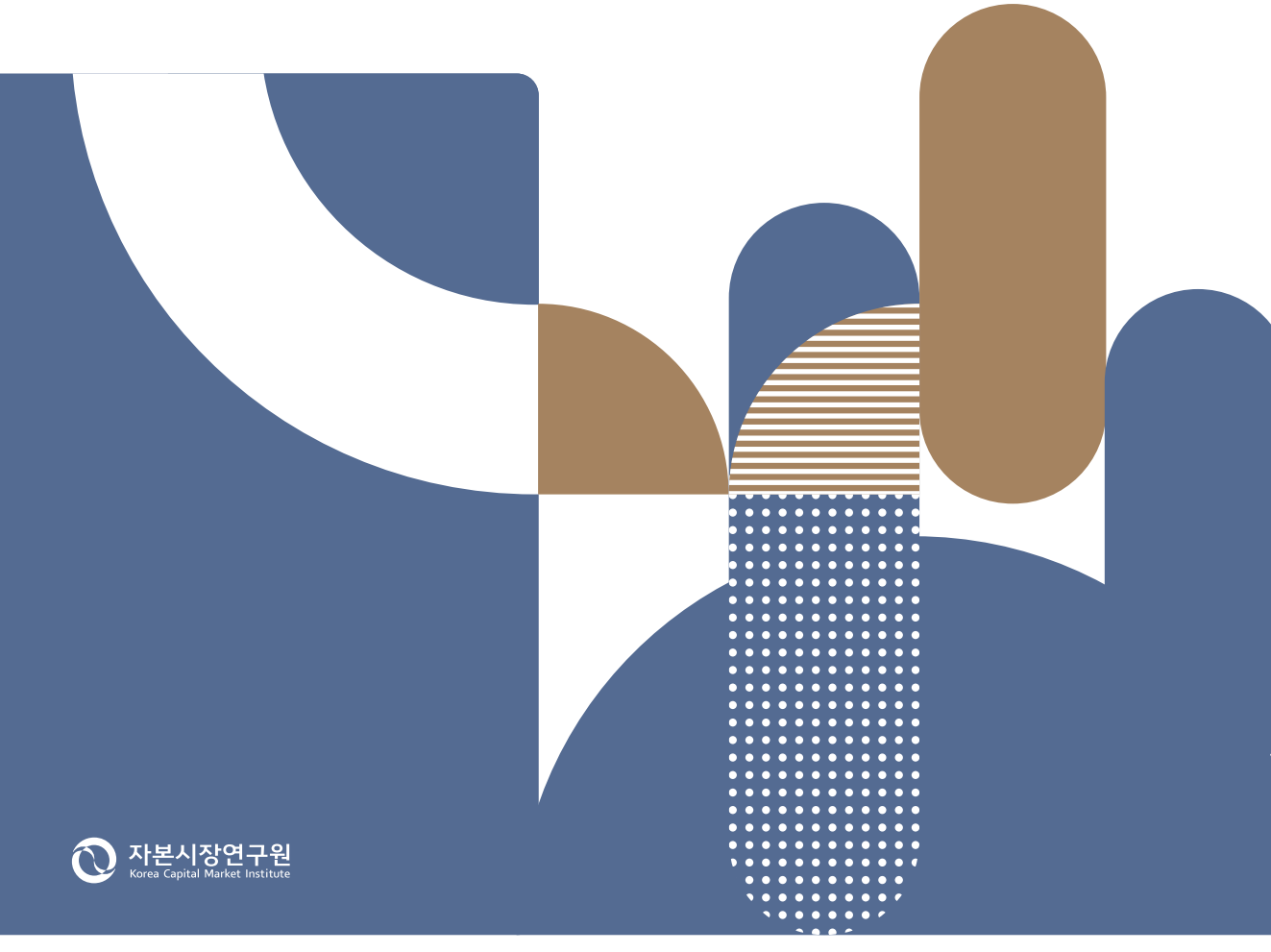
연구보고서 20-01

RESEARCH
REPORT

금융투자회사 아웃소싱 관리 해외사례

조성훈



자본시장연구원
Korea Capital Market Institute

금융투자회사 아웃소싱 관리 해외사례

2020. 12

선임연구위원 조성훈

자본시장연구원

Contents

Ⅰ. 서론 3

Ⅱ. 국내 금융업 업무위탁 현황

1. 국내 금융투자업 업무위탁 현황 13
2. 국내 금융업 업무위탁 규제 15

Ⅲ. 주요국 공적 기관의 아웃소싱 관리 지침

1. 미국 25
2. 유럽(EU) 32
3. 영국 35
4. 싱가포르 39

Ⅳ. 해외 금융회사 아웃소싱 관리 내부 지침

1. 글로벌 금융회사의 공급업체 행동 강령 43
2. JP Morgan의 ‘Minimum control requirements’ 45

Ⅴ. 시사점 53

Executive Summary

기업이 내부적으로 직접 수행하던 활동이나 기능을 기업 외부의 제3자로 하여금 수행하게 하는 것을 의미하는 아웃소싱은 비용 절감 · 경영효율성 제고 · 핵심역량 강화 등을 목표로 하는 기업의 전략적 의사결정이며, 이러한 중요성은 금융투자업을 비롯한 금융산업에서도 동일하다. 특히 '4차 산업혁명'이라고 불리는 최근의 급속한 기술 발전에 따라 금융산업의 가치사슬이 변화하면서 아웃소싱은 더욱 중요해지고 있다. 그러나 국내 금융업의 경우 아웃소싱(업무위탁)에 대한 법령상의 규제가 경직적으로 운영되어 금융회사가 아웃소싱을 활용하는 데 제약이 많고, 급변하는 환경에 대응하지 못한다는 의견이 제기되었으며, 이에 따라 아웃소싱 규제는 완화되는 추세에 있다.

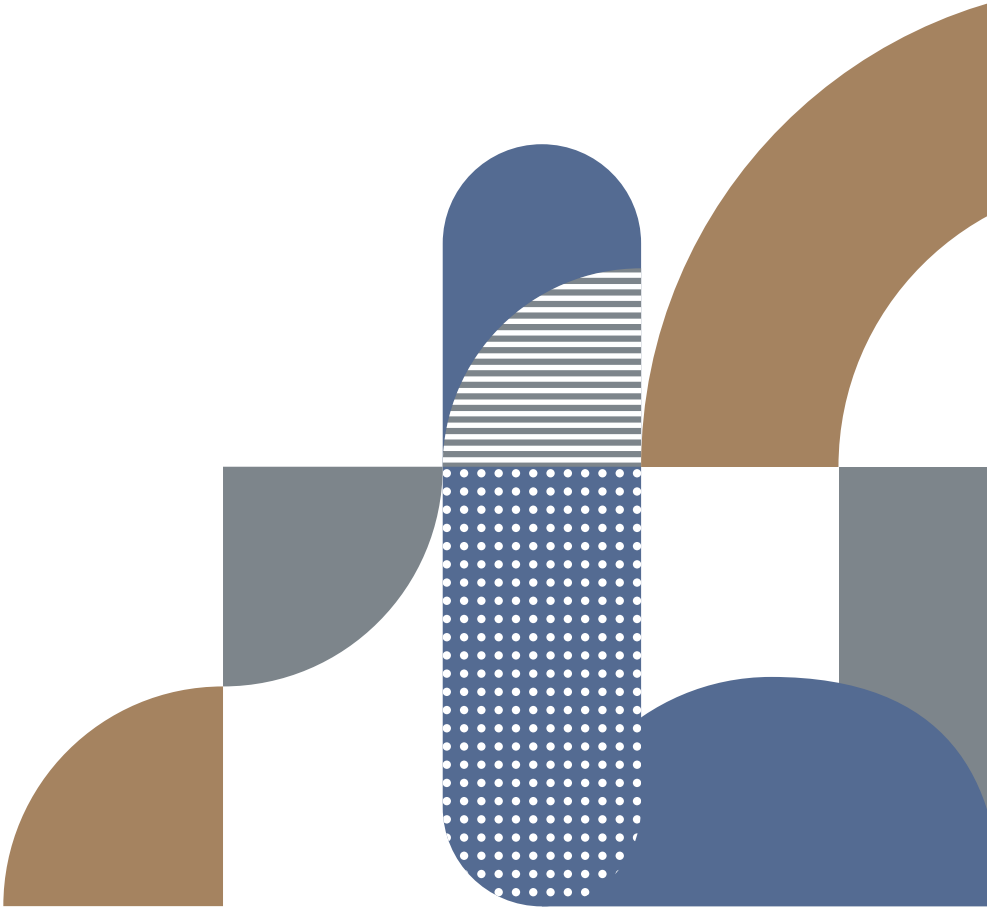
미국, 유럽(EU), 영국, 싱가포르 등 주요 외국에서는 금융회사의 아웃소싱에 대하여 법령으로 규제하고 있지 않으며, 대신 FRB, FDIC(이상 미국), EBA(EU), FCA(영국), MAS(싱가포르)와 같은 공적 기관들이 금융회사의 아웃소싱 관리를 위한 지침 또는 가이드라인을 만들어 제공하고 있다. 이 기관들의 지침은 공통적으로 아웃소싱 의사결정과 관리에 있어서 이사회와 최고경영진의 역할과 책임을 강조한다. 그리고 아웃소싱 리스크 평가, 아웃소싱 공급업체 실사 및 선정, 아웃소싱 계약의 설계 · 체결, 공급업체 모니터링으로 이어지는 관리 프로세스도 대동소이하게 제시하고 있다. 국내 금융투자회사의 업무위탁에 적용되는 자본시장법 및 시행령, 금융투자업규정에 담겨 있는 내용에 비하여 이 기관들의 지침은 보다 상세하고 구체적이며 기술적인 부분까지 언급하고 있다.

해외의 글로벌 금융회사들은 모두 자사의 아웃소싱 관리를 위하여 '공급업체 행동 강령'을 마련하여 공급업체에게 적용하고 있는데, 이 강령은 공급업체가 준수해야 하는 기본적 사항들을 비교적 추상적이고 선언적 수준에서 제시한 것이다. 이 행동 강령은 공통적으로 사업에 있어서 윤리 및 무결성(integrity), 노동 및 인권, 환경 및 지속가능성, 다양

성 및 포용(inclusion)에 관한 사항들을 담고 있으며, 아웃소싱 관리를 위한 내부 지침과는 약간 차이가 있다. 본 보고서에서는 구체적인 아웃소싱 관리 내부 지침으로 JP Morgan의 'Minimum control requirements'의 내용을 소개하고 있는데, 이것은 IT 아웃소싱을 효과적으로 통제하고 관련 리스크를 효과적으로 관리하기 위한 최소한의 통제 요구사항을 규정한 것으로 매우 구체적이고 상세한 내용을 담고 있다.

우리나라의 아웃소싱 규제가 지속적으로 완화되고 궁극적으로 원칙중심으로 전환되면 본 보고서에서 소개한 외국 사례와 같은 지침이 필요할 것이다. 그리고 그 지침이 연성규범으로서 효과적으로 작동하고, 금융회사가 아웃소싱을 추진할 때 실질적인 도움을 줄 수 있기 위해서는 구체적이고 전문적이어야 한다. 금융회사의 내부적 아웃소싱 관리 지침 역시 전문적 · 구체적 · 기술적이어야 하는 바, 이러한 내부 지침을 만들고 시행하기 위한 자체 인력의 기술역량 확보 노력이 필요하다. IT 아웃소싱의 증가에 따라 고객과 금융회사의 데이터 및 정보와 관련된 리스크 관리의 중요성이 커지고 있으며, 금융회사는 아웃소싱 관리에 있어서 이사회와 최고경영진의 책임에 대한 인식을 높일 필요가 있다.

I. 서론



Ⅰ. 서론

아웃소싱(outsourcing)은 '전통적으로 기업의 종업원에 의하여 기업이 보유한 설비를 사용하여 내부적(in-house)으로 수행되던 활동이나 기능을 기업 외부의 제3자(third party)로 하여금 수행하게 하는 것'으로 정의된다.[01] 국내 금융 법규에서는 '업무위탁'이라는 용어를 사용하고 있으며, '금융투자업자가 영위하는 업무의 일부를 제3자에게 위탁'하는 것(「자본시장과 금융투자업에 관한 법률」(이하 '자본시장법') 제42조 제1항), 또는 '금융기관이 인가 등을 받은 금융업을 영위하기 위하여 제3자의 용역 또는 시설 등을 계속적으로 활용하는 행위'(「금융기관의 업무위탁 등에 관한 규정」(이하 '업무위탁규정') 제2조 제2항)로 정의하고 있다. 따라서 기업이 설비를 보유하고 외부인력의 파견을 받아 기업의 의사결정 하에 활동 · 기능을 수행하는 것은 업무위탁으로 보지 않는다.

아웃소싱 또는 업무위탁 외에 거의 동일한 의미를 갖는 용어로 '외주', '하청' 등이 사용되고 있으며, 본 보고서에서는 국내 현황과 법규를 설명하는 경우(주로 제Ⅱ장)에만 '업무위탁', 그 외에는 '아웃소싱'이라는 용어를 사용한다. 아웃소싱 계약에 의하여 기업(위탁자)에게 업무 · 기능을 제공하는 주체를 지칭하는 용어도 '수탁자(업체)', '(제3자) 공급업체((third party) supplier)', '(제3자) 제공업체((third party) provider)', '벤더(vendor)', '외주업체', '하청업체' 등으로 다양하며, 본 보고서에서는 역시 국내 법규를 설명하는 경우에는 법규의 용어대로 '수탁자', 그 외에는 '(제3자) 공급업체'라는 표현을 사용한다.

흔히 아웃소싱과 혼동되는 개념으로 'offshoring'이 있는데, 아웃소싱과 offshoring은 각각의 핵심이 다른 개념이다. 아웃소싱은 기업 내부의 활동을 제3자에게 이전하는 것이 핵심인 반면, offshoring은 기업 활동 장소의 지리적 이동에 핵심이 있다.[02] 본 보고서에서는 아웃소싱만을 조사 대상으로 하며, offshoring은 다루지 않는다.

기업이 어떤 업무나 기능을 내부에서 수행할 것인지, 제3자에게 아웃소싱할 것인지의 결정에 관한 이론적 설명의 뿌리는 Coase의 기업이론에서 찾을 수 있다. 업무 · 기능을 기업 외부로부터 (즉 시장으로부터) 조달할 경우 기업과 그 업무 · 기능을 제공하는 제

01 고대영 외(2015), 정홍준 외(2017), 하헌식(2017), EBA(2019), Economist(2008), Webb(2017), Investopedia(2019) 등을 참고하여 정리하였다.

02 콜센터나 IT 설비를 낮은 인건비로 우수한 인력을 고용할 수 있는 국가(예: 인도)로 이전하는 것이 offshoring의 대표적 사례이다.

3자 간의 불완전계약(incomplete contract)으로부터 발생하는 비효율이 그 업무 · 기능을 내부적으로 수행하는 경우 부담하는 비용보다 클 때 기업은 내부 수행, 즉 수직적 통합(vertical integration)을 선택한다.[03] 다시 말해 기업이 아웃소싱을 선택하는 이유는 아웃소싱에 따른 비용(불완전계약으로부터 발생하는 비효율)이 내부 수행에 따른 비용보다 작다고 판단하기 때문이다.

아웃소싱이 내부 수행보다 효율적일 수 있도록 만드는 요인, 즉 아웃소싱의 장점으로는 우선 기업이 자신이 비교우위를 갖는 부문에 역량을 집중하고 그렇지 못한 부문을 아웃소싱함으로써 얻을 수 있는 선택과 집중에 의한 경영효율성 제고를 들 수 있다. 그리고 아웃소싱하고자 하는 업무 · 기능에 특화된 전문업체에 그 수행을 맡김으로써 해당 업무 · 기능의 질적 수준을 제고할 수 있다. 다음으로는 IT(information technology) 부문에서 많이 볼 수 있는 것으로서, 대규모 설비투자 부담을 완화하고 이를 통하여 초기 시장 진입에 필요한 투자 규모를 줄일 수 있다. 이는 경기변동이나 시장상황의 변화로 수요가 감소할 경우 설비의 구조조정을 쉽게 해주는 효과도 갖는다. 아웃소싱 공급업체의 입장에서는 여러 기업으로부터 동일한 업무를 수탁받아 운영 · 공급함으로써 규모의 경제를 달성할 수 있다.

아웃소싱의 단점으로는 우선 아웃소싱을 공급하는 제3자 공급업체의 통제와 관련하여 발생가능한 모든 상황과 가능성을 고려한 계약을 만들 수 없다는 불완전계약의 문제가 있다. 또한 아웃소싱된 업무 · 기능의 수행에 있어서 아웃소싱 공급업체에 대한 의존도가 지나치게 높아지게 되면 소위 'hold-up' 문제가 발생하여 기업은 공급업체에 대한 통제력을 상실하게 되고, 이는 경영전략, 구조조정 등에서의 유연성을 내부 수행의 경우보다 오히려 더 떨어뜨리는 결과를 초래할 가능성도 존재한다.

따라서 아웃소싱은 단순히 어떤 업무나 기능의 수행을 외부에 위탁한다는 수준을 넘어서, 비용 절감 · 경영효율성 제고 · 핵심역량 강화 등을 위하여 수행되는 기업의 전략적 의사결정이며, 아웃소싱을 할 것인지의 여부는 이사회를 포함한 최고경영진의 의사결정 영역에 포함되는 문제이다. 자사의 IT 부문을 아웃소싱했으나 아웃소싱 공급업체의 관리가 효과적으로 이루어지지 않아 당초 기대했던 성과를 얻지 못하고 결국 내부수행으로 회귀하면서 이 과정에서 회사와 경영진의 평판, 인력을 비롯한 경영자원의 낭비를 경험했던 J.P. Morgan Chase의 사례는 이를 잘 보여준다.

03 Bolton & Scharfstein(1998)

[사례] JP Morgan Chase(JPMC)의 IT 아웃소싱 실패[04]

2002년 12월 30일, JPMC는 자사의 IT 부문을 아웃소싱하기로 하고, 그 파트너(제3자 공급업자)로 IBM을 선정, 계약했다고 발표하였다. 비용 절감, 혁신 촉진, IT 부문 인력의 복지(benefit) 증진이 아웃소싱을 추진하게 된 동기로 언급되었다. 아웃소싱 계약기간은 7년이며, 아웃소싱의 범위는 데이터센터, 고객지원(help desk), 분산컴퓨팅(distributed computing), 데이터 및 음성 네트워크(data and voice network) 등을 포괄하였다.

그러나 당초 발표와는 달리, JPMC의 IT 부문 인력의 IBM으로의 고용승계가 100% 이루어지지 않았고, 동시에 상당한 급여 삭감이 발생하였다. IBM 자신이 이미 사업의 상당 부분을 'offshoring'하고 있었기 때문에 자체 고용은 최소한의 수준을 유지하려고 했기 때문이다. 또한 JPMC는 아웃소싱 보수를 IBM의 요구대로 인상하지 않으려고 했고, 이에 대하여 IBM은 JPMC가 필요로 하는 모듈의 추가를 거부하는 사태가 발생하여 JPMC IT 인프라의 문젯거리가 되었다.

이러한 어려움을 겪는 와중에, 2004년 7월 1일 JPMC는 Bank One과의 합병을 발표하였는데, Bank One의 CEO Jamie Dimon은 과거 IBM, AT&T와의 아웃소싱 거래를 취소한 전력이 있었다. 그리고 Jamie Dimon이 합병 후 JPMC의 COO를 거쳐 CEO가 되었다. 이후 2004년 9월 15일 JPMC는 IT 아웃소싱을 취소하고 다시 직접 내부적으로 수행하기로(backsourcing) 결정했다고 발표하였다. 이 과정에서 IBM에서 JPMC로 돌아오게 될 IT 인력과 Bank One IT 인력의 중복 문제가 발생하였고, 결국 인력 구조조정이 불가피해졌다. 그에 따라 다수의 IT 인력이 JPMC 경영진에 대한 신뢰, 사기, 생산성을 잃었고, 경영자원 및 시간의 낭비가 초래되었다.

금융투자업을 비롯한 금융산업에서도 아웃소싱은 중요한 경영전략으로 다양한 부문에서 활용되고 있다. 해외 금융회사들의 아웃소싱 실태에 대한 서베이 자료들에 의하면[05], 아웃소싱이 가장 활발하게 이루어지고 있는 업무 영역은 인프라 및 후선(post-trade pro-

04 Overby(2005)

05 참고한 서베이 자료는 다음과 같다. BNP Paribas & Oliver Wyman(2017), McCahery & De Roode(2018)

cessing)업무이다. 그 중에서도 인프라에 해당하는 IT 및 데이터관리 부문에서 아웃소싱이 가장 많이 이루어지고 있으며, 대사(reconciliation), 결제, 승인 등의 후선업무 부문이 그 뒤를 따르고 있다. 후선업무는 이미 고도로 상품화(commoditize)되었으며 차별화의 중요성이 감소하고 있기 때문에 아웃소싱을 통하여 비용을 절감하고 핵심전략에 집중할 수 있게 된다는 것이 그 이유이다. 이어서 회계, 컴플라이언스 등 중선(middle-office)업무에서의 아웃소싱이 점차 증가하고 있으나, 아직까지 활발하게 이루어지고 있지는 않은 것으로 보인다. 또한 전선(front-office)업무는 대부분의 금융회사들이 자신의 핵심업무로 인식하고 있으며, 따라서 전선업무를 아웃소싱하는 사례는 드물다.[06]

일반 산업과 달리, 금융소비자 보호와 금융시스템 안정을 도모해야 하는 금융산업의 경우 아웃소싱이 내포하는 불완전계약, 즉 아웃소싱 공급업체에 대한 불완전한 통제의 문제와 관련한 다양한 리스크를 안고 있다. 여기에는 공급업체에 의한 기업내부의 중요 정보나 고객 정보의 누출과 같은 보안사고, 공급업체의 법령 위반으로 인한 금융회사 자신의 평판 훼손, 시스템상의 오류나 인간의 실수 등으로 인한 운영리스크(operational risk) 등이 포함된다.

[사례] 2014년 신용카드 개인정보 유출 사건[07]

2012년 12월부터 2013년 12월까지 1년여에 걸쳐 국내 3개 신용카드회사로부터 회원 개인정보 약 1억건이 외부로 유출되는 사건이 발생하였다. 유출된 정보는 성명, 주민등록번호, 주소, 휴대전화번호, 직장명 등 개인의 신상정보와 결제계좌, 연소득 등 신용정보이다. 검찰의 수사 결과 신용카드 위 · 변조 방지 시스템 개발을 맡은 공급(외주)업체의 용역 작업 과정에서 외부 파견직원이 카드 회원의 개인정보 등을 불법으로 수집하였으며, 수집된 정보는 대출광고업자 및 대출모집에게 유출된 것이 밝혀졌다. 외부인의 USB 사용 차단, 고객정보 암호화 등 기본적인 보안절차가 있었음에도 불구하고 신용카드회사 및 공급업체가 이를 제대로 준수하지 않았던 것이 이 사건의 핵심 원인으로 지목되었다. 이 사건을 계기로 고객정보 유출 방지를 위한 금융회사의 내부통제절차 강화, 외부 공급업체 및 그 직원에 대한 관리 강화 조치가 발표되었다.

06 본 문단은 조성훈(2019)의 일부를 인용하였다.

07 금융위원회(2014. 1. 8, 2014. 1. 22, 2014. 3. 10)

2013년 말에서 2014년 초에 걸쳐 발생한 신용카드회사의 개인정보 유출 사건은 이러한 리스크를 보여준 대표적 사례이다.

금융산업의 아웃소싱이 갖는 특성과 리스크를 고려하여 우리나라에서는 법령을 통하여 아웃소싱의 범위, 방법, 공급업체 관리 등을 직접적으로 규제하고 있다. 금융투자회사의 아웃소싱은 자본시장법 및 그 하위규정, 여타 금융회사의 아웃소싱은 업무위탁규정을 통하여 규제하고 있다.

그런데 최근 금융산업의 아웃소싱 환경에는 큰 변화가 일어나고 있다. 특히 '4차 산업혁명'이라고 불리는 최근의 급속한 기술 발전은 금융산업에서 디지털 혁신(digitalization)을 일으키면서 금융서비스 또는 상품이 만들어져서 제공되는 과정, 즉 금융산업의 가치사슬(value chain)을 근본적으로 변화시키고 있다. 인공지능(artificial intelligence: AI)을 활용한 자산관리ㆍ대출심사, 블록체인(blockchain)을 활용한 해외송금 또는 자산거래 플랫폼, 생체인증 기술을 활용한 본인확인 등이 현재 구현되고 있는 혁신적 기술의 활용 사례이며, 이러한 기술 기반 서비스를 제공하는 새로운 기술기업들이 등장하고 있다. 이와 같이 급변하는 환경에서 금융회사들은 기존의 방식대로 가치사슬의 전 과정을 내부적으로 통합하여 서비스를 제공할 수도 있지만, 어떤 기능이나 서비스를 아웃소싱을 통하여 해결하는 것이 더욱 효율적이거나 불가피할 가능성도 보다 커졌으며, 따라서 아웃소싱의 중요성이 커지고 있다. 또한 금융산업 가치사슬의 변화는 기존의 업무 구분에 따른 아웃소싱 규제 방식이 한계에 봉착했음을 의미하기도 한다. 기존의 업무 구분으로는 명확하게 규정하기 어려운 새로운 기능이 출현할 수 있기 때문이다.

따라서 금융산업, 특히 자본시장법이 직접 규율하고 있는 금융투자업의 경우 현재의 규제 방식으로는 아웃소싱 환경 변화 및 이로 인한 금융회사의 수요 증가에 효과적으로 대응할 수 없다는 의견이 지속적으로 제기되어 왔다. Ⅱ장에 서술된 바와 같이 금융투자업에서 업무위탁은 2010년 620건에서 2013년 136건, 2016년 52건, 2019년에는 40건으로 지속적으로 감소하였는데, 아웃소싱 공급업체의 역량 부족 등과 더불어 아웃소싱에 대한 경직된 규제가 이러한 감소를 초래한 주요 원인으로 제기되었다.[08] 이러한 변화와 업계의 의견을 반영하여 금융위원회는 핵심업무와 비핵심업무 구분 폐지, 재위탁의 원칙적 허용, 단순 정보처리 업무에 대한 자유로운 위탁 허용 등을 담은 업무위탁 규제 개선방안을 발

08 금융투자협회(2018), 금융위원회(2019. 5. 27)

표하였고[09], 이에 따라 자본시장법도 일부 개정되었다.[10]

금융산업의 선진국으로 알려진 미국, EU, 영국 등 주요 외국에서 금융회사의 아웃소싱에 있어서 아웃소싱이 가능한 범위, 아웃소싱의 방법 등에 대하여 법령에 의한 공적 규제를 하는 경우는 거의 없다. 대신 개별 금융회사들이 아웃소싱에 따른 리스크를 효과적으로 관리하는 데 도움을 주기 위하여 규제 · 감독기관을 포함한 공적 기관들이 지침 또는 가이드라인을 마련하여 제시하고 있다. 그리고 개별 금융회사들은 각각 내부적으로 아웃소싱 리스크 관리를 위한 '제3자 공급업체 행동 강령(code of conduct)'을 마련하고, 아웃소싱 계약 및 공급업체 관리에서 활용하고 있다.

금융회사의 아웃소싱을 법령으로 규제하지 않는다는 것이 아웃소싱에 대한 규제가 전혀 없다는 것을 의미하지는 않는다. 공적 기관들의 아웃소싱 관리 지침들은 연성규범(soft norm)으로서 원칙적으로 지침의 준수를 요구하며, 그렇지 않은 경우에는 그 이유를 설명하도록 함으로써 강제력을 가진다. 또한 아웃소싱으로부터 어떤 문제가 발생한 경우 금융회사의 책임 범위를 판단하는 기준으로 활용되며, 따라서 금융회사로 하여금 지침을 준수할 유인을 부여하는 효과를 갖는다.

우리나라에서도 아웃소싱 규제가 본격적으로 완화되면 이들 국가들과 유사하게 아웃소싱 의사결정부터 아웃소싱 리스크 관리에 이르기까지 개별 금융회사들의 자율의 폭이 크게 넓어질 것이며, 동시에 그 결과에 대한 책임도 직접적으로 지게 될 것이다. 그리고 이러한 환경에서 아웃소싱 리스크의 효과적 관리를 위하여 자체적인 내부 지침이나 가이드라인을 마련하여 운영해야 할 필요성이 커진다.

본 보고서는 장기적으로 국내의 금융회사 아웃소싱 규제가 완화되어 궁극적으로는 원칙중심으로 전환되고, 개별 금융회사들이 아웃소싱을 자율적으로 관리해야 하는 시대의 도래에 대비하여, 이미 이러한 환경에 있는 주요 외국의 사례를 조사 · 정리하여 국내 금융당국 및 금융회사에 대한 참고자료를 제공하는 것을 목적으로 한다. 이를 위하여 본 보고서에서는 주요 외국 공적 기관의 아웃소싱 관리 지침 · 가이드라인과 개별 금융회사의 내부지침의 핵심적 내용들을 정리하여 소개한다.

아웃소싱을 다룬 기존 연구로서 임형석 외(2014), 이승준 · 정인영(2017)은 각각 은행업과 보험업에서의 아웃소싱 관련 규제의 개선 방안을 제시하였고, 정흥준 외(2017)는 아

09 금융위원회(2019. 5. 27)

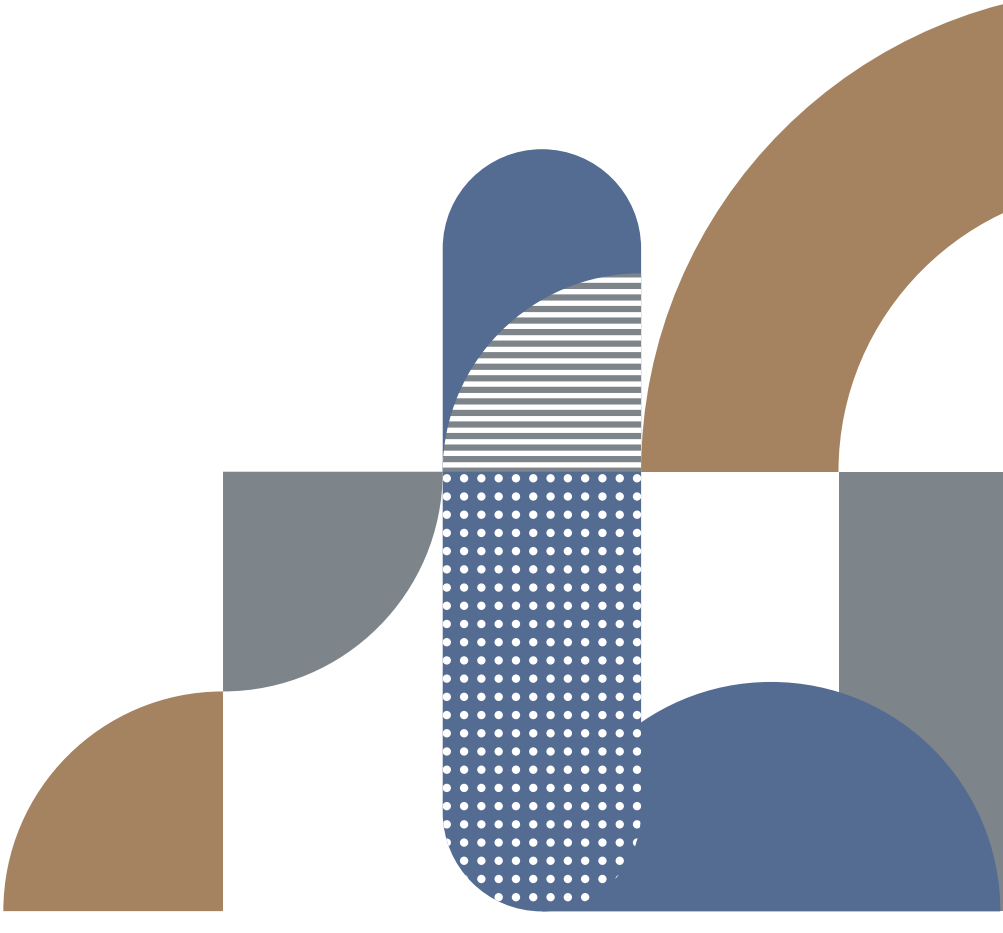
10 금융위원회(2020. 4. 29), 개정된 자본시장법은 공포 후 1년 후부터 시행된다.

웃소싱이 기업 내부의 고용관계에 미치는 영향 및 사회경제적 효과를 평가하였다. 본 보고서는 현행 아웃소싱 규제의 개선 방향을 제시하는 것이 아니라, 원칙중심 규제로의 개선을 전제로 하여 그 준비를 위한 참고자료를 정리 · 제공하는 것이 목적이라는 점에서 이들 선행연구와 구별된다.

보고서의 Ⅱ장에서는 우리나라의 현행 업무위탁 규제의 내용을 정리 설명한다. Ⅲ장에서는 주요 외국 공적 기관의 아웃소싱 관리 지침 · 가이드라인의 핵심 내용을 정리하고, Ⅳ장에서는 글로벌 금융회사들의 내부지침의 핵심 내용을 정리하여 소개한다. 마지막으로 Ⅴ장에서 국내 금융회사의 아웃소싱 관리를 위한 시사점을 제시한다.

II. 국내 금융업 업무위탁 현황

1. 국내 금융투자업 업무위탁 현황
2. 국내 금융업 업무위탁 규제



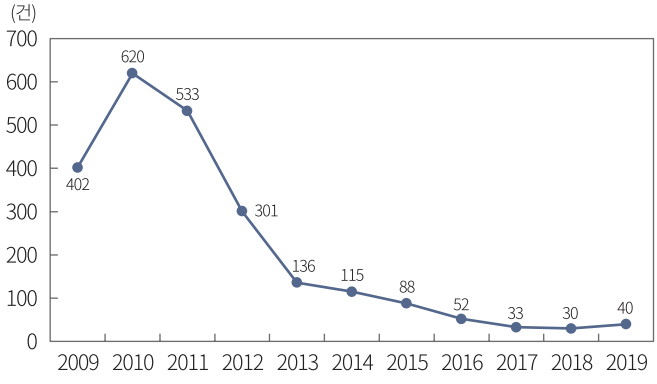
II. 국내 금융업 업무위탁 현황

금융업에서의 업무위탁에 대한 국내의 규제 체계는 금융투자업에 적용되는 자본시장법과 금융투자업을 제외한 여타 금융업에 적용되는 업무위탁규정으로 이원화되어 있다. 이 외에 4차 산업혁명 등에 따른 기술 혁신의 금융서비스 도입을 촉진하기 위한 목적으로 제정된 「금융혁신지원특별법」, 금융회사의 정보처리 업무의 업무위탁을 규율하는 「금융회사의 정보처리 업무위탁에 관한 규정」(이하 '정보처리업무위탁규정')이 있다. 본 장에서는 먼저 국내 금융투자업에서의 업무위탁 현황을 알아보고, 이어 업무위탁을 규율하는 법규들의 핵심적 내용을 정리 · 소개한다.

1. 국내 금융투자업 업무위탁 현황

후술하는 바와 같이 어떤 업무를 외부의 공급업자에게 위탁하려는 금융투자회사는 업무위탁이 개시되기 7일 전까지 금융위원회에 보고(사전보고)해야 한다. <그림 Ⅱ-1>은 자본시장법이 시행된 2009년부터 2019년까지 접수된 업무위탁 사전보고 건수의 연도별 추이를 보여준다. 금융투자업에서의 업무위탁은 자본시장법 시행 직후인 2010년 620건을 정점으로 이후 지속적으로 감소하여 2018년에는 30건으로 2010년의 1/20 아래로 떨어졌다. 이와 같이 업무위탁이 급감한 원인은 확실하지 않으나, 금융투자협회(2018), 금융위원회(2019. 5. 27) 등은 업무위탁 수행업체(공급업체)의 역량 부족, 경직된 업무위탁 규제로 인한 제약을 감소의 원인으로 언급하고 있다.

<그림 Ⅱ-1> 국내 금융투자업 업무위탁 추이

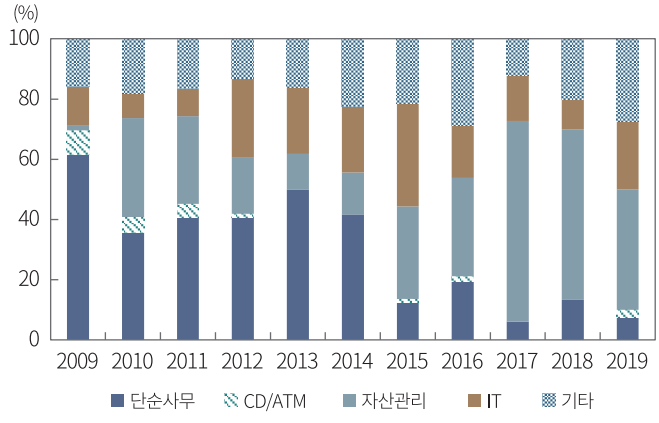


주 : 금융위원회에 접수된 업무위탁 사전보고 건수
자료: 금융감독원

<그림 Ⅱ-2>는 외부 공급업자에게 위탁된 업무의 내역을 몇 개의 그룹으로 분류하여 그 비중의 연도별 변화를 나타낸 것이다. 2009년부터 2014년까지는 실명확인, 우편물 출력 · 발송과 같은 반복적인 단순사무업무가 가장 큰 비중을 차지하였으나, 이후 급감하였다. 이와 같은 단순사무 업무위탁의 급감은 다른 부문에서의 업무위탁이 뚜렷하게 증가하지 않은 것과 맞물려 <그림 Ⅱ-1>에서 나타난 전체적인 업무위탁의 감소를 부분적으로 설명하는 것으로 보인다. 현금지급기(CD · ATM) 설치 · 운영의 위탁은 2011년까지는 어느 정도 발견되나, 2013년 이후로는 거의 나타나지 않는다. 한편 금융투자회사의 일임자산 또는 랩어카운트 등의 운용에 대한 투자자문을 외부의 자산운용사나 투자자문사에 위탁하거나[11], 관련 부수업무를 외부 공급업체에 위탁하는 유형의 비중이 급격하게 증가하였다. IT 부문에서의 업무위탁은 그 비중이 8~34% 범위에서 증감하고 있으며, 뚜렷하게 큰 비중을 차지하고 있지는 않다.

11 이것은 증권회사와 자산운용사·투자자문사 간의 자문계약의 성격을 띠며, 본 보고서에서 의미하는 아웃소싱과는 그 성격이 다르다.

<그림 II-2> 국내 금융투자업 위탁업무별 비중 추이



주 : 1) 단순사무: 실명확인, 우편물 발송 등
2) CD/ATM: 현금지급기(CD/ATM기) 설치 및 운영 등
3) 자산관리: 일임자산·랩어카운트 등의 운용을 위한 투자자문, 자산보관·평가 등 부수업무
4) IT: 시스템 개발·유지보수, 데이터 저장·관리 등
자료: 금융위원회에 접수된 업무위탁 사전보고 자료를 이용하여 저자 계산

2. 국내 금융업 업무위탁 규제

가. 금융투자업: 자본시장법

국내에서 금융투자업의 업무위탁에 대해서는 은행, 보험 등 여타 금융업과는 별도로 자본시장법에서 규율하고 있다. 자본시장법 시행 전까지 모든 금융업의 업무위탁은 업무위탁규정에서 통일적으로 규율하였으며, 수차례의 규정 변경을 통해 업무위탁 허용 범위를 점차 넓혀 왔다. 그러나 자본시장법에서는 금융투자업의 업무위탁에 대해 그 허용 범위를 대폭 넓히고, 그에 비례하여 투자자보호 등을 위한 절차를 강화하는 방향으로 규정함으로써 규제를 체계화하였으며, 그에 따라 금융투자업은 자본시장법의 규율을 받게 되었다.[12]

자본시장법 제42조는 금융투자업자에게 허용되는 업무위탁의 범위, 업무위탁의 운영 및 기타 규제 사항을 정하고 있다. 우선 'negative system' 즉 '원칙허용, 예외금지'의 원칙에 입각하여 고유업무, 겸영업무, 부수업무의 일부를 제3자에게 위탁할 수 있다. 위탁이

12 변제호 외(2015)

금지되는 업무는 본래 '본질적 업무 중 핵심업무'로서 동법 시행령 제45, 47조에 열거되어 있었으나[13], 2020년 4월의 자본시장법 개정에 따라 '시행령으로 정하는 내부통제업무로서 의사결정권한까지 위탁하는 경우'로 단순화되었다.[14] 즉 이 조항에 해당되지 않는 모든 업무는 위탁이 가능하게 된 것으로서, 'negative system' 원칙에 보다 충실한 방향으로 업무위탁의 범위가 대폭 확대된 것이다. 단, 본질적 업무를 위탁하는 경우에, 수탁자(제3자 공급업자)는 해당 업무 수행에 필요한 인가를 받거나 등록을 한 자여야 한다.[15]

금융투자업자는 업무위탁을 할 경우 위탁계약을 체결하여야 하며, 위탁계약의 내용을 업무위탁 수행 개시 7일전까지 금융위원회에 보고해야 한다. 자본시장법 및 그 하위규정에서는 위탁계약에 포함되어야 하는 사항들을 열거하고 있는데, 그 내용은 <표 Ⅱ-1>과 같다. 개별 금융투자회사들은 투자자정보 보호 및 위험관리 · 평가 등에 관한 업무위탁 운영기준을 정하고, 업무위탁 보고시 업무위탁계약서 등과 함께 제출하여야 한다. 다만 이미 보고한 내용을 일부 변경한 경우로서 변경되는 내용이 경미한 경우(예: 수수료 변경, 계약기간 변경) 등에 해당하는 경우에는 사후보고가 가능하다.

그리고 금융위원회는 업무위탁으로 인하여 금융투자업자의 건전성이 저해되거나 투자자보호에 지장을 초래하는 등의 경우에는 업무위탁을 제한하거나 시정을 명할 수 있다. 또한 금융투자업자는 업무위탁을 한 내용을 계약서류 및 투자설명서에 기재하여야 하며, 업무위탁 내용 변경시 투자자에게 통보하여야 한다.

재위탁(재하청)은 본래 원칙적으로 금지되었고, 예외적으로 가능한 경우를 시행령에 규정하고 있었으나, 역시 2020년 4월의 자본시장법 개정에 따라 '위탁자가 동의하는 경우' 원칙적으로 허용하는 것으로 대폭 자유화되었다.

13 본질적 업무 중 핵심업무'의 예로는 투자매매업에서 증권의 인수, 집합투자업에서 집합투자재산의 운용 · 운용지시 등이 있다.

14 금융위원회(2019. 5. 27, 2020. 4. 29), 개정된 자본시장법은 공포 후 1년 후부터 시행된다.

15 수탁자가 외국 금융투자업자인 경우, 그 외국 금융투자업자의 자격요건 증명을 업무위탁 보고시 제출해야 한다.

<표 II-1> 금융투자업자 업무위탁계약 포함 사항

<table>
<tr><th>법(제42조 제2항)</th><th>시행령(제46조 제2항)</th><th>금융투자업규정
(제4-4조 제2항)</th></tr>
<tr><td>– 위탁 업무의 범위</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td>– 수탁자의 행위제한에 관한 사항</td></tr>
<tr><td>– 위탁하는 업무의 처리에 대한 기록 유지에 관한 사항</td></tr>
<tr><td>– 투자자보호, 건전한 거래질서를 위하여 필요한 사항</td><td rowspan="2">– 업무위탁계약의 해지에 관한 사항
– 위탁보수 등에 관한 사항
– 이해상충방지체계 등</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">– 이해상충방지체계
– 수탁자의 정보이용 제한
– 수탁자에 대한 관리·감독
– 위탁업무에서 발생하는 자료에 대한 위탁 금융투자업자의 소유권과 당해 금융투자업자의 물적 설비 및 지적재산권 등의 이용 조건
– 투자자정보 보호
– 업무의 연속성을 확보하기 위한 백업시스템 확보 등 비상계획
– 면책조항, 보험가입, 분쟁해결
– 수탁자의 책임한계
– 검사당국의 검사 수용의무
– 업무 재위탁의 제한
– 준거법 및 관할법원 (외국 업무위탁의 경우)
– 기타 위험관리 등을 위하여 필요한 사항</td></tr>
</table>

금융투자업의 업무위탁을 자본시장법에 별도로 규제하게 된 동기는 전술한 바와 같이 금융투자업 업무위탁에서 자율의 폭을 대폭 넓히자는 취지에서 비롯되었다. 그러나 실제로는 여전히 업무위탁 금지 업무를 시행령에서 열거하고, 재위탁을 원칙적으로 금지하는 등 열거주의에서 벗어나지 못한 부분이 존재하였고, 타 금융업권은 금융위원회 규정의 규율을 받는 데 비해 법의 규율을 받는 등 금융투자업의 업무위탁에 대한 규제가 오히려 더 경직적이었다고 볼 수 있다. 최근의 자본시장법 개정은 이러한 상황에서 벗어나고자 그동안 제시된 의견들을 반영하여 상당한 개선을 이룬 것으로 평가할 수 있다.

나. 금융투자업 이외의 금융업: 업무위탁규정

은행, 보험 등 금융투자업을 제외한 여타 금융업의 업무위탁에 대해서는 업무위탁규정이 적용된다.[16] 본 규정에서는 업무위탁을 '금융기관이 인가 등을 받은 금융업을 영위하기 위하여 제3자의 용역 및 시설 등을 계속적으로 활용하는 행위'로 정의하고 있으며, 후선업무와 관련한 단순집행업무(예: 인사관리, 총무, 법률, 세무), 전산설비 · 시스템(프로그램) 구입 및 유지보수 등 관리 차원의 단순집행업무 등 금융업 영위와 직접적으로 관계되지 않은 위탁계약을 규율 대상에서 제외하고 있다.[17] 따라서 금융감독원이 정하는 바에 따라 보고의무 없이 개별 금융회사가 자유롭게 업무위탁을 할 수 있다는 점에서 보고의무에서 제외되는 업무에 관한 사항을 정하고 있지 않은 자본시장법보다 유연하다고 볼 수 있다.

업무위탁규정 역시 'negative system'에 따라 업무위탁이 금지되는 경우를 정하고 있는데, 여기에는 인가 등을 받은 금융업의 본질적 요소를 포함하는 경우(예: 은행의 예금계약 체결, 대출심사 및 승인)[18], 관련 법령에서 금융회사가 직접 수행하도록 의무를 부여하고 있는 경우, 금융회사의 건전성 · 신인도를 크게 저해하거나 금융질서의 문란 및 금융이용자의 피해 발생이 심히 우려되는 경우가 포함된다.

16 금융지주회사 및 보험회사의 업무위탁에 대해서는 각각 금융지주회사법 및 보험업법의 적용을 받는 부분이 일부 존재한다.

17 단 후선업무 중에서도 금융업의 본질적 요소를 포함하거나 중요 경영판단 사항 등 의사결정을 요하는 업무는 금감원 보고절차를 통해 적합성을 검증받은 경우에 위탁이 가능하다. 예를 들어 후선업무 지원 관련 전산시스템 개발·운영 등에 관한 위탁은 금융업의 본질적 요소 포함 여부, 고객정보 유출 가능성 및 금융회사의 건전성에 미치는 파급효과 등을 고려하여 금융감독원이 위탁가능 여부를 판단하며, 따라서 보고가 필요하다.(금융감독원, 2018a)

18 인가 정책의 형해화를 방지하기 위한 것이다.

재위탁은 위탁자의 동의 하에 원칙적으로 허용되며, 이는 개정된 자본시장법과 동일하다. 또한 업무위탁의 실제 개시 7 영업일 이전까지 위탁계약의 내용(사본)과 업무위탁 운영기준 등을 첨부하여 보고하도록 규정한 것도 자본시장법과 동일하다. 또한 위탁의 내용이 당해 금융기관 또는 동일한 금융업을 영위하는 다른 금융기관이 금융감독원장에게 보고한 내용과 동일한 경우, 해당 금융기관이 이미 보고한 내용을 일부 변경하는 경우로 해당 내용이 경미한 경우, 동일한 수탁자에게 반복 · 지속적으로 업무위탁이 이루어진 경우로서 최초 업무위탁시에 사전보고가 이루어진 경우 등에는 사후보고가 허용된다.

다. 혁신적 금융서비스에 대한 특례: 금융혁신지원특별법

최근의 급속한 기술 발전, 특히 컴퓨터와 정보통신 기술을 중심으로 한 IT의 발전은 금융업에도 큰 영향을 끼치고 있으며, 금융상품이나 금융서비스가 만들어지고 제공되는 방식을 근본적으로 변화시키고 있다. 기술과 금융의 결합을 의미하는 '핀테크(fintech)'는 최근 가장 많은 관심을 받는 산업의 한 영역이 되었다. 이러한 추세를 반영하고 혁신적 금융서비스의 개발과 발전을 촉진하기 위하여 정부는 '금융규제 테스트베드 도입방안'을 통하여 일정한 요건을 충족하는 신규금융서비스 개발업체에게 '지정대리인' 자격을 부여하고, 금융회사로부터 본질적 업무를 위탁받아 영업할 수 있도록 허용한다는 내용을 발표하였다.[19] 이에 따라 업무위탁이 금지되는 본질적 업무의 범위를 축소하는 업무위탁규정 개정이 이루어졌고[20], 이후 이러한 내용을 담은 금융혁신지원특별법이 2018년 12월 31일에 제정되어 3개월 후인 2019년 4월 1일부터 시행되었다.

금융회사는 금융서비스를 보다 혁신적으로 제공하기 위하여 동법에 의하여 금융위원회의 지정을 받은 자(지정대리인)에게 시범운영에 필요한 업무위탁을 할 수 있다(제25조). 동법에 의하면 '혁신금융서비스'는 제4조에 따라 금융위원회가 지정하며, 지정 유효기간은 2년이다. 그리고 혁신금융서비스를 제공하려는 자[21]는 금융위원회에 지정대리인 신청을 할 수 있고, 금융회사는 지정대리인과 혁신금융서비스의 시범운영을 위한 업무위탁 계약을 체결한 경우 금융위원회에 보고하여야 하며, 업무위탁 기간은 2년 이내이다. 2018년 5월 금융규제 테스트베드 제도가 시행된 후 2020년 9월까지 123건의 혁신금융서

19 금융위원회(2017. 3. 20)

20 금융위원회(2017. 11. 13)

21 금융회사 및 국내에 영업소를 둔 상법상의 회사가 포함된다(제5조 제1항).

비스, 31개의 지정대리인이 지정되었다.[22]

라. 금융회사의 정보처리 업무: 정보처리업무위탁규정

정보처리업무위탁규정은 금융회사의 정보처리 업무의 위탁에 관한 사항을 규율하며, 금융투자회사를 비롯한 모든 금융회사가 규율 대상이 된다. 본 규정에서 '금융거래정보'는 금융회사가 고객과 금융거래행위를 함으로써 거래상대방인 고객으로부터 수집한 해당 고객의 정보 및 금융거래행위의 결과로 생성된 고객의 거래내역 정보를 의미한다(제2조 제4항). 또한 '정보처리'는 금융회사가 전산설비를 활용하여 정보의 수집 · 생성 · 기록 · 저장 · 보유 · 가공 · 편집 · 검색 · 출력 · 정정 · 복구 · 이용 · 제공 · 공개 · 파기 등의 행위를 하는 것을 가리킨다(제2조 제5항). '정보처리의 위탁'은 금융회사가 자신의 정보처리 업무를 제3자로 하여금 계속적으로 처리하도록 하는 행위로 정의된다(제2조 제6항).

본 규정 역시 정보처리 업무위탁을 원칙적으로 허용하고, 금지되는 경우를 명시하고 있는데, 각 금융 관련 법령에서 업무위탁을 금지하는 경우, 최근 3년 이내에 금융이용자의 정보관리 등 검사와 관련한 사항으로 기관경고 이상의 제재 또는 형사처벌을 2회 이상 받은 경우, 업무위탁으로 인하여 금융회사의 건전성 또는 신인도를 크게 저해하거나 금융질서의 문란 또는 금융이용자의 피해 발생이 심히 우려되는 경우가 여기에 해당한다. 자본시장법 및 업무위탁규정과 마찬가지로 재위탁은 원칙적으로 허용된다.

한편 정보처리 업무 수탁자는 정보처리 과정에서 이전받은 정보를 당초 위탁의 범위를 초과하여 다른 목적에 활용할 수 없으나, 다만 해당 정보주체의 동의를 받은 경우에는 동의의 범위 내에서 활용이 가능하다. 또한 위탁회사는 수탁회사가 계약상의 의무를 위반하여 발생하는 정보주체 및 이용자의 손해에 대하여 수탁회사와 연대하여 책임을 진다. 금융회사는 정보 보호를 위하여 각 관련 법령상의 안정성 확보조치를 충실히 이행하여야 하며[23], 안정성 확보조치의 구체적 내용을 홈페이지 등을 통해 공시하여야 한다.

정보처리 업무위탁에서도 금융회사는 실제 업무수행 개시일의 7 영업일 전까지 업무위탁계약서 사본, 업무위탁 운영기준 등을 첨부하여 금융감독원장에게 보고하여야 한다.

22 31개 지정대리인의 기반기술과 제공 서비스를 살펴보면, 빅데이터·인공지능(AI)을 활용한 대출심사 및 시세·담보가치 산정이 22개로 가장 많고, 이 외에 온라인플랫폼 운영, 바이오정보를 활용한 인증·본인확인, 자산관리·금융상품 추천, 보험 접수·심사·지급·환급·변경 일괄 서비스 등이 있다.

23 개인고객 고유식별정보의 암호화, 정보의 국외 이전 방지 등이 포함된다.

그러나 개인고객의 금융거래정보를 제외한 금융거래정보의 처리를 위탁하는 경우에는 실제 업무수행 개시일로부터 10 영업일 이내에 사후보고하면 된다. 그리고 금융거래정보 처리업무의 위탁으로서 해당 금융회사 또는 동일한 금융업을 영위하는 다른 금융회사가 이미 보고한 내용과 동일한 경우로서 수탁자의 업종이 동일한 경우, 이미 보고한 내용을 일부 변경하는 경우로서 변경되는 내용이 경미한 경우, 금융거래정보 이외의 정보처리 업무를 위탁하는 경우에는 반기별로 사후보고가 허용된다.

III. 주요국 공적 기관의 아웃소싱 관리 지침

1. 미국
2. 유럽(EU)
3. 영국
4. 싱가포르

III. 주요국 공적 기관의 아웃소싱 관리 지침

본 장에서는 미국, 유럽(EU), 영국, 싱가포르의 금융 관련 공적 기관들이 제시한 금융회사의 효과적인 아웃소싱 리스크 관리를 위한 지침(guidance) 또는 가이드라인의 핵심적 내용을 정리한다.

1. 미국

미국은 금융회사의 아웃소싱에 대하여 법령으로 규제하고 있지 않으며, 대신 다양한 공적 기관들이 금융회사의 효과적인 아웃소싱 리스크 관리를 위한 지침을 마련하여 제시하고 있다. 본 장에서는 FRB(2013), FDIC(2008), OCC(2013), FFIEC(2004)의 주요 내용을 정리한다.[24]

먼저 지침의 목적에 대하여 FRB(2013)는 '아웃소싱의 잠재적 리스크를 설명하고, 효과적 리스크 관리를 위한 금융회사 리스크 관리 프로그램이 갖춰야 할 주요 내용을 제시하는 것', FDIC(2008)는 '이사회 · 최고경영진이 제3자 공급업체를 적절하게 감독하고 리스크를 관리하기 위한 틀(framework)을 제공하는 것', OCC(2013)는 '미국 은행들에게 제3자 공급업체 관계와 관련된 리스크를 평가 · 관리하기 위한 지침을 제공하는 것', FFIEC(2004)는 '금융회사가 IT 부문을 아웃소싱하는 경우 계약-운영-감시에 이르는 리스크 관리 절차에 대한 지침을 제공하는 것'으로 언급하고 있다.

아웃소싱의 범위에 대해서는 FRB(2013)가 언급하고 있는데, 금융회사의 핵심업무 뿐 아니라 IT 서비스, 회계 · 성과관리 · 내부감사 · 인사 · 자산관리 · 조달 등의 운영업무까지도 아웃소싱이 가능하여, 사실상 제한을 두지 않고 있다.

이 4개 기관의 지침들은 공통적으로 아웃소싱 리스크 관리에 있어서 이사회와 최고경영진의 역할과 책임을 명시적으로 강조한다. 금융회사의 이사회와 최고경영진은 아웃소싱 활동이 안정적이고 건전하게 이루어질 수 있도록 적절한 정책을 수행할 책임을 가지며, 구체적으로 아웃소싱과 관련된 정책은 이사회에 의해 승인되어야 하고, 최고경영진

24 OCC는 Office of the Comptroller of the Currency, FFIEC는 Federal Financial Institutions Examination Council의 약자이다.

은 이사회가 승인한 정책을 적절하게 실행하는 책임을 진다(FRB, 2013). FDIC(2008)는 지침의 목적 자체가 이사회 · 최고경영진을 위한 것임을 명시하고 있고, 특히 OCC(2013)는 아웃소싱 관리에 있어서 이사회와 최고경영진 각각의 책임을 상세하게 나열하고 있으며 그 내용은 <표 III-1>과 같다.

<표 III-1> 아웃소싱 관리에 있어서 이사회와 최고경영진의 책임

이사회	최고경영진
– 제3자 공급업체 관계 및 리스크 관리 전체 프로세스와 은행의 전략적 목표, 리스크 감내 정도와의 일관성 확보 – 제3자 공급업체 리스크 관리 프로세스를 통할하는 은행의 리스크 정책 승인 – 핵심적 활동을 아웃소싱 할 때 관리 계획의 검토 및 승인 – 핵심적 활동을 수행할 제3자 공급업체에 대한 실사 및 경영진의 권고 검토 – 핵심적 활동이 포함된 아웃소싱 계약의 승인 – 경영진의 상시 모니터링 결과의 검토 – 심각한 성과 저하에 대하여 경영진의 적절한 처방 조치 확보 – 정기적으로 이루어지는 독립적 검토 보고의 검토	– 은행의 제3자 공급업체 리스크관리 프로세스 개발 및 실행 – 제3자 공급업체 리스크관리 프로세스를 통할하는 은행의 리스크 정책 수립 – 아웃소싱 계획 수립, 핵심적 활동의 포함 여부 파악, 포함된 경우 이사회에 보고 – 적절한 실사 확보 – 계약의 검토 및 승인, 핵심적 업무가 포함된 경우 이사회 승인 – 제3자 공급업체에 대한 상시 모니터링 확보 – 전체 생애주기에 걸친 적절한 문서화 확보 – 정기적으로 독립적 검토가 이루어지도록 담보, 검토 결과의 분석, 적절한 조치 시행, 그 결과를 이사회에 보고 – 제3자 공급업체 관리 담당 직원의 책임성 확보 – 기대수준에 못미치거나, 은행의 전략적 목표와 일피하지 않는 제3자 공급업체 관계의 종료 – 전사적 리스크 관리 감독

자료: OCC(2013)

FRB(2013)와 FDIC(2008)는 아웃소싱으로부터 발생 가능한 잠재적 리스크의 유형을 정리하여 제시하고 있는데, 그 내용은 <표 Ⅲ-2>와 같다.

<표 Ⅲ-2> 아웃소싱으로부터 발생 가능한 리스크 유형

준법 리스크 (compliance risk)	공급업체의 서비스, 제품, 활동이 미국 내 해당 법률과 규정을 준수하지 않을 경우 발생
집중 리스크 (concentration risk)	서비스나 제품이 제한된 지리적 위치 또는 한정된 수의 공급업체에게 아웃소싱된 경우에 발생
평판 리스크 (reputational risk)	공급업체의 행동이나 낮은 성과로 인해 소비자들이 금융회사에 대해 부정적 의견이 형성되는 경우 발생
국가 리스크 (country risk)	금융회사가 국외에 있는 공급업체와 관련되어 해당 국가의 경제, 사회, 정치적 상황 등에 노출되는 경우 발생
운영 리스크 (operational risk)	공급업체가 부적절(실패)한 내부 프로세스나 시스템 또는 외생적 사건, 임직원 실수로 인해 금융회사에 손실을 입히는 경우 발생
법적 리스크 (legal risk)	공급업체가 금융회사를 법적비용과 소송 가능성 등에 노출시킴으로써 발생
전략적 리스크 (strategic risk)	아웃소싱 의사결정이 금융회사의 전략적 목표와 일치하는 방향으로 이루어지지 않는 경우 발생
거래 리스크 (transaction risk)	공급업체의 불충분한 설비, 기술적 실패, 실수, 사기 등으로 서비스나 제품의 인도(delivery)에서 문제가 생기는 경우 발생
신용 리스크 (credit risk)	공급업체가 금융회사와의 계약상 조건을 만족하기 못하거나 약정된 재무적 성과를 달성하지 못하는 경우 발생

자료: FRB(2013), FDIC(2008)

아웃소싱 관리 지침의 핵심은 아웃소싱 리스크를 관리하기 위하여 금융회사가 갖추고 실행해야 할 프로세스를 구체적으로 설명하는 부분으로, 4개 기관의 지침은 대동소이한 내용을 담고 있다. 아웃소싱 리스크 관리 프로세스의 첫번째 단계는 '리스크 평가'로서, 결정된 아웃소싱이 회사의 전략적 방향과 일치하는지 여부, 아웃소싱에 따른 위험 · 편익 분석, 비용효과 평가, 자사의 아웃소싱 관리 능력에 대한 평가 등이 포함된다.

두번째 단계는 공급업체 후보들에 대한 실사(due diligence) 및 공급업체의 선정이다. 실사를 통해 확인해야 할 항목에는 공급업체의 재무정보(재무제표 등), 아웃소싱하려는 서비스 또는 업무를 수행하고 모니터링할 수 있는 경험 및 능력, 평판, 공급업체 소유주

및 지배주주의 평판, 서비스 철학 · 품질에 대한 강조 · 효율성 · 고용정책 등을 포함한 기업전략 및 목표, 소송 · 제재 여부, 현재 상태로 요구되는 서비스를 제공할 수 있는지 또는 추가적 투자가 필요한지 여부, 재아웃소싱(재하청) 업체의 사용 여부, 내부통제 · 데이터 보안 · 개인정보 보호 관련 사항, 관련 소비자 보호 및 시민 권리와 관련된 법령 · 규제에 대한 지식, 경영정보시스템의 충분성, 필요한 보험 가입 여부 등이 포함된다.

실사를 거쳐 공급업체가 선정된 다음 이어지는 세번째 단계는 선정된 공급업체와 아웃소싱 계약을 맺는 것이다. 4개 기관의 지침 모두 아웃소싱 계약은 서면(written)으로 체결되어야 하며, 아웃소싱 계약을 치밀하게 설계하여 체결하는 것이 전체 리스크 관리 프로세스에서 가장 중요한 단계임을 강조하면서 계약에 필수적으로 포함되어야 할 사항을 매우 세부적인 수준까지 열거 · 제시하고 있다. <표 Ⅲ-3>은 이 중에서 FDIC(2008)에서 제시된 계약 포함 사항을 정리하여 보여준다. <표 Ⅲ-3>에서 제시된 사항 외에 FRB(2013)는 공급업체의 보험 가입 의무, 공급업체가 국외에 소재하는 경우 적용 법규 및 관할권(jurisdiction) 관련 사항, 재아웃소싱을 허용하는 경우의 권리 · 책임 등에 관한 사항도 계약에 포함되어야 하는 사항으로 제시하고 있다.

<표 III-3> 아웃소싱 계약에 포함되어야 할 사항 (미국)

범위	계약기간, 공급되는 서비스/제품의 빈도/형식/제원, 소프트웨어 지원/유지, 준법감시, 고객공시, 보험 커버리지, 금융회사 부지/장비 사용조건, 재하청 허가/금지 여부, 성과 모니터링, 면책 등의 사항에 대한 금융회사와 공급업체 각각의 권리와 책임을 명확하게 규정하여야 함
비용 및 보수	모든 정액보상(fixed compensation), 변동요금(variable charges), 일회성 수수료 등을 포함한 보수 구조를 규정하여야 함
성과표준	공급업체의 성과를 측정하고 보상 결정의 기준을 사용하기 위하여 명확하게 정의된 성과표준이 마련되어야 함
보고	공급업체가 금융회사에 제출하는 경영정보보고의 유형 및 보고주기를 규정하여야 함
감사	공급업체가 금융회사에 제출하는 감사보고서의 유형과 주기, 공급업체에 대한 성과 모니터링을 위한 금융회사의 감사 권한을 명시해야 함
기밀유지 및 보안	계약에 의하여 지정된 기능을 수행하는 데 필요한 경우를 제외하고는 공급업체가 금융회사의 정보를 사용하거나 공개하는 것을 금지해야 함
고객 불만	금융회사가 공급업체를 통하여 고객으로부터 접수한 모든 불만에 대한 응대 의무가 누구에게 있는지를 명확하게 규정하여야 함
사업재개 및 비상계획	운영상의 실패(operational failure) 발생시 계약에 의하여 공급되는 서비스의 지속에 대한 공급업체의 책임을 명시하여야 함
계약불이행 및 종료	불이행의 구성 요건, 복구 방법, 계약의 종료 권한 관련 사항 등이 규정되어야 함
분쟁 해결	문제를 적절히 해결하기 위한 분쟁해결 절차를 포함하여야 하며, 분쟁해결 기간 중에도 아웃소싱 공급은 지속되어야 한다는 것을 명시해야 함
소유권 및 라이센스	소유권 이슈 및 공급업체가 금융회사의 데이터, 장비, 소프트웨어, 지식재산, 저작권 등록자료 등을 사용할 수 있는 권리와 관련된 사항을 규정해야 함
면책	공급업체[금융회사]의 부주의로 인한 책임(liability)으로부터 금융회사[공급업체]가 피해를 입지 않도록 절연해야 함
책임 한도	책임의 한도를 계약에 명시할 수도 있음

자료: FDIC(2008)

실사를 거쳐 공급업체가 선정되고 아웃소싱 계약이 체결되어 공급업체가 정해진 아웃소싱 서비스 또는 업무의 제공을 개시하면, 공급업체가 계약의 내용을 실제로 이행하고 있는지를 감독(supervision) 또는 모니터링하는 것이 아웃소싱 관리 프로세스의 네번

째 단계이다. 금융회사는 공급업체가 제공하는 제품 · 서비스에 대한 충분한 품질관리 및 공급업체에 대한 적절한 감독을 항상 유지해야 한다. 이사회는 최소 1년에 1회 중요한 아웃소싱 계약을 승인 · 감독 · 검토하고, 아웃소싱 프로그램에 중요한 변화가 있는 경우 서면합의 내용을 검토해야 하며, 최고경영진은 공급업체의 운영이 계약대로 이루어지고 있는지 검증해야 한다(FDIC, 2008). 또한 공급업체의 아웃소싱 계약상의 의무 이행 여부를 효과적으로 모니터링하기 위해서는 공급업체에 대한 합당한 성과표준 · 지표가 마련되어야 하며, 금융회사는 공급업체에 대한 감독 및 관리 책임을 지는 직원이 책임 이행에 필요한 적절한 수준의 전문지식과 능력을 갖추도록 해야 한다(FRB, 2013). FDIC(2008)은 보다 구체적으로 공급업체의 성과 모니터링에서 확인해야 할 사항들을 <표 III-4>와 같이 열거하고 있다.

<표 III-4> 공급업체 성과 모니터링 확인 사항

- 공급업체와의 관계의 전반적 효과성(effectiveness) 및 전략목표와의 일관성 평가
- 공급업체가 업무 수행에 필요한 허가, 등록 등 법적 요건을 갖추고 있는지 여부
- 최소 1년에 1회 공급업체의 재무상태 평가
- 보험 커버리지의 충분성 검토
- 공급업체의 타인에 대한 재무적 의무(financial obligation) 이행 확인
- 감사보고서 검토
- 공급업체의 내부통제 및 보안 정책의 충분성 및 준수 정도 검토
- 준법 여부 모니터링
- 공급업체의 비상계획(contingency plan) 검토
- 공급업체 핵심인력 변동의 영향 평가
- 계약상의 요건 및 표준에 따른 공급업체의 성과 관련 보고서 검토
- 금융회사 및 공급업체 직원에게 제공된 훈련의 충분성 검토
- 공급업체와 고객 간의 직접 접촉(direct interaction) 테스트
- 공급업체의 상품/서비스에 대한 고객 불만 및 불만처리 검토

자료: FDIC(2008)

금융회사는 아웃소싱 공급업체가 더 이상 계약된 제품 · 서비스를 공급할 수 없는 경우를 대비하여 업무 연속성(business continuity)을 위한 대안조치를 포함한 비상계획(contingency plan)을 마련해야 한다. 업무 연속성을 위한 비상계획은 특히 IT 아웃소싱

에 초점을 둔 FFIEC(2004)에서 강조되고 있다. FFIEC(2004)에 의하면 금융회사는 업무 연속성 계획의 효과성을 위하여 업무 연속성에 대한 공급업체 모니터링을 지속적으로 실시해야 한다. 금융회사 경영진은 공급업체가 정기적으로 업무 연속성 계획을 테스트하도록 하고 이에 대한 결과를 보고하도록 함으로써 업무 연속성 계획을 적절하게 유지 · 관리할 책임이 있다. IT 아웃소싱에 있어서 외부적 요인에 의한 사건이 발생한 경우, 중요 데이터 및 관련 처리 기능에 대한 적절한 백업절차가 수립되어 있는지 확인해야 한다. 그 외에 업무 연속성과 관련하여 금융회사가 공급업체에 대하여 고려하고 점검해야 할 사항은 <표 Ⅲ-5>와 같다.

<표 Ⅲ-5> 업무 연속성 관련 공급업체 점검·고려 사항

직원 충원	공급업체는 복구 사이트에서 운영을 적시에 재개할 수 있도록 적절한 현장 기술지원을 제공할 수 있는 충분한 지식을 보유한 직원을 배치해야 함
처리 시간	공급업체는 복구를 위한 충분한 시간을 할당해야 함
접근 권한	긴급상황 발생 시 공급업체는 금융회사의 해당 사이트 접근 권한을 보장해야 함
하드웨어/ 소프트웨어	복구 사이트에는 호환되는 하드웨어 및 소프트웨어가 설치되어 있어야 함
보안 통제	금융회사는 복구 사이트에서 적절한 물리적, 논리적 보안 통제가 유지되도록 해야 함
테스트	정기적 테스트를 위한 금융회사의 복구 사이트 접근 권한이 아웃소싱 계약에 명시되어야 함
데이터 기밀유지	금융회사는 공급업체가 고객 데이터의 기밀을 유지하도록 충분한 통제를 확보해야 함
통신	공급업체는 복구 사이트가 적절한 통신 서비스(음성 및 데이터)를 갖추도록 해야 함
상호 합의	금융회사는 복구 사이트를 위해 다른 기관과 계약을 체결한 경우에도 동일한 사항들을 점검·고려하여야 함
공간	복구 사이트는 금융회사의 관련 직원을 수용할 수 있는 충분한 공간이 있어야 함
인쇄 설비	복구 사이트에는 충분한 인쇄 설비가 갖추어져 있어야 함
접촉점	금융회사 경영진은 사고(disaster) 선언, 복구 사이트 가동 절차를 숙지하고 있어야 하며, 복구 사이트와 관련된 담당자 명단과 연락처를 현행으로 유지해야 함

자료: FFIEC(2004)

2. 유럽(EU)

2006년 CEBS(Committee of European Banking Supervisors)는 EU 회원국의 금융회사들을 대상으로 아웃소싱에 관한 지침을 발표하였다. 이후 아웃소싱 방식이 지속적으로 발전해온 가운데 핀테크의 중요성과 활용성이 높아짐에 따라, EBA(European Banking Authority)는 2017년 12월 클라우드 서비스를 아웃소싱하는 경우 준수해야 할 권고사항(EBA, 2017)을 새롭게 발표하였고, 2019년 2월에는 2006년 CEBS 아웃소싱 지침과 2017년 클라우드 서비스 아웃소싱 권고사항을 통합하여 새롭게 개정된 아웃소싱 지침(EBA, 2019)을 공표하였다.[25] 동 지침은 EBA의 권한 범위에 해당하는 모든 금융회사에 적용된다. 본 절에서는 EBA(2019)의 핵심 내용을 정리하여 소개한다.

미국 공적 기관들의 아웃소싱 지침들과 마찬가지로 EBA(2019) 역시 아웃소싱이 가능한, 또는 불가능한 업무를 규정하고 있지는 않다. 대신에 미국 기관들의 지침과는 달리 아웃소싱 결정에 앞서 금융회사가 아웃소싱하고자 하는 업무의 중요도를 평가할 것을 요구하고 있다. 업무의 중요도를 평가함에 있어서 고려해야 할 요소로는 ① 해당 업무가 승인된 은행업무 또는 지불서비스와 직접적으로 연결되어 있는지의 여부 ② 아웃소싱 공급업체가 아웃소싱된 업무를 제공하지 못할 경우 금융회사의 재무상태, 금융회사 사업의 연속성 · 복원력, 금융회사의 운영 리스크 · 평판 리스크, 복구 및 업무 연속성 등에 미치는 영향 ③ 잠재적 리스크의 식별 · 관리 · 모니터링, 준법, 감사 등의 수행에 미치는 영향 ④ 고객 서비스 · 데이터 보안 등에 미치는 영향 등이 포함된다.

또한 EBA(2019)는 아웃소싱 리스크 관리를 위한 금융회사의 내부통제 체계가 갖추어야 할 요구사항도 상세하게 규정하고 있다. 금융회사는 아웃소싱으로 인한 모든 잠재적 리스크를 식별 · 평가 · 모니터링 · 관리해야 한다. 모든 아웃소싱 계약, 내부적 리스크 관리 체계와 책임은 문서화되어야 한다. 금융회사는 특별히 ICT 및 핀테크 관련 리스크의 식별 · 평가 · 관리, 데이터 및 기타 정보에 대한 기밀유지에 대해서는 반드시 명시적 조치를 취해야 한다. 이 외에도 금융회사는 업무 연속성에 관한 계획을 수립 · 관리해야 하고, 아웃소싱 활동에 대한 내부감사가 이루어져야 하며, 모든 아웃소싱 관련 정보는 현행화 · 문서화하여 유지 · 보존해야 한다.

25 EBA(2019)의 시행과 동시에 CEBS(2006)과 EBA(2017)은 폐지되었다.

미국 공적 기관들의 지침과 마찬가지로 EBA(2019) 역시 아웃소싱 계약은 서면으로 만들어져 체결되어야 할 것을 요구하고 있으며, 계약에 필수적으로 포함되어야 하는 사항은 <표 Ⅲ-6>에 정리되어 있는데, 그 내용 역시 대동소이하다.

한편 핀테크가 급속하게 성장하는 환경 변화를 반영하여 2018년 7월 EBA는 감독당국과 업계 내의 핀테크에 대한 인식 제고를 위하여 보고서(EBA, 2018)를 발표하였는데, 이 보고서에서 EBA는 금융회사가 자사 업무를 클라우드 서비스 공급업체(Cloud Service Provider: CSP)에 아웃소싱하는 경우의 장점, 즉 아웃소싱의 동인과 잠재적 리스크를 언급하고 있다. EBA(2018)에 의하면 금융회사는 비용절감, 규모의 경제 등의 이유로 핵심 및 비핵심 업무를 제3자 CSP에 아웃소싱한다. 특히 CSP 아웃소싱은 비용 측면에서 가장 효율적인 것으로 나타난다. CSP는 전문업체로서 자신의 IT 운영을 최적화할 수 있으며, 안정적인 사용패턴을 보이는 금융회사는 사내 자체 개발보다 아웃소싱할 때 비용을 절감할 수 있다. 그리고 서비스 수요가 변할 때 이 변화를 수용하기 위하여 금융회사 자신의 인프라를 조정할 필요 없이 유연하게 대응할 수 있다. 또한 전문업체에 의한 클라우드 서비스가 금융회사 자신이 개발한 클라우드 서비스에 비하여 고품질일 가능성이 높다는 것도 장점으로 들 수 있다.

반면 금융회사가 제3자 CSP에 아웃소싱하는 경우 다양한 측면에서 리스크가 증가할 수 있음을 EBA(2018)는 지적하고 있다. 보안 통제, 법률 · 규제 준수에 있어서 제3자 CSP 측에서 문제가 발생할 수 있고, 다수의 금융회사가 동일한 CSP를 이용하는 경우 집중 리스크가 높아질 수 있으며 이는 다시 거시건전성에도 영향을 미칠 수 있다. CSP가 전세계적으로 서비스를 제공하는 글로벌 사업자인 경우에는 고위험 지역 · 국가에서 발생하는 리스크가 금융회사의 운영 리스크 또는 평판 리스크에 부정적 영향을 미칠 수도 있다. 그리고 금융회사의 CSP에 대한 의존도가 너무 높아지면 금융회사가 CSP에 종속되는 'hold-up' 또는 'vendor lock-in' 문제에 빠질 수도 있다.

<표 III-6> 아웃소싱 계약에 포함되어야 할 사항 (EU)

금융회사와 공급업체의 권리·의무	– 아웃소싱 대상 업무에 대한 명확한 설명 – 아웃소싱 계약기간, 시작 및 종료 일자 – 아웃소싱 계약 관련 적용 법률 – 계약 당사자들의 재무적 의무 – 아웃소싱이 제공되는 위치(국가 또는 지역), 데이터 보관·처리 위치 – 데이터 접근·이용·무결성·보안 관련 사항 – 공급업체 성과표준 및 모니터링 관련 사항 – 공급업체의 서비스 제공 능력에 중요한 영향을 미칠 수 있는 사건이 발생한 경우 보고의무 – 법률·규제 준수에 영향을 미칠 수 있는 경우 공급업체의 내부감사 기능에 대한 보고 – 공급업체의 보험 가입 관련 사항 – 공급업체의 운영 부실 또는 중단의 경우 금융회사의 데이터 접근권 보장 사항 – 중요업무를 아웃소싱하는 경우 공급업체를 감독·감사할 수 있는 금융회사 및 감독당국의 권리
재아웃소싱	– 중요업무의 재아웃소싱 허용 여부를 명시해야 하며, 재아웃소싱의 경우 해당 내용 문서화 – 재아웃소싱 공급업체가 모든 법률·규제·계약상의 의무를 이행하고, (원) 공급업체 계약사항과 동일하게 재아웃소싱 공급업체에 대한 감독·감사 권한을 부여받은 경우에만 재아웃소싱 허용
데이터 보안	– 공급업체에 대한 데이터·시스템 보안 요구사항을 명시하고, 이 요구사항의 준수여부를 지속적으로 모니터링
정보접근 및 감사 권한	– 금융회사 및 감독당국이 아웃소싱된 서비스·기능이 정상적으로 제공되는지 검토·감시할 수 있는 권한 보장
아웃소싱 감독	– 금융회사는 위험기반 접근법에 따라 모든 아웃소싱 계약과 관련하여 공급업체의 성과를 지속적으로 모니터링
계약종료 및 출구전략	– 공급업체가 법률·규정·계약을 위반하는 경우, 아웃소싱된 서비스의 품질을 저하시킬 수 있는 장애요소가 발견된 경우, 정보의 관리와 보안에 취약점이 발견된 경우, 감독당국의 지시가 있는 경우 등에 계약을 종료할 수 있는 권한 – 금융회사는 공급업체로부터 데이터를 삭제하고, 이 데이터를 새로운 공급업체 또는 금융회사로 이전시키는 등 서비스의 지속적 제공을 보장할 수 있도록 대체방안과 전환계획을 수립해야 함 – 출구전략은 충분히 테스트되어야 하며 문서화되어야 함

자료: EBA(2019)

3. 영국

영국 역시 법률에서 금융회사의 아웃소싱을 제한하고 있지 않으며, 감독규정에 해당하는 FCA(Financial Conduct Authority) Handbook의 SYSC(Senior Management Arrangements, System and Controls) 8.1에서 금융회사의 아웃소싱에 관한 일반적인 내용과 아웃소싱 리스크 관리에 대한 규정(rules)과 지침(guidance)을 제시하고 있다. 그리고 FCA와 PRA(Prudential Regulation Authority)가 공동으로 SYSC 8.1을 통하여 금융회사의 아웃소싱을 규율한다.

SYSC 8.1에 의하면 금융회사의 아웃소싱은 전반적으로 허용되나 운영 리스크가 과도하게 증가하지 않도록 적절한 조치를 취해야 하며, 핵심업무 기능의 아웃소싱으로 인해 내부통제의 질이 떨어지거나 감독당국의 모니터링 능력이 현저하게 저하되는 경우에는 아웃소싱이 허용되지 않는다. 금융회사는 핵심(critical and important)업무를 아웃소싱하는 경우 운영 리스크를 효과적으로 관리할 수 있는 내부통제 메커니즘을 갖추어야 한다. 또한 금융회사는 아웃소싱을 추진할 때 <표 Ⅲ-7>에 정리된 요건들이 충족되는지의 여부를 확인하는 절차를 취해야 한다. 영국 역시 금융회사의 아웃소싱 계약은 서면으로 체결되어야 함을 규정하고 있고, 아웃소싱을 하는 경우 감독당국(FCA, PRA)에 사전 보고할 것을 요구하고 있다.

<표 III-7> 아웃소싱 추진 시 확인해야 할 사항 (영국)

- 공급업체가 아웃소싱 받은 업무를 전문적·안정적으로 수행하기 위한 능력과 역량 및 권한을 보유하고 있는지의 여부
- 공급업체의 아웃소싱 받은 업무 수행을 평가하기 위한 성과표준
- 공급업체가 아웃소싱 받은 업무를 효과적으로 수행하고 관련 리스크를 관리하고 있는지의 여부
- 공급업체가 관련 법규·규정을 준수하면서 업무를 수행하지 못한다고 판단되는 경우 조치 사항
- 아웃소싱 공급업체를 효과적으로 감독하고 관련 리스크를 관리하기 위해 필요한 전문지식을 금융회사가 갖추고 있는지의 여부 및 확보 방안
- 아웃소싱 받은 업무 수행에 중요한 영향을 미칠 수 있는 모든 변화를 금융회사에게 보고할 공급업체의 의무 규정
- 고객 서비스 제공의 지속성과 품질에 영향을 주지 않으면서 아웃소싱을 중단할 수 있는 종료 계획
- 아웃소싱 받은 업무에 관련한 공급업체의 규제당국(FCA, PRA) 협조 의무
- 공급업체의 시설·데이터·자료 등에 대한 금융회사 및 규제당국의 접근 권한 확보
- 금융회사 및 고객 관련 정보에 대한 공급업체의 기밀유지 의무
- 공급업체 백업 설비·절차에 대한 정기적 검사, 복구를 위한 대책 수립

자료: SYSC 8.1.8R

한편 FCA는 2016년 7월, 클라우드 및 IT 서비스 아웃소싱에 관한 지침을 마련하였고, 전 절에서 소개한 EBA(2018)의 권고 및 관련 법률의 변경사항을 반영하여 2018년 7월 클라우드 및 IT 서비스 아웃소싱에 관한 최종 지침(FCA, 2018)을 발표하였다. FCA(2018)는 금융회사가 인터넷을 통해 다양한 형태로 제공되는 IT 서비스를 제3자 공급업체에 아웃소싱하는 경우, 금융회사가 운영 리스크를 효과적으로 식별 · 감독하기 위한 규제 지침을 제시하고 있으며, 주요 내용은 <표 III-8>에 요약되어 있다.

<표 III-8> 클라우드·IT 아웃소싱 지침(FCA, 2018) 주요 내용

업무 중요성 평가	– 핵심(critical or important)업무: 업무 운영상의 결함이나 실패로 인해 인가 조건 및 해당 규제에 대한 의무, 재무성과, 서비스의 건전성·지속성에 큰 영향을 미치는 업무 – 중요(material)업무: 서비스의 취약 또는 실패 시 금융회사의 임계조건을 지속적으로 만족시킬 수 없거나 원칙 준수에 심각한 영향을 미치는 업무 – 중요 운영기능(important operational functions): 업무 수행상의 결함이나 실패로 인해 컴플라이언스·재무실적·건전성에 심각한 영향을 미치는 기능
보고 의무	– 금융회사는 핵심 또는 중요업무의 아웃소싱 계약을 체결하거나 중요한 변경사항이 생긴 경우 FCA에 보고하여야 함
법·규제적 고려 사항	– 복수의 공급업체에 아웃소싱하는 경우 명확하게 문서화된 근거가 갖춰져야 함 – 아웃소싱하려는 업무가 금융회사에게 적합한지 여부 확인 – 아웃소싱 계약 관련 정확한 기록 유지 – 금융회사와 공급업체의 관할지역이 계약에 미치는 영향 확인 – 공급업체가 영국 관할권에 소재하지 않는 경우, 금융회사 및 규제기관의 공급업체 데이터·사업장 접근 권한 보장 – GDPR(General Data Protection Regulation)[26] 준수 관련 요구사항
리스크 관리	– 아웃소싱 관련 리스크의 식별 및 완화를 위한 단계별 리스크 평가 수행 – 리스크 평가 내용 문서화 – 리스크 관리 관련 규정·지침 및 업계의 우수사례 파악 및 참고 – 관할권이 다른 지역이 위치한 경우 리스크에 미치는 영향 검토 – 금융회사가 책임지고 있는 서비스와 관련된 전반적인 운영 리스크 평가 및 관리 – 집중(concentration) 리스크 모니터링 및 대책 마련 – 사업 복구 및 연속성 계획 – 계약 위반 및 기타 부정적 상황이 발생하는 경우 대책 마련
국제적 표준	– 공급업체 실사 및 모니터링 수행 시 ISO 등 국제 표준 준수
공급업체 감독	– 모든 의무의 궁극적 책임은 금융회사에게 있고 이 책임은 공급업체에게 위임할 수 없으며, 금융회사는 수탁자 감독에서 높은 수준의 의무를 이행해야 함 – 금융회사와 공급업체 간 책임과 의무가 시작되고 끝나는 지점 명확화 – 기존 공급업체와의 계약해지 시 필요한 적절한 관리 기술과 자원 확보 – 분쟁 해결을 위한 적절한 조치 확보

26 2018년 5월부터 시행된 EU의 개인정보보호 법령이다.

<표 III-8> 클라우드·IT 아웃소싱 지침(FCA, 2018) 주요 내용(계속)

데이터 보안	– 공급업체에 대한 보안 리스크 평가 – 금융회사의 데이터를 저장·처리·관리할 수 있는 관할권을 규정하는 데이터 상주정책(data residency policy) 마련 및 합의 – 공급업체의 데이터 손실·침해 보고절차 확인, 이 절차가 금융회사의 리스크 수용 범위 및 법적·규제적 의무사항을 충족하는지 확인 – 필요한 경우 데이터 민감도에 따른 데이터 전송·저장·암호화 방법 마련
GDPR	– 금융회사 및 공급업체는 GDPR을 준수해야 함
사업장 방문	– 공급업체의 사업장(business premises) 방문에 관한 규정이 적용되는 금융회사의 경우 해당 계약에 과련 규정이 반드시 포함되어야 함 – 모든 사업장을 방문하여 감독할 필요는 없으며, 효과적인 감독을 위해 어느 사업장을 방문해야 하는지 판단
공급업체 관계	– 금융회사가 최종 공급업체와 직접 계약하지 않는 경우(재아웃소싱), 아웃소싱 대상 업무와 관련된 재아웃소싱 계약 검토 – 금융회사는 최종 공급업체와 직접 계약하지 않더라도 규제요건을 준수할 수 있어야 함 – 공급업체와의 협업 방안 – 공급업체의 서비스와 금융회사의 내부 시스템 또는 기타 제3자 시스템(예: 결제 대행) 간 호환성(interoperability) 확인
변경 관리	– 프로세스와 내부절차가 변경되는 경우 변경 관리를 위한 조치 마련 – 변경 사항에 대한 테스트 수행 방안 수립
사업 연속성	– 예상하지 못한 운영 중단의 가능성과 영향 평가 – 사고 발생 후 복구 조치를 포함하여 사업의 연속성을 유지하기 위한 전략 수립 및 이 전략의 적절성과 실효성에 대한 정기적 테스트 문서화
종료 계획	– 필요한 경우 서비스 제공에 영향을 주지 않고 규정을 준수하면서 아웃소싱을 종료할 수 있어야 함 – 중분히 검증된 종료 계획과 해지 약정 수립·문서화 – 대체 공급업체로의 전환을 비롯한 업무 연속성 유지 방법 마련 – 아웃소싱 종료 시 공급업체 시스템에서 데이터를 삭제하는 방법 숙지 – 집중 리스크 모니터링

4. 싱가포르

싱가포르는 금융회사의 아웃소싱에 대하여 법적으로 아웃소싱이 가능한 (또는 불가능한) 업무 등을 규정하거나 규제하고 있지 않으며, 2016년 7월 감독기관인 MAS (Monetary Authority of Singapore)는 금융회사의 아웃소싱 리스크 관리를 위한 지침(MAS, 2016)을 발표하였다. 본 지침은 아웃소싱과 관련하여 금융회사에 대한 MAS의 요구사항을 정리한 것으로, 크게 아웃소싱과 관련한 MAS의 감독, 리스크 관리 수행, 클라우드컴퓨팅(cloud computing) 서비스의 아웃소싱과 관련한 관리 · 감독에 관한 사항을 제시하고 있다. 금융회사는 본 지침을 기준으로 기존의 모든 아웃소싱 계약에 대한 자체평가를 수행해야 하며, MAS는 금융회사가 이사회의 질적 측면 및 최고경영진의 감독과 지배구조, 내부통제, 리스크 관리 등을 평가하기 위해 본 지침을 준수하고 있는지를 검토한다.

먼저 금융회사의 아웃소싱에 대한 MAS의 감독과 관련하여, 금융회사는 MAS에 지침을 준수하고 있음을 입증해야 하며, MAS가 금융회사의 준수 수준에 대하여 만족하지 못하는 경우 지적된 결함을 시정하기 위한 추가적 조치를 취할 것을 요구할 수 있다. 또한 MAS는 특정 상황이 발생하는 경우 금융회사 측에 아웃소싱된 업무를 변경 또는 대체할 다른 계약을 체결하도록 하거나 내부수행으로 재통합하도록 요구할 수 있다. 금융회사는 아웃소싱으로부터 '부정적 사건'이 발생한 경우 관련 내용을 가능한 한 신속하게 MAS에 통보하여야 한다. '부정적 사건'에는 아웃소싱 계약과 관련하여 장기간 서비스 공급 불가 또는 중단으로 이어질 수 있는 각종 사고가 포함되며, 금융회사 고객 정보에 대한 보안사고도 여기에 포함된다.

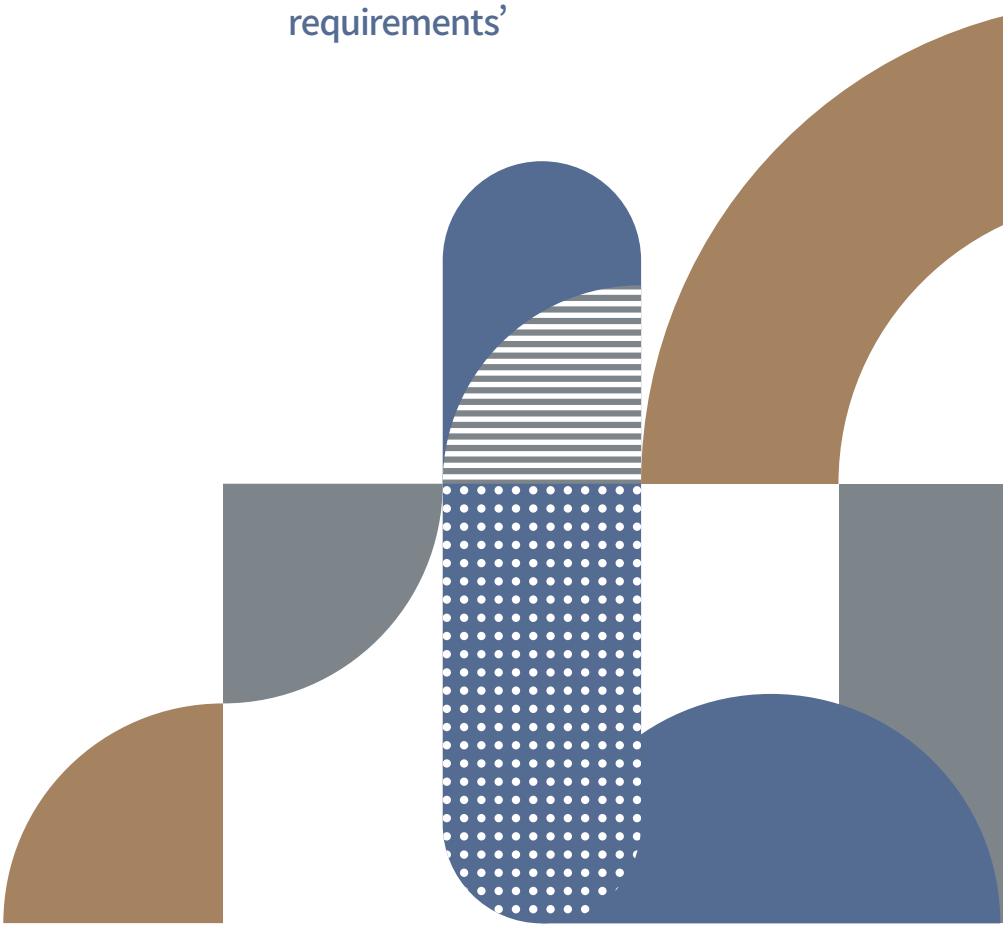
아웃소싱 리스크 관리에 있어서 MAS의 지침 역시 이사회와 최고경영진의 책임을 강조하고 있다. 금융회사의 아웃소싱 계약에 대한 효과적인 감독, 리스크 관리, 이를 위한 적절한 관리체계 구축 책임은 금융회사 이사회 및 최고경영진이 지며, 제3자에게 위임할 수 없다고 본 지침은 명시하고 있다. 공급업체 후보들에 대한 실사 및 선정, 아웃소싱 계약에 포함되어야 하는 사항, 기밀유지 및 보안, 업무 연속성 관리, 공급업체에 대한 모니터링 및 통제 등으로 구성된 아웃소싱 리스크 관리 프로세스에 관한 내용은 미국을 비롯한 다른 국가의 공적 기관들의 지침과 거의 유사하다.

MAS의 지침은 금융회사가 제3자가 제공하는 클라우드 컴퓨팅 서비스를 이용하는 경우도 아웃소싱으로 간주하고, 이 경우의 관리에 대하여 별도로 언급하고 있다. 즉 금융회

사는 이 경우에도 MAS의 지침에 따라 리스크 관리를 이행해야 한다. 특히 다양한 데이터가 혼재되어 있고, 다양한 고객이 소프트웨어를 공유하여 사용하는(multi-tenancy) 클라우드 컴퓨팅의 특성을 고려하여 금융회사는 데이터 접근, 기밀성, 무결성, 복구 가능성 등을 위한 적극적 조치를 취하야 한다. 또한 공급업체가 고객 데이터를 명확하게 식별하고 분리할 수 있으며, 고객 정보 보호를 위한 강력한 통제장치를 보유하고 있는지 확인해야 한다.

IV. 해외 금융회사 아웃소싱 관리 내부 지침

1. 글로벌 금융회사의 공급업체 행동 강령
2. JP Morgan의 ‘Minimum control requirements’



IV. 해외 금융회사 아웃소싱 관리 내부 지침

본 장에서는 해외의 주요 금융회사들이 내부적으로 마련하여 운영하고 있는 아웃소싱 관련 지침의 주요 내용을 살펴본다. 세계 유수의 글로벌 금융회사들은 모두 아웃소싱 공급업체 행동 강령(vendor 또는 supplier code of conduct)를 마련하여 공급업체에게 적용하고 있는데, 이것은 공급업체가 준수해야 할 사항을 금융회사들이 자체적으로 마련하여 적용하는 것으로서, 아웃소싱 관리를 위한 내부 지침과는 약간 차이가 있다. 본 장에서는 먼저 글로벌 금융회사들의 공급업체 행동 강령의 주요 내용들을 정리하여 살펴본 다음, 구체적인 아웃소싱 관리 내부 지침으로서 JP Morgan Chase(JPMC)의 'IT 아웃소싱의 최소 통제 요구사항(minimum control requirements)'의 내용을 소개한다.

1. 글로벌 금융회사의 공급업체 행동 강령

금융회사들이 마련하여 아웃소싱 공급업체에게 적용하고 있는 행동 강령(code of conduct)은 아웃소싱된 서비스의 공급을 위하여 금융회사와 계약한 공급업체가 준수해야 하는 기본적 사항들을 비교적 추상적이고 보편적인 수준에서 제시한 것으로, 그 내용은 세부적인 부분에서 일부 차이는 있으나 거의 대동소이하다. 금융회사들은 UN 세계인권선언, 국제노동기구(International Labor Organization: ILO) 기본협약 등 국제적으로 인정된 규범에 기초하여 행동 강령을 마련했음을 밝히고 있으며(예: BoA, 2019), 아웃소싱 뿐 아니라 offshoring까지 포괄한다(예: Goldman Sachs, 2017). <표 IV-1>은 Bank of America(BoA), Citi, Credit Suisse, Goldman Sachs, Morgan Stanley의 5개 글로벌 금융회사의 공급업체 행동 강령에 공통적으로 포함되어 있는 주요 내용을 정리하여 보여준다. <표 IV-1>에서 볼 수 있듯이, 5개 금융회사의 행동 강령은 공통적으로 사업(business)에 있어서 윤리 및 무결성(integrity), 노동 및 인권, 환경 및 지속가능성, 다양성(diversity) 및 포용(inclusion)에 관한 사항들을 담고 있으며, 아웃소싱의 관리를 위한 지침이라기보다는 추상적이고 선언적인 수준의 내용이 대부분이나, 회사별로 구체성에는 차이가 있다. 특히 Citi는 각 사항에 대하여 타사에 비하여 상당히 구체적인 수준의 공급업체 준수 요구사항을 기술하고 있다.

<표 IV-1> 글로벌 금융회사 공급업체 행동 강령 주요 내용

윤리적 사업 관행 사업 무결성(integrity)	– 관련 법규 준수 및 공정 경쟁 – 이해상충 방지 – 사기 방지 – 뇌물, 부당한 이익 취득 금지, 부패 방지, 청렴 유지 – 선물 및 접대 관련 제한사항 준수 – 정치적 활동 및 기부 금지 – 자금세탁방지 준수 – 개인정보, 프라이버시, 금융회사 정보 보호 – 고충 처리 메커니즘 설치 – 금융회사 상호, 상표, 자산, 데이터 사용상의 제한 준수 – 내부고발자 보호 – 업무 연속성 확보
노동 및 인권	– 자유노동 보장, 강제노동 금지 – 아동노동, 인신매매 금지 – 고용상의 차별 금지 – 직장 내 차별, 괴롭힘 금지 – 임금 및 복리후생 – 근로 시간 준수 – 직장 내 안전, 위생, 음식 – 종업원의 건강 및 안전 – 약물 없는 직장 – 결사의 자유(freedom of association) 보장
환경 및 지속가능성	– ESG에 초점 – 자원·에너지 소비 절감 및 배출 감소 노력 – 유해물질 감소 노력
다양성 및 포용	– 소수자를 포함한 고용 다양성 – 공급업체 다양성
기타	– 지속적 혁신 노력 – 산업 표준 준수 – 문서화, 감사, 보고 체계 – 수정 조치 프로세스

자료: BoA(2019), Citi(2019), Credit Suisse(2020), Goldman Sachs(2017), Morgan Stanley(2020)

5개 금융회사 중에서 Citi의 행동 강령은 <표 IV-1>에서 제시된 내용에 추가적으로 아웃소싱 관리 지침 수준의 구체적이고 세부적인 사항도 일부 포함하고 있다. 예를 들어, 공급업체의 비용 청구는 영수증을 근거자료로 첨부하여 서면으로 이루어져야 하고, Citi의 정보를 보관하고 있는 모든 공급업체는 정보 관리 작업을 반드시 Citi 담당자와 함께 공동으로 해야 한다. 공급업체는 사무실 내의 기기와 정보에 대한 보안 수칙을 준수해야 하며, 책상 아래나 캐비넷 상단과 같이 화재 및 신체적 위험을 초래할 수 있는 장소에는 개인 물품 보관을 금지한다. 특히 Citi의 행동 강령은 정보와 데이터 보안에 대하여 매우 자세하고 구체적인 사항들을 규정하고 있는데, 공급업체는 정보 보안을 위한 사내 정책을 수립 · 집행해야 하고, 외부인의 접근 금지, 자산관리상의 보안 유지, 물리적 · 환경적 안전의 보장, 통신 보안, 외부로부터의 접속 통제, 공급업체의 정보시스템 구입 · 개발, 정보보안 사고 관리 등에 관한 사항들이 여기에 포함된다.[27] 이 외에 모든 공급업체의 직원을 대상으로 해당 현지의 법규에 따라 신원조회를 실시하며, 신원조회에서 확인해야 하는 사항들도 규정하고 있다.

2. JP Morgan의 'Minimum control requirements'

JP Morgan(JPMC)의 'Minimum control requirements(JPMC, 2018)'는 IT 아웃소싱을 효과적으로 통제하고, 관련 리스크를 효과적으로 관리하기 위한 JPMC의 내부통제 점검 · 확인사항 및 IT 아웃소싱 공급업체가 준수하여야 하는 통제 요구사항을 규정 · 문서화한 것으로 2018년에 마련, 발표되었다. JPMC(2018)는 IT 아웃소싱 리스크 평가, 보안, 데이터 사용 · 보호 · 백업, 고객 개인정보 보호, 운영(operation)의 안정성, 사고 대응, 변화 관리, 재아웃소싱 등의 영역에 걸쳐 26개 항목의 통제 요구사항을 담고 있는데, 그 내용은 매우 구체적이고 상세하게 설명되어 있다. 구체적인 내용은 <표 IV-2>에 정리되어 있는데, 예를 들어 IT 시스템에 대한 외부로부터의 접근을 어떻게 통제할 것인지, 시스템 네트워크 · 애플리케이션 · 데이터파일 구조 등의 변화에 대한 관리는 어떻게 이루어져야 하는지와 같은 구체적이고 개별적인 상황에 대한 기술적 요구사항을 제시하고 있다.

27 Citi의 행동 강령에 포함된 사항은 매우 구체적이고 기술적으로 서술되어 있다. 예를 들어, 외부로부터의 접속을 효과적으로 통제하기 위하여 디지털 인증서(certificate)는 2년마다 갱신되어야 하며, 모든 인터넷 웹사이트 상 또는 Citi와 공급업체 간 점대점(point-to-point) 통신을 위해서는 'extended validation(EV)' 인증서가 사용되어야 한다고 규정하고 있다.

<표 IV-2> JP Morgan 'Minimum control requirements' 주요 내용

리스크 관리	– 문서화된 리스크 평가(assessment) 프로그램과 적절한 교정(remediation) 노력을 통하여 통제의 효과성 검증 – 리스크 평가는 매년 실행
보안 정책	– 문서화된 규칙과 절차에 의하여 정보와 관련 서비스의 수취·전송·처리·저장·통제·배포·추출·접근·설명·보호를 규율 – 보안 정책과 책임은 금융회사 및 공급업체 직원들에게 소통되고 공유되어야 함
조직상의 보안	– 공급업체 직원들에 대한 적절한 훈련을 통하여 책임성있는 보안 조직을 확보하기 위한 공급업체 직원 보안 정책과 동의(agreements) 절차 마련 – 공급업체 직원은 JPMC 서비스에 배정되거나 JPMC 시스템 및 정보에 대한 접근권한이 부여되기 전에 반드시 기밀 유지 의무에 서면으로 동의하여야 함
기술 자산 관리	– JPMC 자산을 보호하기 위한 통제가 마련되어 있어야 하며, 여기에는 정확한 재고 파악, 모든 자산의 도입·이전·제거·처분 등에 대한 표준을 유지하는 메커니즘이 포함됨
물리적·환경적 보안	– 악의적인, 또는 승인되지 않은 사람의 물리적 침임을 막고, 환경 오염 물질에 의한 피해, 전자적 방법에 의한 침투를 막기 위한 통제장치 마련
통신(communication) 및 연결(connectivity)	– 공급업체는 데이터 보호를 위하여 자신의 통신 네트워크에 대한 통제를 실행해야 하며, 통제는 네트워크 보안·암호화·기록관리(logging)·모니터링·불필요한 통신 차단 등을 포함 – 네트워크 식별(identification), 데이터 저장, 방화벽, 시계 동기화(clock synchronization), 원격접속, 무선접속, 데이터 손실 방지 등에 대한 JPMC의 요구사항 준수
변화 관리	– 시스템, 네트워크, 애플리케이션, 데이터파일 구조, 기타 시스템 구성 요소 및 물리적·환경적 변화는 공식적인 변화 통제 환경 하에서 감시·통제되어야 함 – JPMC의 서비스에 중대한 영향을 미치는 비상변화는 반드시 JPMC와 소통을 거쳐야 함
운영(operations)	– 운영 절차(operational procedures)는 문서화되어야 하며, 설비·성과·서비스수준에 대한 동의, 핵심성과지표(KPI)를 포함해야 함
논리적 접근 통제 (logical access control)	– 본인확인(authentication)과 승인(authorization) 통제는 데이터, 애플리케이션, 플랫폼에 관계없이 강건(robust)해야 함

<표 IV-2> JP Morgan 'Minimum control requirements' 주요 내용(계속)

데이터 무결성	– 데이터의 전송(transmission) 및 거래(transaction) 통제: 저장되어 있거나, 새로 받았거나 접근한 데이터의 정확성과 신뢰성을 담보하는 통제가 이루어져야 함
암호화	– 데이터는 전송중이거나 사용하지 않을 때를 막론하고 암호화에 의하여 보호되어야 함 – 암호화 정책은 데이터 분류·키(key)와 인증서 유효기간 관리·암호화 알고리즘 등을 포괄해야 하며, 경영진의 감독 하에 정기적으로 문서화·검토·승인되어야 함
사고 대응	– 정보 보안 사고가 발생한 경우, 공급업체 직원의 책임 및 사고 발생이 통지되어야 하는 대상을 포함한 문서화된 계획 및 절차가 마련되어 있어야 함 – 사고 대응 정책 및 절차는 우선순위 설정, 역할과 책임, 공급업체 내부보고 및 JPMC에의 통보, 추적(tracking) 및 보고, 봉쇄(containment) 및 복구, 법의학적(forensic) 무결성 유지를 위한 데이터 보전 등을 포함해야 함
업무 연속성 및 재난 복구	– 운영 복구(business recovery) 및 기술 복구(technology recovery) 계획은 경영진의 감독 하에 정기적으로 문서화·시험·검토·승인되어야 함
이메일 및 문자메시지	– JPMC의 데이터를 포함하는 이메일·문자메시지 시스템에 대한 적절한 통제를 담보하기 위한 정책과 절차가 마련되어야 함
백업 및 회사외부(offsite)에 설치된 저장장치	– 백업 데이터는 회사 외부에 설치된 저장장치에 보관되어야 하며, 폐기 또는 재사용 전에 반드시 완전 삭제되어야 함 – 모든 시스템·애플리케이션·데이터의 완전한 복구를 가능하게 하기 위한 절차가 경영진의 감독 하에 정기적으로 문서화·검토·승인되어야 함 – 백업 장치의 폐기시 읽을 수 없는 상태로 만들어져야 함
매체 및 중요 기록	– 공급업체에 의한 JPMC 데이터가 저장되어 있는 전자장치 및 종이문서의 취급 및 보관을 통제하는 정책과 절차는 경영진의 감독 하에 정기적으로 문서화·검토·승인되어야 함 – 이 정책에는 기록 통제(record control)와 수송(transportation) 로지스틱스가 포함됨
표준 설정	– 정보시스템은 적절한 보안구성(security configuration)을 갖추어야 하며, 공급업체의 보안정책 및 표준 준수 여부를 정기적으로 점검하여야 함 – 시스템 보안 패치, 운영체제, 데스크톱 통제 등에 관한 사항 포함

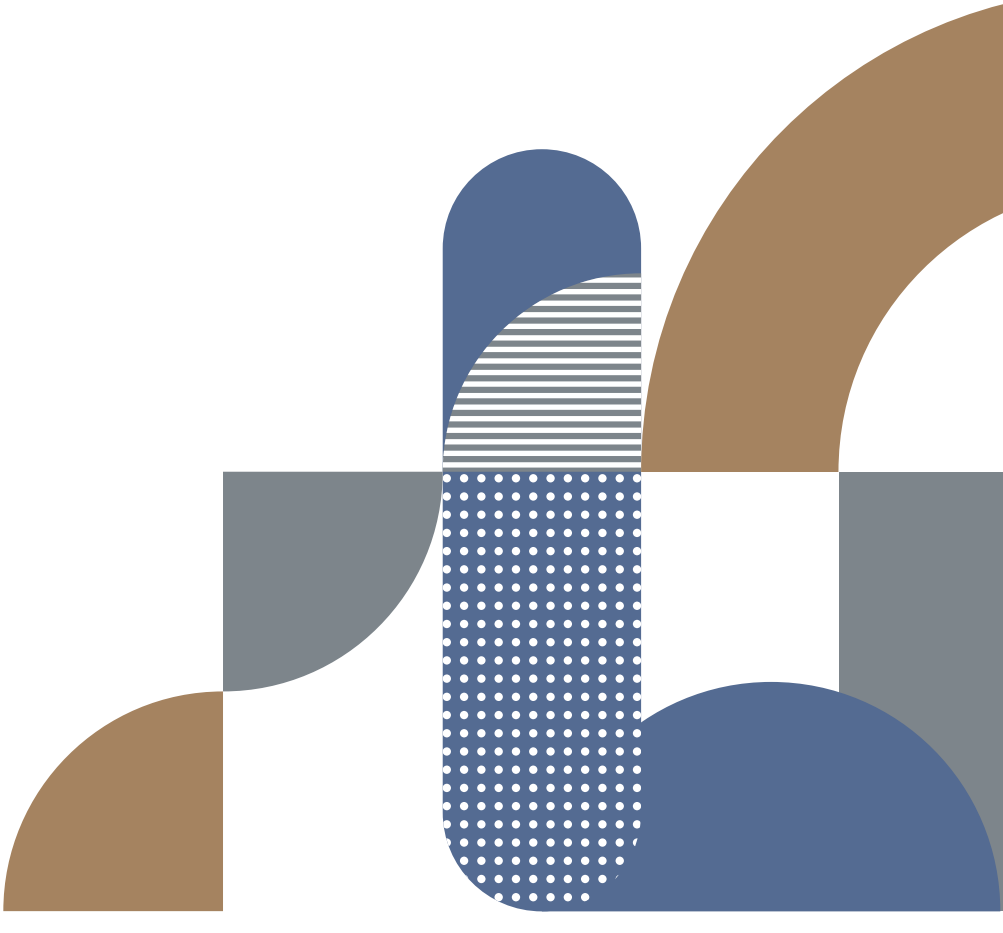
<표 IV-2> JP Morgan 'Minimum control requirements' 주요 내용(계속)

재아웃소싱 공급업체 관계	– 모든 재아웃소싱 공급업체(dependent supplier)가 파악·관리·모니터링되어야 하며, 중요한 서비스를 공급하는 재아웃소싱 공급업체 또는 JPMC에게 중요한 서비스를 제공하는 공급업체를 지원하는 재아웃소싱 공급업체는 모든 통제 요건을 준수하여야 함 – 공급업체는 재아웃소싱 공급업체를 파악·선정하는 절차를 갖고 있어야 하며, 이 재아웃소싱 공급업체는 JPMC에게 공개되어야 하며, 주협약(master agreement)에 따라 승인되어야 함
애플리케이션	– 공급업체는 정보시스템의 정의·취득·개발·고도화·수정·시험·구현을 목적으로 하는 S/W 개발 주기를 정해놓아야 하며, 공급업체는 JPMC 데이터를 저장·수신·송신·접근하는 모든 웹 기반 및 모바일 애플리케이션이 모니터되고 통제되고 보호되도록 해야 함 – 애플리케이션의 기능적 요구사항, S/W 개발 생애주기, 시험 및 복구에 관한 세부적 사항 규정
고객 접점	– 콜센터나 텔레마케팅을 제공하는 공급업체는 JPMC 데이터의 보안·무결성·이용가능성을 보장하는 운영 절차를 정의하여 준수하여야 함
취약점 모니터링	– 공급업체는 현존하는, 그리고 새롭게 나타나는 위험과 실제 공격에 대비하여 끊임없이 정보를 수집하고 취약점을 분석해야 하며, 이 과정에는 취약점 스캔·악성코드 백신·침임탐지시스템·침입방지시스템·기록(logging)·보안정보 및 사건관리의 분석 등이 포함됨
규제 준수	– JPMC 데이터의 보호와 법적·규제적 요건의 준수를 담보하기 위한 절차가 마련되어 있어야 함
개인정보 보호	– 공급업체는 기밀정보에 적용되는 JPMC Minimum control requirements를 개인정보에 대해서도 적용해야 함 – 사회보장번호와 같은 공적 식별번호는 애플리케이션 로그온을 위한 사용자 ID로 사용되어서는 안됨 – 개인정보 보호에 대한 영향 평가는 시스템 개발의 요구사항 단계에서 수행되어야 함 – 관련 규제의 준수

<표 IV-2> JP Morgan 'Minimum control requirements' 주요 내용(계속)

클라우드 기술	– 클라우드 기술을 사용하여 저장·처리·전송된 JPMC 데이터의 보안성·무결성·이용가능성을 담보하기 위한 충분한 안전장치가 마련되어 있어야 함 – 클라우드 환경의 산업표준·규제 요구사항 만족, 애플리케이션 및 인터페이스의 보안, 암호와 및 기 관리, 거버넌스 및 위험관리, ID 및 접근관리, 상호연동성(interoperability) 및 이동성(portability) 확보, 가상화(virtualization) 보안 등이 포함됨
사업 관행	– 정책과 절차는 모든 사기 의심 사례에 대한 적절한 대응 뿐 아니라 사업 운영에 대한 관리감독을 담보해야 함
데이터 사용	– JPMC 데이터를 수취·전송·저장·창출·수집·통제·처리하거나 JPMC 데이터에 접근권한을 가진 모든 공급업체와 재아웃소싱 공급업체는 JPMC에 서비스를 제공하는 목적으로만 그렇게 해야 함

V. 시사점



Ⅴ. 시사점

본 보고서의 Ⅲ장에서 살펴본 바와 같이 미국, 유럽, 영국, 싱가포르는 금융회사의 아웃소싱에 대하여 법령으로 제한을 두고 있지 않으며[28], 금융회사는 영위하는 모든 업무에 대하여 원칙적으로 자유롭게 아웃소싱이 가능하다. 대신에 이들 국가의 규제 · 감독 등 공적 기관들은 연성규범으로서 금융회사의 아웃소싱 관리를 위한 지침 또는 가이드를 만들어 제시하고 있다. 이 기관들의 지침 중 특히 미국과 싱가포르의 경우 아웃소싱 의사결정과 관리에 있어서 이사회와 최고경영진의 역할과 책임을 강조한다. 아웃소싱이 금융회사의 효율성 제고 및 경쟁력 강화를 목표로 하는 전략적 의사결정이라는 점에서 이것은 당연하며, 우리나라 금융회사들도 이에 대한 인식을 높일 필요가 있다.

자본시장법 및 그 하위규정, 업무위탁규정 등 우리나라의 금융회사 아웃소싱(업무위탁)을 규율하는 법규들의 내용과 비교할 때, 외국의 지침들은 보다 구체적 · 전문적 · 기술적 내용을 담고 있다. <표 Ⅴ-1>은 우리나라의 자본시장법과 조사 대상 4개국 공적 기관의 지침의 구성을 비교하여 보여준다. 표에서 볼 수 있듯이 이 지침들은 공통적으로 자본시장법에서는 규정하지 않고 있는 아웃소싱 리스크 평가, 아웃소싱 공급업체 실사 및 선정, 아웃소싱 계약의 설계 · 체결 · 공급업체 모니터링으로 이어지는 관리 프로세스를 제시하고 있다. 또한 자본시장법 및 그 하위규정에서 정한 업무위탁 계약 포함 사항(<표 Ⅱ-1>)은 미국 공적 기관들의 지침이 제시하고 있는 것과 큰 차이가 없으나, 우리나라 법규가 항목만 제시하고 있는데 반하여 미국의 지침들은 이 항목들을 구체적으로 어떻게 계약에 구현하여 담을 것인지까지 언급하고 있다는 점에서 다르다. 우리나라의 자본시장법은 법령으로서 금융회사가 준수해야 하는 최소한의 사항만 제시하면 되지만, 향후 아웃소싱 규제가 지속적으로 완화되고 궁극적으로 원칙중심으로 전환되면 우리나라에서도 이들 국가와 마찬가지로 지침이 필요하게 될 것이다. 그리고 <표 Ⅴ-1>은 그 지침이 연성규범으로서 효과적으로 작동하고, 금융회사가 아웃소싱을 추진할 때 실질적인 도움을 줄 수 있기 위해서는 현재의 법령 수준보다는 보다 구체적이고 전문적이어야 한다는 것을 시사한다.

28 영국은 감독규정에 해당하는 SYSC 8.1에서 아웃소싱을 규율한다는 점에서 약간의 차이가 있다.

<표 V-1> 아웃소싱 법령·지침 구성의 국가별 비교

	한국 (자본시장법)	미국	EU	영국	싱가포르
아웃소싱이 금지되는 경우·업무	○	×	× (업무중요도 평가)	○	× (업무중요도 평가)
사전보고 의무	○	×	×	○	×
이사회·최고경영진 역할 및 책임	×	○	×	×	○
아웃소싱 리스크관리 프로세스·내부통제	×	○	○	○	○
공급업체 실사 점검사항	×	○	○	○	○
아웃소싱 계약 포함사항	○	○	○	×	○
공급업체 감독·모니터링	×	○	○	○	○

금융회사의 내부적 아웃소싱 관리 지침 역시 JP Morgan의 사례에서 볼 수 있듯이 매우 세부적인 사항까지 상세한 내용을 담고 있다. 이와 같은 전문적 · 구체적 · 기술적인 내부지침을 만들고 자사의 아웃소싱에 대해 시행하려면 관련 인력의 전문성 역시 상당한 수준이어야 할 것이다. 특히 급속한 기술 발전에 따라 클라우드 컴퓨팅을 비롯한 IT 부문 아웃소싱의 중요성이 커지고 있는 현시점에서 금융회사의 기술적 전문성이 더욱 요구되고 있다는 점에서 금융회사들은 실제 업무는 아웃소싱하더라도, 그 아웃소싱을 효과적으로 관리하기 위해서는 자체 인력의 기술역량을 확보하는 노력도 병행해야 할 것이다.

또한 IT 아웃소싱의 증가는 고객의 개인정보, 금융회사의 데이터 및 기업정보 등과 관련된 리스크 관리의 중요성을 증대시킨다. 영국 FCA의 지침에는 이미 GDPR 준수와 관련된 내용이 포함되어 있다. 우리나라에서도 소위 '데이터 3법'[29]의 개정, 오픈뱅킹 · 마이데이터 등의 도입, 금융혁신지원특별법에 의한 혁신적 금융서비스 제공을 위한 아웃소싱이 규제완화 등이 이루어지면서 정보 · 데이터 보안이 매우 중요해지고 있다. 아웃소싱이 내포하는 리스크에 대한 철저한 인식을 바탕으로, 아웃소싱 관리의 실패로 인하여 금융소비자 보호 및 금융시스템 안정에 부정적 영향이 가지 않도록 금융회사들은 자사의 아웃소싱을 관리해야 한다.

29 개인정보보호법, 신용정보법, 정보통신망법을 일컫는다.

참고문헌

고대영·조현승·문종철, 2015,『제조업 가치사슬상 서비스 아웃소싱에 대한 분석 및 활성화 방안』, 연구보고서 2015-751, 산업연구원.

금융감독원, 2018a,「금융기관의 업무위탁 등에 관한 규정」업무해설서.

금융감독원, 2018b, 금융투자업자의 업무위탁 매뉴얼.

금융감독원, 2020, 금융투자업자 업무위탁 사전보고 내역(2020 상반기).

금융위원회, 2014. 1. 8, 신용카드업자 고객정보 유출 관련 현황 및 대응방안, 보도참고자료.

금융위원회, 2014. 1. 22, 금융회사 고객정보 유출 재발방지 대책, 보도자료.

금융위원회, 2014. 3. 10, 금융분야 개인정보 유출 재발방지 종합대책, 보도자료.

금융위원회, 2017. 3. 20,「4차 산업혁명 금융분야 TF」출범 및「금융규제 테스트베드」도입방안 마련, 보도자료.

금융위원회, 2017. 11. 13, 금융회사의 영업자율성 제고 및 혁신적 금융서비스 도입 확대를 위한「금융기관의 업무위탁 등에 관한 규정」개정, 보도자료.

금융위원회, 2019. 5. 27, 금융투자업 영업행위 규제 개선방안, 보도자료.

금융위원회, 2020. 4. 29, 금융투자업자의 정보교류차단장치(차이니즈월) 규제체계 개편 등 자본시장법 개정안 국회 본회의 통과, 보도참고자료.

금융위원회, 2020. 6. 5, 핀테크기업이 금융회사의 핵심업무를 시범운영할 수 있는 지정대리인으로 3개 기업을 지정하였습니다, 보도자료.

금융위원회·금융감독원, 2016, 정보처리 위탁 관련 FAQ.

금융투자협회, 2018, 금융투자회사 업무위탁제도 개선방안.

변제호·홍성기·김종훈·김성진·엄세용·김유석, 2015,『자본시장법』제2판, 지원출판사.

이승준·정인영, 2017,『보험회사 업무위탁 관련 제도 개선방안』, 연구보고서 2017-8, 보험연구원.

임형석 · 이순호 · 이대기, 2014, 『「금융회사의 업무위탁」 관련 제도개선 방안』, 연구용역보고서, 한국금융연구원.

정흥준 · 김근주 · 노성철 · 박명준 · 송민수 · 정슬기 · 황선웅, 2017, 『아웃소싱의 메커니즘과 기업 내외에 미치는 영향』, 연구보고서 2017-06, 한국노동연구원.

조성훈, 2019, 금융투자회사의 아웃소싱 관리: 해외 사례, 자본시장포커스 오피니언 2019-26, 자본시장연구원.

하헌식, 2017, 『4차 산업혁명과 아웃소싱』, 바른북스.

Bank of America(BoA), 2019, Bank of America vendor code of conduct.

BIS, 2005, Outsourcing in financial services.

BNP Paribas, Oliver Wyman, 2017, Post-trade processing: Investment banks rethink third-party strategies.

Bolton, P., Scharfstein, D.S., 1998, Corporate finance, the theory of the firm, and organizations, *Journal of Economic Perspectives* 12, 95-114.

Citi, 2019, Citi standards for suppliers.

Credit Suisse, 2020, Credit Suisse supplier code of conduct.

EBA, 2017, Recommendations on outsourcing to cloud service providers, Final report.

EBA, 2018, EBA report on the prudential risks and opportunities arising for institutions from fintech.

EBA, 2019, Final report on EBA guidelines on outsourcing arrangements.

Economist, 2008. 9. 29, Outsourcing.
https://www.economist.com/news/2008/09/29/outsourcing.

FCA, 2018, FG 16/5 guidance for firms outsourcing to the 'cloud' and other third-party IT services, Finalised guidance.

FCA, 2019, Outsourcing, Chapter 8 of Senior management arrangements, systems and controls (SYSC).

FDIC, 2008, Guidance for managing third-party risk.

Federal Financial Institutions Examination Council (FFIEC), 2004, Outsourcing technology services.

FRB, 2013, Guidance for managing outsourcing risk.

Glen, J., 2013, Offshoring vs outsourcing. http://www.businessdictionary.com/article/1090/offshoring-vs-outsourcing-d1412/.

Goldman Sachs, 2017, Goldman Sachs vendor code of conduct.

Investopedia, 2019, Outsourcing. https://www.investopedia.com/ terms/o/outsourcing.asp

JP Morgan Chase(JPMC), 2018, JPMC's minimum control requirements.

McCahery, J.A., De Roode, F.A., 2018, Governance of financial services outsourcing: Managing misconduct and third party risks, ECGI working paper series in law No. 317/2018.

Monetary Authority of Singapore (MAS), 2016, Guidelines on outsourcing.

Morgan Stanley, 2020, Supplier code of conduct.

Office of the Comptroller of the Currency (OCC), 2013, Third-party relationships: Risk management guidance.

Overby, S., 2005, Outsourcing – and backsourcing – at JP Morgan Chase. https://www.cio.com/article/2448539/outsourcing-and- backsourcing-at-jp-morgan-chase.html.

Sparrow, E., 2006, *Successful IT outsourcing* (김명식 역,『성공적인 IT 아웃소싱 관리』), 도서출판 아진.

Webb, J., 2017, What is offshoring? What is outsourcing? Are they different? https://www.forbes.com/sites/jwebb/2017/07/28/what-is-offshoring-what-is-outsourcing-are-they-different/ #457ff75d2a2e.

금융감독원	fss.or.kr
Bank of America	www.bankofamerica.com
Citi	www.citigroup.com/citi
Credit Suisse	www.credit-suisse.com
EBA	eba.europa.eu
FCA	www.fca.org.uk
FDIC	www.fdic.gov
FFIEC	www.ffiec.gov
FRB	www.federalreserve.gov
Goldman Sachs	www.goldmansachs.com
JP Morgan Chase	www.jpmorganchase.com
MAS	www.mas.gov.sg
Morgan Stanley	www.morganstanley.com
OCC	www.occ.treas.gov

Abstract

Outsourcing, which means allowing a third party outside the company to perform activities or functions that the company has performed internally, is a strategic decision-making aimed at reducing costs, enhancing management efficiency, and strengthening core competencies, and this importance is the same in the financial services industry. In particular, outsourcing is becoming more important as the value chain of the financial services industry changes according to the recent rapid technological development called the '4th industrial revolution.' However, in Korea, there have been opinions that the statutory regulations on outsourcing are rigidly operated, limiting financial services firms' use of outsourcing, and thus failing to respond to rapidly changing environments, and outsourcing regulations are on the trend of easing.

Major foreign countries, such as the United States, European Union, United Kingdom, and Singapore do not regulate outsourcing of financial services firms by law. Instead, regulatory or supervisory agencies have created and provided guidelines or guidances for outsourcing management of financial services firms. The guidelines of these agencies commonly emphasize the roles and responsibilities of the board of directors and top management in making and managing outsourcing decisions. In addition, the management process leading to outsourcing risk management, due diligence and selection of outsourcing suppliers, design and conclusion of outsourcing contracts, and supplier monitoring is presented in a similar manner.

All global financial services firms have developed a 'Code of Conduct' to manage their outsourcing and apply them to their suppliers. The Code of Conduct commonly

contains matters concerning business ethics and integrity, labor and human rights, environment and sustainability, diversity and inclusion. This report also introduces the contents of JP Morgan's 'Minimum Control Requirements' as a specific internal guideline for outsourcing management, which are very specific and detailed as defining minimum control requirements to effectively control IT outsourcing and manage related risks.

If Korea's outsourcing regulations are continuously eased and ultimately shifted to principle-based, guidelines as soft norms will be needed, and these guidelines should be specific and specialized to provide practical assistance to financial services firms. Financial services firms' internal outsourcing management guidelines should also be specialized, detailed and technical, and efforts should be made to secure the technical capabilities of their own personnel to create and implement these internal guidelines. With the increase of IT outsourcing, the importance of risk management related to data and information of customers and firms is growing, and firms need to raise awareness of the responsibilities of the board and top management for outsourcing management.