탁 또는 수탁으로 인하여 당해 금융기관의 건전성 또는 신인도를 크게 저해하거나 금융질서의 문란 또는 금융이용자의 피해 발생이 심히 우려되는 경우

② 제1항 제1호의 본질적 요소에 해당하는 사항은 <별표 2>과 같다.

1. <본호 삭제 2005. 7. 27>
2. <본호 삭제 2005. 7. 27>
3. <본호 삭제 2005. 7. 27>
4. <본호 삭제 2005. 7. 27>

③ 금융기관이 제1항의 규정에 따라 제3자에게 업무를 위탁하거나 제3자로부터 업무를 수탁하는 경우에는 다음 각 호의 사항을 고려하여 동 업무가 적정하게 처리될 수 있도록 하여야 한다.

1. 업무위탁 또는 수탁에 따른 비용·편익분석
2. 금융이용자 피해발생 및 금융질서 문란 여부
3. 제3자가 관련 법규(다만, 제3자가 외국인인 경우에는 국제사법 제3조)에 따라 업무수탁이 가능한지의 여부
4. 제3자가 수탁업무를 적절히 수행할 수 있는지의 여부
5. 「금융실명거래 및 비밀보장에 관한 법률」 등 관련 법령에의 저촉 여부

④ 제1항에 따라 금융기관의 업무를 위탁받은 자는 위탁자의 동의를 얻어 위탁받은 업무를 제3자에게 재위탁할 수 있다. 이 경우 제2조, 본조 제1항·제2항·제3항, 제4조, 제5조, 제6조를 준용하되, 재위탁시 보고의 주체는 원위탁 금융회사로 한다.

⑤ 제1항에 따라 업무를 위탁하는 경우(제4항에 따라 재위탁하는 경우를 포함한다) 위탁회사는 수탁회사가 이 규정 등 금융관련법령 및 제3조의2에 따른 업무위수탁기준상의 의무를 위반하여 발생하는 손해에 대해서 수탁회사와 연대하여 배상책임을 진다.

제3조의2(업무위수탁기준) 금융기관은 제3조에서 정한 업무위탁 등에 따른 리스크의 체계적 관리를 위하여 <별표 3>에서 정하는 업무위수탁기준에 따라 금융권역 및 위탁대상자의 특성 등을 감안하여 자체 업무위수탁 운영기준을 마련하고 이를 준수하여야 한다.

제3조의3(혁신적 금융서비스에 관한 특례) ① 금융기관은 혁신적 금융서비스의 도입을 위하여 금융위원회가 지정하는 제3자(이하 "지정대리인"이라 한다)에 대해서는 제3조제1항제1호에도 불구하고 혁신적 금융서비스의 시범 운영을 위해 필요한 범위 내에서 위탁의 범위를 별도로 정하여 위탁할 수 있다. 이 경우 업무를 위탁할 수 있는 기간은 2년 이내로 한다.

② 금융위원회는 제1항의 지정대리인을 지정할 때 다음 각 호의 요소를 고려하여야 한다.

1. 지정대리인이 되고자 하는 자가 국내 금융시장 내에서 주된 활동을 하는 것을 목표로 하고 있는지 여부
2. 공급하려는 새로운 금융서비스가 기존에 공급되고 있는 금융서비스와 비교할 때 충분한 혁신성을 지니는지 여부
3. 공급하려는 새로운 금융서비스가 국내 금융소비자에게 직간접적인 혜택을 제공하는지 여부
4. 공급하려는 새로운 금융서비스를 업무위탁 이외의 방법으로 수행하는 것이 가능한지 여부
5. 지정대리인이 되고자 하는 자가 업무위탁을 받아 혁신적 금융서비스를 시범 운영할 수 있는 준비가 되어 있는지 여부

제4조(보고) ① 금융기관이 제3조제1항의 규정에 따라 제3자와 업무위탁 계약을 체결하거나 제3자(금융기관 및「자본시장과 금융투자업에 관한 법률」에 따른 금융투자업자, 종합금융회사는 제외한다)와 업무수탁계약을 체결하고자 하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은 업무를 실제로 수행하려는 날의 7영업일 이전에 <별지 제1호 서식>에 따라 다음 각호의 서류를 첨부하여 감독원장에게 보고하여야 한다.

1. 위탁 또는 수탁 관련 계약서(안) 사본
2. 업무위수탁계약이 제3조제3항 각 호의 고려사항에 저촉되지 아니하고 제3조의2에 따른 자체 업무위수탁 운영기준에 위배되지 아니하다는 준법감시인(준법감시인이 없는 경우에는 감사 등 이에 준하는 자를 말한다)의 검토의견 및 관련 자료 사본
3. 위탁 또는 수탁의 필요성 및 기대효과
4. 위탁 또는 수탁에 따른 업무처리절차의 주요변경내용

② 금융기관은 제1항의 규정에 불구하고 다음 각호의 1에 해당하는 경우에는 제1항에 의한 사전보고를 생략하고, <별지 제2호 서식>에 따라 업무위수탁현황을 그 금융기관의 설립근거가 되는 법률 등에 따른 업무보고서에 포함하여 감독원장에게 반기별로 사후보고할 수 있다.

1. 당해 금융기관 또는 동일한 금융업을 영위하는 다른 금융기관이 감독원장에게 보고한 내용과 동일한 경우
2. 금융기관이 약관 등을 보고하면서 당해 약관 등의 내용과 관련된 위탁 또는 수탁예정업무를 보고한 경우(제1항에 의한 첨부서류를 제출한 경우에 한한다)
3. 해당 금융기관이 이미 보고한 내용을 일부 변경하는 경우로서 변경되는 내용이 경미한 경우
4. 동일한 수탁자에게 반복, 지속적으로 업무위탁이 이루어지는 경우로서 최초 업무위탁시에 사전보고가 이루어진 경우. 단, 이 경우 금융회사는 사전보고시에 향후 발생 가능한 추가적인 업무위탁의 대략적인 내용을 작성하여 금감원장에게 제출하여야 한다.
5. 금융기관이 제3자로부터 업무를 수탁하는 경우

③ 감독원장은 제1항 및 제2항의 규정에 의하여 금융기관이 보고한 업무위탁 또는 수탁현황을 매반기 금융위에 보고하여야 한다.

제5조(변경권고등) 감독원장은 업무위탁 또는 수탁이 제3조의 규정에 적합하지 아니하다고 판단하는 경우에는 당해 금융기관에 대하여 그 내용의 변경권고 등 필요한 조치를 할 수 있다. 이 경우 감독원장은 그 조치결과를 지체없이 금융위에 보고하여야 한다.

제6조(적용배제) 금융관련법령에서 정하는 바에 따라 금융기관이 제3자에게 업무를 위탁하거나 제3자로부터 업무를 수탁하는 경우에는 이 규정을 적용하지 아니한다.

제7조 <삭제 2005. 7. 27>

제8조(재검토기한) 「훈령 · 예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 규정 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 규정의 유지, 폐지, 개정 등의 조치를 하여야 하는 2015년 7월 1일을 기준으로 매 2년이 되는 시점(매 2년째의 6월 30일까지를 말한다)으로 한다.

부칙

제1조(시행일) 이 고시는 공포한 날부터 시행한다.

제2조(적용례) ① 이 규정 시행 당시 종전의 규정에 따라 체결한 업무위수탁 계약에 대해서는 종전의 규정을 적용한다.

② 이 규정 시행 당시 종전의 규정에 따른 금융기관이 아니었던 자가 체결한 업무위수탁 계약에 대해서는 이 규정을 적용하지 아니한다.

[별표 1]

제2조제2항의 후선업무와 관련한 업무위탁규정 적용배제의 범위

※ 동 기준에서 언급하고 있지 않은 후선업무에 대해서는 동 기준에서 정하고 있는 사항을 준용하여 업무위탁규정 적용 여부를 판단한다.

1 인사관리

세부 업무(예시)	업무위탁규정 적용여부
· 확정된 채용정책에 따른 직원 채용절차(공고, 이력서분류, 서류접수, 시험관리, 인성검사, 평판조회 등)의 대행	배제
· 확정된 보수정책에 따른 급여·퇴직금 계산 및 지급	
· 직원 연수 프로그램 운영, 교육 강의	
· 확정된 인사정책에 따른 계약직 및 노무 관리	
· 인사관련 파일 또는 DB의 축적·관리·분석 등	
· 채용·승진·이동관련 기준 설정 및 대상자 선정 등	적용
· 급여·성과급 등의 지급기준 및 산정방법 결정	

2 경영지원·총무

세부 업무(예시)	업무위탁규정 적용여부
· 문서, 우편물, 물품 등 수발 및 관리 · 사무용품, 집기, 비품, 인쇄물 등 구입 및 관리 · 사무기기 및 고정자산 유지·보수 · 건물 임대차 관리 · 인쇄물 및 컨텐츠 발주 · 각종 행사 주최 및 진행 · 보안 관제 서비스(경비업무 포함) · 우편물, 인쇄물 등 각종 서식·디자인 제작 · 안내자료 등 제작/인쇄/안내(전달) 대행 · 고객만족도 조사	배제
· 콜센터 통화원 통화품질 평가 업무 · 고객정보 변경 확인	적용

3 법률·회계·세무업무

세부 업무(예시)	업무위탁규정 적용여부
· 회사 자체적인 법무·회계담당 부서에서 의사결정을 하되, 업무처리 과정에서 외부 법률자문·소송대리 또는 회계용역 등을 이용	배제
· 세무처리와 관련한 업무 일체를 외부에 위탁	배제
· 법무·회계와 관련한 업무처리 권한 일체를 외부에 위탁	적용

4 정보처리업무위탁규정 사항을 제외한 IT업무

세부 업무(예시)	업무위탁규정 적용여부
· help-desk · PC구입 등 전산시스템 구입 · 유선전화 및 인터넷 회선 유지보수 등 · 정비보수서비스 제공업무	배제
· 후선업무지원 관련 전산시스템 개발 · 전산시스템 운영	적용

5 기타

세부 업무	업무위탁규정 적용여부
· 보험상품 관련 부가서비스의 공급 업무	배제
· 조사/리서치 관련 전담부서를 두고, 집행업무(미스터리 쇼핑, 설문조사)만을 외부위탁	배제
· 외국금융회사 국내지점의 후선업무 전반을 본사 또는 후선업무처리센터 등에서 일괄 수탁받아 집중 처리 · 계열 금융회사의 후선업무 전반을 동일계열 회사에서 일괄 수탁받아 집중처리	적용
· 시설대여업 관련 대여장비 유지보수업무	적용

【별표 2】 생략
【별표 3】

업무 위수탁 기준

금융회사가 업무 위수탁을 추진하는 경우 다음 각호의 사항을 참고로 하여 업무 위수탁운영기준을 제정·운영하여야 한다.

1. 위수탁계약에 따른 리스크 평가 및 관리대책

2. 위수탁계약의 결정·해지 절차 및 재위탁에 관한 사항

3. 위탁업무의 모니터링에 관한 사항

- 위탁업무 수행관련 주요사항(수탁자의 재무상태 및 리스크, 비상계획 및 그 테스트 결과 등)에 대한 모니터링 절차, 모니터링 담당직원의 지정, 경영진에 대한 보고체계 등에 관한 사항

4. 고객정보의 보호에 관한 사항

- 위탁금융회사 고객자료의 별도 관리, 인가된 자에게만 접근권 부여 및 비밀보호 위반시 위탁금융회사의 조치권 등 안전장치 확보

5. 비상계획에 관한 사항

- 수탁자의 부도 또는 통신문제 등 우발상황 발생시 대책에 관한 사항

6. 위탁업무관련 자료에 대한 접근권 확보에 관한 사항

- 감독당국 또는 내외부 감사인의 자료접근권 보장

7. 위수탁 계약서 주요 기재사항

- 위수탁업무의 범위(공급주기, 내용, 형태 등)
- 업무수행의 수단
- 정보제공 책임(수탁자 내부의 영업상 중요정보 포함)
- 수탁자에 대한 감사 권한
- 업무위수탁에 대한 수수료 및 보상금
- 위탁업무에서 발생하는 자료에 대한 위탁금융회사의 소유권과 당해 금융회사의 물적설비 및 지적재산권 등의 이용조건
- 고객정보의 보호 및 비밀유지에 관한 사항
- 업무의 연속성을 확보하기 위한 백업시스템 확보 등 비상계획
- 면책조항, 보험가입, 분쟁해결(중재, 조정 등) 방법
- 수탁자의 책임한계
- 계약의 파기 또는 종료(위탁금융회사의 계약해지권, 자료의 복구방법 등)에 관한 규정
- 감독당국의 검사 수용의무
- 재위탁시 발생한 손해에 대해 원위탁자의 연대배상책임에 대한 내용
- 수탁자가 업무 재위탁시 원계약 준수 명시
- 준거법 및 관할법원(업무위수탁 상대방이 외국에 소재하는 경우)
- 기타 업무위수탁에 따른 리스크관리 등을 위하여 필요한 사항 등

8. 기타 고려사항
- 금융회사는 금융권역 및 위탁대상자의 특성 등을 감안하여 상기 각호의 사항을 가감하여 반영할 수 있다.

【별지 1,2】 생략

금융회사의 정보처리 업무 위탁에 관한 규정

제1조(목적) 이 규정은 금융회사가 「금융위원회의 설치 등에 관한 법률」 제17조제3호에 따라 인가·허가 또는 등록 등(이하 "인가등"이라 한다)을 받은 금융업을 영위함에 있어 정보처리 업무의 위탁 등에 관한 사항을 규정함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다. ① "금융회사"라 함은 다음 각 호와 같다.

1. 「은행법」에 따른 은행
2. 「한국산업은행법」에 따른 한국산업은행
3. 「중소기업은행법」에 따른 중소기업은행
4. 「한국수출입은행법」에 따른 한국수출입은행
5. 「자본시장과 금융투자업에 관한 법률」에 따른 금융투자업자, 종합금융회사
6. 「보험업법」에 따른 보험회사
7. 「상호저축은행법」에 따른 상호저축은행
8. 「신용협동조합법」에 따른 신용협동조합
9. 「여신전문금융업법」에 따른 여신전문금융회사
10. 「농업협동조합법」에 따른 농협은행
11. 「수산업협동조합법」에 따른 수협은행
12. 「전자금융거래법」에 따라 허가를 받거나 등록한 전자금융업자

② "외국계 금융회사"라 함은 외국법령에 따라 설립되어 외국에서 금융업을 경영하는 자의 국내 지점 또는 계열사인 전항의 금융회사를 말한다.

③ "계열사"라 함은 해당 금융회사와 주식보유 등을 통하여 하나 이상의 법인이 개재되어 있고, 이들이 모두 상법상의 모회사 또는 자회사의 출자관계로 연결된 경우를 말한다(다만, 상장된 회사의 경우 소유지분 요건을 발행주식 총수의 100분의 30 이상으로 한다).

④ "금융거래정보"라 함은 금융회사(제2조제2항의 외국계 금융회사를 포함한다. 이하 같다)가 인가등을 받은 금융업을 영위하기 위하여 고객과 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조제2호 가목 및 나목에 규정된 금융거래행위를 함으로써 거래상대방인 고객으로부터 수집한 해당 고객의 정보 및 금융거래행위의 결과로 생성된 고객의 거래내역 정보를 의미한다.

⑤ "정보처리"라 함은 금융회사가 전산설비를 활용하여, 정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 기타 이와 유사한 행위를 하는 것을 말한다.

⑥ "정보처리의 위탁"이라 함은 금융회사가 자신의 정보처리 업무를 제3자로 하여금 계속적으로 처리하도록 하는 행위를 말한다.

⑦ "전산사고"라 함은 정보처리 및 전산설비의 장애, 재해, 파업, 테러 등의 사유로 발생하는 업무의 중단 또는 지연 및 해킹 등 전자적 침해행위가 발생하는 경우를 말한다.

⑧ 이 규정에서 사용하는 용어의 정의는 특별히 정한 경우 외에는 관련법령에서 정하는 바에 따른다.

제3조(적용범위 등) ① 금융회사의 정보처리 위탁과 관련해서는 다른 법령에 특별한 규정이 있는 경우를 제외하고는 이 규정에서 정하는 바에 따른다.

② 금융관련 법령에 따라 금융업의 인가등을 신청한 자에게도 이 규정을 적용한다.

③ 삭제

제4조(정보처리의 위탁) ① 금융회사는 인가등을 받은 업무를 영위함에 있어 정보처리가 요구되는 경우 이를 제3자에게 위탁할 수 있다.

② 제1항의 규정에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우는 정보처리를 위탁할 수 없다. 다만, 다음 제2호의 경우 금융감독원장이 허용하는 방식에 따라 코스콤 또는 저축은행중앙회에 원장 등의 관리를 위탁하는 경우는 제외한다.

1. 관련 법령에서 해당 업무의 위탁을 금지하고 있는 경우
2. 최근 3년 이내에 금융이용자의 정보관리, 감독관련 자료 제출 등 감독기관의 검사와 관련한 사항으로 기관경고 이상의 제재 또는 형사처벌을 2회 이상 받은 경우
3. 기타 업무의 위탁으로 인하여 당해 금융회사의 건전성 또는 신인도를 크게 저해하거나, 금융질서의 문란 또는 금융이용자의 피해 발생이 심히 우려되는 경우

③ 금융회사는 제1항에 따른 정보처리 위탁계약을 체결할 경우 데이터에 대한 접근통제, 전산사고 등에 따른 이용자 피해에 대한 위·수탁회사간의 책임관계, 수탁회사에 대한 감독당국의 감독·검사 수용의무, 수탁회사의 분쟁해결 과정에서의 재판관할 등을 계약 내용에 반드시 포함하여 위탁에 따라 발생할 수 있는 책임관계를 명확히 하여야 한다.

④ 제1항에 따라 정보처리를 위탁받은 자는 위탁받은 업무를 제3자에게 재위탁할 수 있다. 이 경우 본조 제2항·제3항·제5항·제6항, 제5조, 제7조, 제8조를 준용한다.

⑤ 제1항에 따라 정보처리를 위탁받은 자는 정보처리 과정에서 이전받은 정보를 당초 위탁의 범위를 초과하여 다른 목적으로 활용할 수 없다. 다만, 해당 정보 주체의 동의를 얻은 경우는 동의의 범위 내에서 활용할 수 있다.

⑥ 제1항에 따라 정보처리를 위탁하는 경우 위탁된 처리와 관련한 전산설비 및 인력 등은 관련 법령상 인허가를 위한 전산설비 및 인력 구비 요건 등의 충족 여부를 판단시 고려한다.

⑦ 제1항에 따라 정보처리를 위탁하는 경우(제4항에 따라 재위탁하는 경우를 포함한다) 위탁회사는 수탁회사가 이 규정 등 관계법령 및 제3항에 따른 위탁계약 내용상의 의무를 위반하여 발생하는 정보주체 및 이용자의 손해에 대하여 수탁회사와 연대하여 책임을 진다.

제5조(특정정보의 보호) ① 제4조에 따라 정보처리를 위탁하는 경우 금융회사는 각 관련 법령상의 안전성 확보조치를 충실히 이행하여야 한다. 이 때 개인고객의 고유

식별정보는 암호화 등의 보호 조치를 하여야 하며, 특히 국외로 이전되지 않도록 하여야 한다.

② 금융회사는 위탁 처리되는 정보의 보호를 위한 안전성 확보조치의 구체적 내용을 홈페이지 등을 통해 공시하여야 한다. 또한 민감정보의 처리를 위탁할 경우에는 정보주체에게 금융감독원장이 정하는 방법에 따라 개별 고지하여야 한다.

제6조 삭제

제7조(보고) ① 금융회사가 제4조제1항에 따라 개인고객의 금융거래정보(금융거래의 내용이 누구의 것인지를 알 수 없는 경우를 제외한다) 처리업무를 위탁하고자 하는 경우로서 업무를 수탁받는 자가 국외에 소재하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은 업무를 실제로 수행하려는 날의 30영업일 이전에 다음 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.

1. 위탁계약서(안) 사본
2. 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따라 금융기관이 마련하고 준수하여야 할 '업무위수탁 운영기준'
3. 업무위탁 계약이 이 규정 등 관련법령에 위배되지 아니한다는 준법감시인(준법감시인이 없는 경우, 감사 등 이에 준하는 자)의 검토의견 및 관련자료 사본
4. 위탁의 필요성 및 기대효과
5. 위탁에 따른 업무처리절차의 주요 변경내용
6. 정보처리업무 운영에 대한 감독기관의 실질적 감독가능성을 확인할 수 있는 서류
7. 위탁계약 상대방(재위탁 예정시 재위탁계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)

[본호신설 2015. 7. 22.]

8. 전산사고 및 정보유출 등 발생시 피해자 구제절차

[본호신설 2015. 7. 22.]

② 금융회사가 제4조제1항에 따라 개인고객의 금융거래정보(금융거래의 내용이 누구의 것인지를 알 수 없는 경우를 제외한다) 처리업무를 위탁하고자 하는 경우로서 업무를 수탁받는 자가 국내에 소재하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은 업무를 실제로 수행하려는 날의 7영업일 이전에 제1항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.

③ 금융회사가 제1항 및 제2항에 따른 보고의 대상이 되는 금융거래정보를 제외한 금융거래정보의 처리를 위탁하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은 업무를 실제로 수행하는 날로부터 10영업일 이내에 제1항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.

[본항신설 2015. 7. 22.]

④ 금융회사는 다음 각 호의 구분에 따라 정보처리 위탁에 관한 반기 현황을 그 금융회사의 설립근거가 되는 법률 등에 따른 업무보고서에 포함하여 금융감독원장에게 반기별로 사후보고하여야 한다.

1. 제2조제4항에 따른 금융거래정보의 처리업무를 위탁하는 경우로서 다음 각 목에 해당하는 경우
   가. 해당 금융회사 또는 동일한 금융업을 영위하는 다른 금융회사가 금융감독원장에게 보고한 내용과 동일한 경우로서, 위탁 상대방의 업종이 동일한 경우
   나. 이미 보고한 내용을 일부 변경하는 경우로서, 변경되는 내용이 경미한 경우
2. 제2조제4항에 따른 금융거래정보 이외의 정보 처리업무를 위탁하는 경우(다만, 전자금융업자가 위탁하는 경우는 제외)

[본항신설 2015. 7. 22.]

⑤ 금융감독원장은 이 규정에 따른 보고 절차 등과 관련하여 필요한 경우 「금융기관의 업무위탁 등에 관한 규정」의 서식을 사용하도록 할 수 있다.

[종전 제3항에서 이동]

제8조(감독 및 검사) ① 위탁 금융회사 및 해당 업무의 수탁회사는 제4조에 따라 위탁 운영되는 정보처리 업무와 관련하여 금융감독원장의 자료 제출 등 감독 및 검사를 위한 요구에 응하여야 한다.

② 삭제

③ 금융감독원장은 이 규정에 따른 금융회사의 업무 위탁 현황을 매 반기 금융위원회에 보고하여야 한다.

④ 금융감독원장은 위탁회사 또는 수탁회사의 정보처리 위탁행위 또는 위탁된 업무의 수행과 관련된 행위가 이 규정 등 관계법령, 제7조제1항제2호의 '업무위수탁 운영기준'에 적합하지 아니하다고 판단하는 경우에는 위탁회사 또는 수탁회사에 대하여 그 내용의 자료제출 및 보완요구, 변경권고 등 필요한 조치를 할 수 있다.

제9조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제334호)에 따라 이 규정 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 규정의 유지, 폐지, 개정 등의 조치를 하여야 하는 기한은 2018년 7월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 6월 30일까지를 말한다)으로 한다.

부칙

이 규정은 공포한 날부터 시행한다.

금융분야 클라우드컴퓨팅서비스 이용 가이드

발 행 : 2019년 1월
발행인 : 김 영 기
발행처 : 금융보안원
주 소 : 경기도 용인시 수지구 대지로 132

〈비 매 품〉

이 가이드 내용의 무단전재를 금하며, 가공 인용할 때에는 반드시 금융보안원 「금융분야 클라우드컴퓨팅서비스 이용 가이드」라고 밝혀 주시기 바랍니다.