금융회사의 정보처리 및 전산설비 위탁에 관한 리스크 관리 가이드라인

목 차

금융회사의 정보처리 및 전산설비 위탁에 관한 리스크 관리 가이드라인

Ⅰ 목 적

□ 이 가이드라인은 금융회사가 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」에 따라 정보처리 및 전산설비를 제3자에게 위탁(이하 “위탁”)함에 있어

◦ 위탁 금융회사(이하 “위탁회사”)가 고려해야 할 기본적 리스크 관리절차*를 권고함으로써 금융이용자 보호 및 금융시스템 안정성을 유지·강화하고자 함

* 경영진의 책무, 수탁회사 선정, 위탁계약 체결, 업무연속성 확보 및 정보보호·보안통제 등

Ⅱ 위탁 관련 리스크

□ 위탁회사는 이 가이드라인을 포함하는 리스크 관리지침(내부관리기준)을 마련하고 발생 가능한 위탁 관련 리스크가 통제되도록 하여야 하며, 위탁 받은 회사(이하 “수탁회사”)로 하여금 위탁회사의 리스크 관리지침 등을 준수하여 서비스를 제공하도록 하여야 함

< 위탁관련 주요 리스크 >

리스크 구분	리스크 내용
전략적 리스크 (Strategic Risk)	- 위탁회사의 불합리한 위탁 의사결정 및 이행 - 리스크 환경 변화에 대한 리스크 관리대책의 유효성 결여
운영 리스크 (Operat ion Risk)	- 수탁회사에 대한 위탁회사의 감독 불충분 - 의무이행 및 비상대응을 위한 수탁회사의 기술적·재무적·관리적 능력 부족 - 수탁회사가 리스크를 자체 발견하고 통제·개선하는 역량 부족
거래상대방 리스크 (Counterparty Risk)	- 수탁회사의 기술력, 서비스 수준 및 업무연속성 변동 및 부적합 - 수탁회사의 재위탁 하도급계약(제3자 의존 등)에 따른 리스크 통제 약화
법규준수 리스크 (Compliance Risk)	- 수탁회사의 법규준수(정보보호, 보안통제 등) 및 내부통제 시스템 미흡 - 수탁회사의 위탁회사 지시 불이행 및 법규 준수 노력(교육, 보안의식)미흡
평판 리스크 (Reputation Risk)	- 금융이용자에 대한 서비스(위탁서비스)가 위탁자가 설정한 기준에 미달 - 수탁회사의 서비스철학, 사업전략, 법규위반 등으로 인한 위탁회사 평판 변동
퇴출전략적 리스크 (Exit Strategic Risk)	- 위탁계약 해지·종료 관련 대응전략이 없을 경우 수탁회사 변경의 어려움 - 위탁업무 회수 능력(데이터 회수·파기, 보안통제 등) 부족
국가 리스크 (Country Risk)	- 수탁회사 국가의 정치, 사회, 법적 환경이 리스크를 증폭시킬 수 있음 - 위탁업무의 연속성 보장이 어렵고 업무연속성 계획이 복잡해지는 문제
계약 리스크 (Contractual Risk)	- 위탁계약 이행을 수탁회사에 강제할 수 있는 통제수단의 확보 미흡 - 위·수탁회사간 분쟁발생시 손해배상 및 준거법규의 적용문제
접근 리스크 (Access Risk)	- 감독기관에 제공하는 정보의 신속성 제약 - 위탁업무에 대한 감독기관의 권한을 제한하는 요소
집중 및 시스템 리스크 (Concentration & Systemic Risk)	- 산업전체, 그룹 계열사, 금융회사의 위탁이 증대하거나, 특정 수탁회사에 집중될 경우 수탁회사 통제의 어려움과 시스템 리스크 증대

Ⅲ 경영진의 책무

□ 위탁회사의 경영진은 위탁 전에 위탁의 목적, 비용 및 편익에 대한 분석을 실시하고 위 'Ⅱ'에 열거한 위탁관련 주요 리스크를 고려하여 발생 가능한 제반 위탁리스크를 명확히 파악하여 의사결정에 활용하여야 함

◦ 위탁회사의 경영진은 정보처리 및 전산설비 위탁(재위탁 포함)으로 제3자에게 개인식별정보 또는 금융거래정보가 이전 될 경우, 자사의 사업전략과의 부합여부, 명료한 업무상의 필요성 및 위탁에 따른 철저한 리스크 분석과 리스크 관리대책을 근거로 위탁 여부를 결정하여야 함

◦ 위탁회사의 경영진은 수탁회사가 제공하는 서비스가 자사의 업무와 조화롭게 융화되고, 위탁서비스가 기존 운영체계와 상충되지 않고 지속 가능하게 제공되도록 위탁업무를 관리하여야 하며, 위탁업무와 관련된 리스크 관리 및 의사결정 등과 관련된 제반사항에 대한 문서화와 보고 및 리스크관리 체계를 구축하여야 함

□ 위탁회사의 경영진은 위탁현황의 관리·기록 및 각 위탁 대상별 리스크 통제 및 관리체계가 적정히 이행되고 있는지 지속적으로 평가·확인*하고 위탁서비스가 원활히 제공되도록 리스크 관리대책을 마련하고 이행하여야 함

* 위탁업무의 세부 내용(이전되는 개인식별정보 및 금융거래정보의 범위 포함), 수탁회사명, 금융감독기관에 위탁 보고(승인)일, 리스크 관리 담당자, 리스크 점검기간, 리스크 평가 및 조치 내용 등

◦ 위탁회사의 경영진은 위탁업무의 중요도, 규모 및 복잡성 등을 고려하여 그 수준에 따라 차별화되고 강화된 리스크 관리절차를 마련*하여야 함

* 위탁으로 이전되는 정보(개인식별정보, 금융거래정보 등) 및 금융회사의 본질적 업무 수행과 연계된 정보처리 및 전산설비 위탁을 고려하여 차별화 된 리스크 관리 및 보고체계(필요시 이사회와 경영진의 책무를 구분·운영)를 구축

Ⅳ 리스크 관리 절차

□ 위탁회사는 위탁업무를 효과적으로 관리·감독할 수 있는 리스크 관리지침(내부관리기준)을 마련하고, 리스크 환경변화에 따라 리스크 관리절차가 유효성을 갖도록 지속적으로 리스크 관리대책을 검토·개선하여야 함

□ 리스크 관리 절차에는 위탁과 관련된 기본적인 리스크 분석, 위탁진행 단계별 세부리스크 분석과 위탁서비스의 유지를 위한 리스크 관리 등이 포함됨

□ 기본적인 리스크 관리 절차는 다음의 6가지 활동으로 구성됨

◦ ①위탁리스크 분석 및 평가, ②수탁회사 선정, ③위탁계약 검토 및 체결, ④수탁회사에 대한 관리·감독, ⑤서비스수준 및 업무 연속성, ⑥정보보호 및 보안통제 등

1 위탁 리스크 분석 및 평가

1-1. 위탁시 발생하는 기본적 리스크를 인식하고 위탁경험 및 다른 위탁회사의 리스크 사례, 환경 변화 등을 고려하여 위탁 업무별, 유형별, 단계별로 리스크를 분석 및 평가하며, 리스크 관리업무가 목적 적합성 및 실효성을 유지하도록 지속적으로 검증하고 보완하는 과정으로서 다음의 사항을 고려하여야 함

① 위탁을 추진하는 사업전략에서 파생되는 'Ⅱ. 위탁관련 리스크' 등

* 위탁서비스를 이용하는 위탁회사 부서 등 이용자그룹의 의견 청취도 필요

② 위탁되는 정보처리 및 전산설비의 중요성*, 위탁 규모 및 복잡성 리스크

* 위탁회사는 위탁되는 전산설비에 저장되는 데이터 정보를 구체적으로 분류하여 문서화하여야 하며, 정보보호를 위한 보안통제 장치와 중요 데이터정보가 훼손될 경우 동일한 정보로의 대체가능 수단 확보 여부를 확인하고 관련 리스크의 해소 가능여부를 판단하여야 함

③ 수탁회사 선정·계약, 업무 연속성 확보, 정보보호 및 감독 등 위탁 단계별 리스크

1-2. 기본적 리스크를 보다 구체화하고 위탁회사의 위탁서비스 기대수준을 반영하여야 하며, 다음 사항에 대한 제반 리스크 관리절차가 문서화되어야 함

① (위탁범위 및 특성) 수탁회사가 제공하는 서비스, 동 서비스에 대한 금융이용자 및 위탁회사 이용부서의 요청사항에 대한 처리와 지원방법

② (서비스 수준) 서비스의 질, 서비스 수준 및 서비스 성과평가

③ (수탁회사의 자격조건) 관련업무의 수탁 경험, 재무상태, 평판, 업무담당 임직원의 변경(핵심 기술인력 유출 등), 업무 연속성 보장(서비스 제공의 유지능력), 정보보호 및 보안통제 장치의 적정성, 적합한 정보처리 및 전산설비 제공 능력, 법적 분쟁이력, 하청업체 의존성, 국외 수탁회사의 경우 국가 리스크 등 제반 리스크

④ (감독 및 보고) 위탁회사의 수탁회사 감독(상시 모니터링, 감사 등) 및 감독결과의 경영진(필요시 이사회) 보고, 수탁회사의 감독 필요서류 제출의무 및 감독 결과에 따른 조치 수용, 감독기관의 실질적 감독가능성 및 서비스 수준과 업무연속성 확보, 보안 및 전산사고 등 문제 발생시 처리방안

⑤ (인계요건) 수탁회사에 데이터 이전, 업무처리 및 리스크 통제를 위한 책임있는 의사전달체계 구축, 계약 종료(중도해지 포함)시 수탁회사로부터의 데이터 이전 및 회수, 수탁회사 직원 교육(기술, 정보보호, 보안, 준법 교육 등)

⑥ (계약기간 및 법규준수) 계약 개시시점 및 기간, 취소 및 중도해지 조건, 데이터 소유권, 제3자에 대한 재위탁 제한, 분쟁 해결, 정보보호, 위탁회사 데이터에 대한 비밀 준수 및 제반 관련 법규의 준수의무

⑦ (책임) 문제 발생시 책임(상호연대책임을 포함), 보험가입 등

2 수탁회사 선정

2-1. 위탁회사는 다음과 같이 리스크 분석 및 평가와 관리방안을 고려하여 위탁 내용을 제안요청서로 작성하고, 수탁회사가 제출한 제안서를 평가하여야 함

① 제안요청서에는 위탁회사의 목표, 위탁 범위와 특성, 기대 서비스 수준, 이행 기한, 정보보호 및 보안통제 장치, 위탁서비스 제공의 연속성, 평가·측정을 위한 요구사항과 위탁회사와 수탁회사의 권리와 책임(의무) 등을 서술

② 위탁회사는 수탁회사가 제출한 제안서에 대해 위탁회사의 리스크 평가·관리기준 및 자체 선정기준 등을 토대로 평가를 실시

③ 제안서를 받은 위탁회사는 위탁요건과의 대조를 통해 차이점을 공정하게 평가하고 회사의 목표와 기대에 미칠 영향을 분석

④ 위탁회사는 수탁회사와 계약을 체결하기 전에 제안요청서와 수탁회사의 제안서간 차이점에 대해 협의하고 해결방안을 마련

2-2. 위탁회사는 수탁회사에 대한 실사뿐만 아니라 제안요청서에 대한 수탁회사의 제안서 내용에 대해서도 실사를 실시하여야 함

① 실사 절차에는 수탁회사에 관한 다음 사항을 확인하고 리스크를 분석·평가하는 과정이 포함되어야 함

가. 수탁회사의 연혁, 자격, 사업전략 및 평판(법규위반 이력을 포함)
나. 수탁회사로부터 유사한 서비스를 제공받는 다른 회사의 의견
다. 재무상태(재무제표, 감사보고서, 외부감사인 의견 등)
라. 서비스 이행능력, 수준(품질) 및 효율성
마. 기술 및 시스템 구조, 정보보호 및 보안통제 장치의 적정성
바. 수탁회사 내부통제의 적정성, 수탁회사에 대한 위탁회사의 감사 수용, 위탁회사의 감독(상시 모니터링) 결과 시정요구사항과 계약의 이행과 관련한 위탁회사의 지시 및 권고사항을 수탁회사가 준수할 수 있는 경영·통제 환경
사. 수탁업무에 대한 소송, 법률 및 규제의 준수여부(수탁회사에 대한 관계 당국의 규제내용 및 제재조치를 받은 이력 등)
아. 서비스 제공과 관련한 수탁회사의 제3자 의존도 및 거래내용
자. 보험 담보범위
차. 재난복구 및 업무연속성 요구사항을 충족할 수 있는 능력
카. 수탁회사의 서비스철학·품질, 경영스타일 등 무형의 정보에 대한 조사 등

② 위탁회사는 제안서를 제출한 복수의 수탁회사에 대해 실사를 실시할 수 있으며, 실사의 수준과 절차는 위탁리스크, 과거 계약 경험(갱신계약 등), 위탁으로 이전되는 정보, 위탁의 복잡성 및 중요도에 따라 달라질 수 있음

2-3. 위탁회사는 평가 및 실사를 실시한 후, 회사의 리스크 관리, 위탁시 요구사항 등 선정기준을 가장 잘 충족한다고 판단되는 하나 이상의 수탁회사와 계약협상을 실시할 수 있음

① 위탁회사의 특수관계인(계열사 등)을 수탁회사로 선정할 경우에도 여타 제안회사와 차별이 없도록 공정하게 선정과정을 진행하여야 함

② 위탁회사는 수탁회사에 대한 실사 및 평가 결과와 수탁회사 선정 의사결정과 관련된 제반 문서를 감독기관이 요청시 즉시 제출할 수 있도록 보관하여야 함

③ 수탁회사 선정이 수의계약에 의하거나 수탁회사 실사를 실시하지 못할 경우에는 합리적인 사유(근거자료 포함)가 있어야 하며, 리스크 관리지침(내부관리기준)에 따른 보고 및 의사결정 절차를 거친 후 관련서류를 보관하여야 함

3 위탁계약 검토 및 체결

3-1. 위탁회사는 회사의 「리스크 관리지침(내부관리기준)」, 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」(이하 "규정") 및 「개인정보보호법」, 「신용정보 이용 및 보호에 관한 법률」, 「전자금융거래법」 등 관계법규에서 정하고 있는 물리적·기술적·관리적 보호조치 등의 요구사항과 금융감독기관 권고사항이 준수·보장될 수 있는 수탁회사를 선정하여야 하며 이러한 수탁회사의 의무가 이행되도록 위탁계약을 체결하여야 함

① 위수탁계약서(부대 문서를 포함하며 이하 "계약서")는 위탁의 제반 과정에 있어 가장 중요한 리스크 통제수단이므로 계약서의 중요성을 감안하여 다음 사항을 확인하여야 함

가. 계약서는 법적으로 구속력이 있는 문서로서 모든 위·수탁 관계를 포괄하도록 작성하여야 하며, 특수관계인(계열사 등)과 계약시에는 제공되는 서비스의 비용과 품질이 특수관계인이 아닌 경우 보다 떨어지지 않도록 해야 함

나. 계약서는 수탁회사가 유발할 수 있는 제반 리스크에 대한 통제수단과 서비스 제공의 균질성 및 연속성과 정보보호 및 보안통제 장치가 확보되도록 작성되어야 함

다. 계약서는 명확하게 작성되어야 하며, 각 당사자의 모든 권리와 책임(의무)을 명료히 정하여* 분쟁의 소지가 제거되어야 함

* 수탁회사의 주의의무 이행 및 위탁회사의 감독이 이루어 질 수 있도록 권리와 의무를 명확하게 규정하고, 합리적인 이유 없이 위탁회사에 불리한 조항이 포함되지 않도록 함

라. 계약서 작성 초기 단계부터 위탁회사 법률 전문가(부서)가 계약서에 대한 지속적인 법률검토를 실시하여야 함

3-2. 규정 별표1「표준계약내용」에서 정한 사항 외에 위탁리스크의 관리를 위해 계약서에 반영하여야 하는 기본적 사항은 다음과 같음

① (위수탁 범위) 계약서에 계약당사자의 권리와 책임(의무)을 명확히 명시해야 함

가. 위탁업무의 세부내용, 서비스수준 및 이행기간

나. 위탁회사 및 수탁회사의 위탁업무 관련 권리와 책임(의무)

다. 계약상 수행되는 기존 서비스를 변경할 경우 계약당사자의 권리와 책임(의무)

라. 다른 위탁업무의 추가 및 계약 재협상에 대한 사항 등

② (서비스수준 협약서) 위탁회사는 수탁회사가 제공하여야 하는 최소 위탁서비스 수준과 불이행에 대한 해결방안 등을 포함하는 서비스수준 협약서('Ⅵ. 5. 5-1.' 참조)를 위탁계약에 포함하여야 함

③ (상시 모니터링) 위탁회사는 수탁회사의 계약이행 준수와 위탁과 관련된 리스크를 관리·통제하기 위해 수탁회사에 대한 상시 모니터링('Ⅳ. 4.' 참조)을 실시하여야 하며 필요한 사항을 계약서에 반영하여야 함

④ (감사) 위탁회사는 수탁회사가 위탁회사의 리스크 관리지침을 준수할 수 있도록 감사 등 적정한 수단과 이행보장에 관한 다음 사항을 계약서에 포함하여야 함

가. 수탁회사가 위탁업무 수행시 발견한 리스크 요인과 내부감사* 결과를 위탁회사에 즉시 통지할 의무

* 위탁회사는 수탁회사가 위탁관련 사항에 대해 내부감사를 실시할 경우 위탁회사에 대한 사전통지, 감사사유, 감사범위, 위탁회사 요청시 공동감사 실시 허용, 내부감사 결과보고 등의 절차를 사전에 마련하고 수탁회사가 준수하도록 하여야 함

나. 위탁회사의 수탁회사 감사는 당해 업무가 위탁회사 내에서 처리되는 경우와 동일한 수준 또는 그 이상으로 이루어져야 하며, 수탁회사에 대한 감사빈도, 감사범위 및 감사권한 등을 구체적으로 명시

다. 위탁회사는 리스크 종류 및 중요도에 따라 수탁회사의 내부감사, 위탁회사의 감사 또는 외부감사에 의존*할지를 선택할 수 있으며, 위탁회사의 자료접근권 보장 및 수탁회사의 자료제출 의무를 명시

* 위탁회사는 중요하거나 기술적으로 복잡한 위탁의 경우 충분한 기술적 전문지식을 가진 독립된 제3자에게 의뢰하여 검증을 받게 할 수 있으며, 수탁회사의 내부감사 의존은 수탁회사 내부통제 운영의 적정성을 검토하여 해당 리스크 통제가 확보될 경우에만 허용됨

라. 수탁회사의 위탁서비스 성과와 리스크 관리(내부감사 포함)가 기대에 미치지 못하는 경우 위탁회사의 적시개입 및 시정조치가 가능하도록 보장하는 내용

마. 위탁회사는 개방형 네트워크(인터넷 관련 서비스 등) 접근권과 관련된 서비스의 보안에 대해 각별한 관심을 기울이고, 전문성을 지닌 독립적인 제3자 또는 위탁회사 부서가 주기적으로 점검 및 통제를 실시(해킹 탐지, 방화벽 배치 및 기타 독립적인 통제를 포함)할 수 있다는 내용

바. 계약의 이행과 관련된 위탁회사의 권고·지시(상시모니터링 및 감사결과에 따른 시정·규제요구 사항 포함)를 수탁회사가 성실하게 이행할 의무

⑤ (보고서) 위탁회사가 제공 받을 보고서의 제출빈도 및 종류(위탁업무 서비스 제공 관련 내부통제·감사, 정보보호·보안통제 장치 및 테스트 보고서, 재무제표 등)에 대한 내용을 명시하여야 함

⑥ (업무연속성 계획) 위탁업무의 연속성 확보를 위한 수탁회사 등의 백업 및 기록보호(프로그램 및 데이터파일, 재난복구 및 비상계획 유지 등)에 대한 책임 등과 관련된 업무연속성 계획('Ⅵ. 5. 5-2.' 참조)을 계약서에 포함하여야 함

가. 업무연속성 계획을 정기적으로 테스트하고 테스트 결과를 위탁회사에 제공하여야 하는 수탁회사의 책임

나. 위탁업무의 연속성 확보에 차질이 발생할 경우 적용하여야 하는 업무 운영절차가 명시된 비상계획서를 수탁회사가 위탁회사에 제공할 책임

다. 수탁회사의 파산 등으로 인한 계약의 유지 불능 또는 통신문제 등 우발상황 발생시 리스크 관리대책에 관한 사항

⑦ (정보보호) 위탁회사의 내부관리기준과 정보보호·보안통제 관련 법규 및 금융감독기관의 권고사항 등 위탁회사가 준수하여야 하는 정보보호·보안통제 절차를 수탁회사도 동일하게 준수하여야 하는 의무

⑧ (수탁회사의 재위탁 하도급계약) 위탁회사의 동의 없이 수탁회사가 제3자(하도급계약자)에게 재위탁하는 것은 금지되며, 재위탁이 가능한 경우 위탁회사는 하도급계약자에 대한 재위탁 리스크를 분석·평가하고 발생 가능한 리스크에 대한 관리·통제 계획을 수립하여야 하며 이를 경영진(필요시 이사회)에 보고하여야 함

가. 위탁회사가 재위탁에 동의할 경우에는 재위탁의 필요성, 효과, 제반 리스크 분석 및 통제·이행방안을 검토하여 의사결정(문서화)을 하여야 하며, 위탁회사는 수탁회사에 대해 적용하였던 동일한 수준의 계약내용(권리와 책임·의무 등), 리스크 관리절차, 법규준수 의무가 재위탁에도 적용*되도록 하여야 함

* 위탁회사는 재위탁 되는 정보처리 및 전산설비의 중요성, 위탁 규모, 복잡성 등을 고려하여 수탁회사 및 하도급계약자에 대해 차별화 되고 강화된 계약내용 및 리스크 관리절차가 적용되도록 하여야 함

나. 수탁회사가 재위탁 계약을 맺을 경우 위탁회사가 하도급계약자에 대해 필요한 사항에 대한 보고를 받고 이를 통제할 수 있는 권한을 보유하는 등 원 계약서, 리스크 관리절차, 법규 상의 수탁회사 의무를 하도급계약자도 동일하게 승계하도록 하여야 함

다. 수탁회사는 하도급계약자의 작업내용에 관계없이 원 계약서에 명시된 위탁서비스 제공에 대한 책임을 져야 함

라. 수탁회사는 원 계약서의 위탁회사와 동일한 수준으로 하도급계약자에 대한 재위탁 리스크를 분석·평가하고 관리하여야 하며, 계약 준수에 영향을 미칠 수 있는 하도급계약자의 사정변화(핵심인력, 기술, 재무, 정보보호, 보안 및 기밀유지 등)를 위탁회사에 즉시 통지하여야 하는 의무를 계약서에 포함하여야 함

⑨ (비용) 위탁업무 서비스 제공 및 유지·관리·통제 등에 대한 수수료 및 계산에 대한 사항을 계약서에 명시*하고 세부내용을 문서화 하여야 함

* 계약서에는 하드웨어와 소프트웨어 구매·유지 책임 및 추가비용에 대해서도 명시하여야 하며, 비용구조가 변화하는 상황(비용증가에 대한 제한 등)도 상세히 기술

⑩ (소유권 및 라이센스) 계약서에는 위탁회사의 데이터, 장비, 하드웨어, 시스템 문서, 시스템 및 응용소프트웨어, 기타 지적재산권 등에 대한 소유권 및 사용에 관한 사항을 포함되어야 함

가. 수탁회사에 이전되거나 생산되는 모든 데이터는 정보처리, 저장, 복사, 재생산 방법에 상관없이 모두 위탁회사 소유이며, 기타 지적재산권에는 회사의 명칭, 로고, 트레이드마크, 저작권 보호자료, 도메인 이름, 웹사이트 디자인, 수탁회사가 위탁회사를 위해 개발한 기타 작업결과물 등이 포함됨

나. 계약의 종료(계약기간 만료 또는 중도해지 포함)시에 위탁회사가 자신의 데이터 등을 적시에 회수할 수 있는 권리를 명확하게 기술

⑪ (기간) 위탁회사는 계약기간과 갱신기간 협상시 정보처리 및 전산설비 기술의 종류 및 해당 산업의 현재 상태 및 산업변화 속도 등을 고려하여 결정하여야 함

⑫ (분쟁해결) 신속히 문제를 해결하고자 하는 분쟁해결 절차에 관한 사항뿐만 아니라 분쟁해결 기간 동안에도 수탁회사가 지속적으로 서비스를 이행할 수 있도록 하는 내용을 포함하여야 함

⑬ (계약종료) 위탁계약 종료에 대한 위탁회사의 권한 및 수탁회사의 책임(의무), 계약종료 통지 등의 내용을 포함하여야 함

가. 위탁회사는 인수·합병, 비용 증가, 수탁회사의 서비스·정보보호·보안 통제장치 불충족, 위탁회사의 위탁서비스 유지와 정보보호·보안통제 관련 권고·지시사항의 수탁회사 불이행, 재무건전성 악화, 파산 등 다양한 조건별 종료 및 조기종료(중도해지) 권한을 계약서에 명시

나. 계약의 종료에 따른 위탁회사의 데이터 적시 회수, 데이터 파기계획(파기 확인서 징구) 및 불이행시 패널티(손해배상 등), 종료 통지요건 및 종료의 사전통지 일정과 계약전환과 관련된 수수료·비용에 대해 명시

다. 위탁회사는 수탁회사의 정보보호 및 보안통제 문제, 재무건전성 악화 및 파산 등으로 인한 계약 조기종료(중도해지 포함)시 위탁서비스 유지를 위한 비상계획 수립과 이행 및 수탁회사의 관련 책임(의무)사항을 명시

4 수탁회사 관리·감독

4-1. 위탁회사는 수탁회사가 위탁계약과 관련된 리스크 관리, 법규준수 의무를 이행할 능력을 보유하고 있는지와 수탁회사의 업무환경 및 내부사정 변화에 따른 잠재적 리스크 변화를 상시 모니터링하고 관리·통제하여야 함

① 위탁회사는 위탁관련 사항을 감시하는데 충분한 인적·물적 자원을 투입하고, 상시 모니터링을 위한 감시책임의 소재를 명확히 하여야 함

② 위탁회사는 상시 모니터링 담당자(부서) 지정, 역할 및 책임, 제반 리스크 통제활동을 문서화하고 경영진(필요한 경우 이사회)에 보고하는 체계를 구축하여야 하며, 상시 모니터링 결과에 대한 평가 및 조치방안(감사 연계 등)을 마련하여야 함

③ 위탁회사는 위탁회사 내에서의 모니터링, 수탁회사 상주 모니터링, 수탁회사 자체 모니터링 활용 등 다양한 상시 모니터링 수단을 선택*하여 발생 가능한 리스크를 사전에 분석 및 관리할 수 있도록 주의의무를 다하여야 함

* 위탁회사는 위탁되는 정보처리 및 전산설비의 중요성, 위탁 규모와 복잡성 등을 고려하여 상시 모니터링 활동수단(수탁회사 상주 모니터링 등)을 선택(의사결정)

4.2. 위탁회사는 수탁회사가 계약상의 서비스를 안정적으로 제공하도록 리스크 통제의 적정성과 정보보호 및 법규 준수 여부를 점검하고 보완·개선 등의 조치를 적시에 취할 수 있도록 상시모니터링 체계를 구축*하여야 함

* 상시모니터링은 금융회사가 위탁되는 정보처리 및 전산설비의 중요성, 위탁 규모와 복잡성 등을 고려하여 실효성 있는 방안(상시모니터링 주기 포함)을 채택

① 상시 모니터링 프로그램은 계약관계 및 리스크 관리의 핵심부분을 대상으로 효과적이고 실효성 있게 가동되도록 구체화 되어야 함

② 위탁회사는 상시 모니터링, 내부통제 및 감사결과 등을 종합하여 주기적으로 수탁회사를 평가하여야 하며, 이를 통해 어떤 수탁회사 또는 어떤 서비스 부문이 보다 면밀한 상시 모니터링을 필요로 하는지 결정*하여야 함

* 리스크가 높다고 평가받은 수탁회사는 수탁 수주실적(재무건전성 포함), 정보보호, 규제준수 및 리스크 관리에 대해 더욱 빈번하고 엄격한 상시 모니터링을 받아야 하며, 필요한 경우 실사실시 및 독립적인 외부 제3자를 통한 검증방안도 고려되어야 함

③ 위탁회사는 계약 체결, 갱신, 중도해지 등 계약의 전환시와 수탁회사에 대한 감사 및 비상계획 수립시 상시모니터링 결과를 활용하여야 하며, 필요한 경우 위탁계약 및 비상계획 등을 적시에 변경하여 위탁서비스의 균질성과 연속성 및 정보보호·보안통제 등이 확보되도록 하여야 함

④ 위탁회사의 이용자집단(부서)은 서비스 이용 과정 자체가 수탁회사를 상시 모니터링하는 또 하나의 유효한 수단임을 인식하고 이를 모니터링에 활용하여야 함*

* 상시 모니터링은 이용자집단의 위탁서비스 이용에 따른 업무의 불편성, 문제점, 개선 요청 사항 등의 의견수렴을 병행하여야 함

4.3. 위탁회사의 수탁회사에 대한 상시 모니터링은 기본적으로 다음과 같은 사항이 고려될 수 있음

① 위탁계약서에 부대한 서비스수준 협약서의 주요 내용

가. 서비스수준 협약서 운영 전략 및 목표 수립 등을 위한 공식적인 정책과 이행

나. 서비스수준 협약서 이행상황에 대한 상시 모니터링 프로세스

다. 서비스수준 협약서 불이행에 대한 페널티 적용 등 상환청구(recourse) 프로세스

라. 성과지표에 대한 단계적 확대 프로세스, 분쟁해결 및 종료 프로세스

② 수탁회사의 재무상황 악화는 수탁회사 내부통제의 약화 등 위탁 리스크의 주요 요인으로 작용하므로 다음 사항이 포함된 수탁회사 재무건전성의 상시 모니터링과 리스크 관리방안을 수립하고 이행하여야 함

가. 위탁회사는 위탁책임 이행을 위해 수탁회사의 재무적인 경영능력을 주기적으로 판단하여야 하며, 수탁회사의 재무상황이 악화되고 있거나 불안정해지고 있다면 상시 재무건전성 검토*를 시행

* 재무건전성 검토는 최소한 수탁회사의 재무제표에 대한 분석내용을 포함하며, 수탁회사의 재무상황을 판단하기 위해 제3자의 각종 분석보고서 및 언론보도 내용 등을 활용

나. 위탁회사는 수탁회사의 재무상황 악화 또는 내·외부 상황으로 인해 내부통제가 정상적으로 작동하지 아니하여 위탁서비스 이행에 부정적 영향을 미칠 정도로 불안정하거나 악화되고 있다는 것을 인지할 경우 비상계획을 이행*

* 수탁회사가 적절한 금융데이터를 제공하지 않는 경우 등에는 수탁회사의 서비스 제공 안전성에 심각한 문제가 발생했을 수 있다는 신호로 볼 수 있다는 내용을 계약서에 반영

다. 위탁회사는 수탁회사가 파산하거나 재무건전성 및 내부통제 문제 등으로 인해 비상계획 이행이 필요한 단계에 이를 경우 리스크 관리절차에 따라 다각적인 방안*으로 대응하여야 하며, 관련 업무수행 및 위탁서비스 제공에 차질이 없도록 제반절차에 대한 법률적 검토를 사전에 완료

* 외부전문가를 고용하여 위탁서비스 센터 운영, 위탁업무 처리를 위해 필요한 장비와 소프트웨어를 입수, 데이터 파일을 다른 제공자에게 이전, 수탁회사 변경 등

③ 위탁회사는 수탁회사와 관련된 리스크를 효과적으로 감시하기 위해 다음 사항을 포함하여 수탁회사의 내부통제(정보보호·보안통제, 교육실시 등) 및 리스크 통제환경의 적정성을 상시 모니터링하고 평가하여야 하며, 미흡한 사항에 대하여는 적시에 대응방안을 마련·실행하여야 함

가. 위탁회사는 수탁회사가 적절한 정책, 절차, 기준을 개발하고, 위탁업무의 문제점과 리스크를 사전에 발견하여 예방·조치할 수 있는 기술력과 내부통제 등의 환경을 갖추고 있는지 평가

나. 수탁회사가 위탁업무와 관련된 내부통제 절차를 이행할 수 있도록 하여야 하며, 위탁회사는 상시 모니터링 또는 이용자그룹의 평가내용 등을 검토하여 수탁회사에 시정 요구사항 등을 통지하고 그 결과가 반영되었는지 평가

다. 위탁업무와 관련된 수탁회사의 자체 내부감사 실시에 대한 적정성 및 문제점 해소능력과 자체 감사주기 등을 검토하고, 수탁회사의 부정이나 고의적 조작으로 인해 위탁회사가 손실을 입지 않도록 하기 위해 수탁회사 자체 내부감사의 실효성을 점검

라. 위탁회사는 수탁회사의 위탁업무 처리관련 전산시스템의 신뢰성, 안전성, 보안성, 효율성과 내부통제 적정성을 제고하기 위하여 주기적 또는 비주기적으로 필요한 시스템 감사(예시 : 컴퓨터 주변감사, 컴퓨터 처리과정 감사, 컴퓨터 이용 감사 등) 및 상시 모니터링을 수행하고 평가를 실시

- 컴퓨터 주변(around-the-computer) 감사 : 정보처리 과정에 관계없이 입·출력 자료만을 대상으로 감사

- 컴퓨터 처리과정(through-the-computer) 감사 : 컴퓨터 처리 대상이 광범위하고 그 내용이 복잡할 때 내부통제 질문서와 시스템 순서도 및 매뉴얼 등을 통해 감사

- 컴퓨터 이용(with-the-computer) 감사 : 컴퓨터 처리내용이 고도로 복잡화되었을 때 실제로 컴퓨터를 사용하여 자료처리를 시연

5 서비스 수준 및 업무 연속성

5-1. 위탁회사는 서비스수준 협약서*(Service Level Agreement, 이하 “SLA”)를 계약서에 포함시켜 수탁회사가 제공하여야 할 위탁서비스의 성과 목표치를 구체적으로 명시하고 책임을 명확히 하여야 함

* 위탁회사가 요구하는 서비스에 대한 정의·범위 및 수준, 서비스 제공과 관련된 수탁회사의 책임 및 의무사항, 서비스에 대한 평가방법 및 평가결과에 대한 후속조치 등에 대해 위탁회사와 수탁회사가 맺은 협약서를 의미

① 위탁회사는 수탁회사가 목표한 성과 미달에 따른 피해를 최소화하기 위해 SLA를 위탁계약서의 내용으로 포함하여야 함

가. SLA을 통해 서비스의 양과 질을 측정할 성과지표를 정형화하여야 하며, 수탁회사가 제공하는 서비스 수준을 측정하기 위한 중요 평가요소를 포함* 하여 SLA를 작성

* 평가요소는 수탁회사의 업무(예: 프로세스 오류 비율, 시스템 가동시간 등) 및 조직(예 : 담당자 변경) 등을 반영하며, 해당 요소의 성과를 객관적으로 측정하는 방법을 마련

나. 위탁회사는 측정빈도 및 수탁회사의 SLA 위반에 대한 허용 가능한 범위를 결정

다. 다음의 주요사항을 SLA에 포함하여야 함

- 서비스 가용성 및 추진 일정
- 데이터 기밀성 및 무결성
- SLA에 영향을 주는 사항에 대한 변경 통제
- 보안기준 준수(취약성 및 침해 관리)
- SLA 불이행에 대한 페널티 적용 등 상환청구 프로세스
- 업무 연속성 준수
- 헬프데스크 지원

라. 업무 연속성을 위해 SLA를 통해 데이터 백업 및 보존, 데이터 보호, 재해복구 및 비상계획 유지 등에 대한 수탁회사의 계약상의 책임을 측정

- 정기적으로 비상 대응훈련을 실시하도록 하고 계약서나 SLA에서 수탁회사의 비상계획 실행의무를 면제해 주는 예외 조항은 배제되어야 함

② 위탁회사는 수탁회사의 업무위탁 서비스 운영전략 및 목표 수립 등 공식적인 업무수행방침과 그 이행이 SLA와 부합되도록 하여야 함

③ 위탁회사는 모든 가능한 가격결정(pricing) 옵션*을 고려하여 계약에 가장 적절한 방법을 선택하여야 함

* 고정·변동 가격, 특정 서비스별 가격, 인센티브 기반 가격, 물가 변동 등

④ 위탁회사는 자신에게 불리한 영향을 주는 조항이나 유인책을 포함하는 서비스 계약을 체결하지 말아야 함*

* 계약기간 연장(최대 10년) 및 계약 이후 부적정한 비용의 급격 증가 등 불리한 계약조항이나 위탁회사나 수탁회사 자산에 대한 부당한 손실 이연 및 비용 인식 회피 등을 통해 부적정 하게 자산(자본)을 유지하거나 증가시키는 유인책 등을 포함

5-2. 위탁회사는 위탁업무의 연속성을 보장하기 위한 업무연속성계획(Business Continuity Plan, 이하 “BCP”)에 다음과 같은 방안을 수립하고 이행하여야 함

① 위탁회사는 상시 모니터링 프로그램에 BCP의 중요사항을 반드시 포함하여 위탁서비스와 관련된 리스크(정보보호 리스크 포함)를 통제하도록 하여야 함

② 정보보호와 BCP의 측면에서 모든 당사자의 책임을 구체화 하고, 위탁회사는 어떤 서비스를 제3자(주요 통신 및 네트워크 서비스 제공자 포함)에게 위탁업무를 의존하고 있는지 파악 하여야 함

③ 위탁회사는 모든 수탁회사가 수행하고 있는 업무를 이해하고 이를 회사의 BCP에 통합시켜야 하며, 수탁회사는 주기적으로 동 계획을 테스트하여야 함

가. 수탁회사는 모든 테스트 계획 및 결과를 위탁회사에 보고하여야 하고, BCP에 영향을 미칠 수 있는 업무 변경시 위탁회사에게 관련내용을 사전 통지하고 협의하여야 함

나. 위탁회사는 수탁회사의 BCP를 위탁회사의 계획에 통합시키고, 통합된 계획을 유지하며 주기적인 검토를 실시하여야 함

다. 위탁회사는 BCP를 통해 회사 내부에서 수행되는 업무 이외에 수탁회사가 개발하거나 위탁하는 업무에 대해서도 BCP에 영향을 미치는지 여부를 확인하여야 함

라. 다수의 수탁회사 관계가 효과적으로 관리되도록 BCP를 수립 및 이행하여야 함

마. 수탁회사는 현재의 데이터와 프로그램을 대체 site에 보관하고 다른 장소에서 처리할 수 있도록 하여야 하며, 위탁회사의 BCP는 수탁회사의 BCP를 보완하도록 하여 서비스 공백이 발생하지 않도록 하여야 함

④ 위탁회사는 자연재해, 장애 등*에 대비하기 위해 중요 데이터 및 처리기능에 대한 백업을 준비하여야 함

* 자연재해, 사고, 소프트웨어 장애, 하드웨어 장애, 시설 정전, 정치·경제·사회적 불안정 등

가. 데이터 통신시스템이 작동하지 않는 경우에도 효과적인 백업절차를 통해 데이터 처리의 계속 수행이 가능하도록 하며, 다양한 옵션*을 고려하여 조치하여야 함

* 실시간 처리 보다는 일괄처리 방법을 이용, 컴퓨터를 오프라인 모드에서 운영, 통신회선 이상 발생시 제어기에서 데이터를 캡쳐, 여분의 데이터 통신회선과 백업 모뎀 및 국내 통신회사가 재설정한 회로를 통해 통신회선 변경 등

나. 내부적으로 데이터 캡쳐 및 기타 기능을 수행하는 위탁회사는 대체 site나 기타 수단을 백업 계획에 명시하여 동 기능들을 복구·지속할 수 있도록 조치하여야 함

다. 종합적인 백업계획을 마련하여 인력과 장비를 어떻게 획득하고 사용할 것인지에 대한 절차를 자세히 명시하여야 함

라. 주기적으로 백업 능력을 테스트하여 보호조치를 마련하고 관련 임직원이 백업계획을 숙지하여야 함

⑤ 위탁회사는 BCP와 관련하여 다음 사항을 이행하여야 함

가. 수탁회사의 BCP를 정기적으로 검토하여 '핵심업무'로 간주되는 서비스가 적절한 기간 내에 복구될 수 있도록 조치

나. 수탁회사의 BCP 테스트 프로그램을 검토하고, 중요 서비스에 대해서는 BCP를 정기적(연 1회 이상)으로 테스트하는 것이 필요

다. 핵심업무 서비스 및 응용프로그램에 대한 수탁회사의 상호 연관성을 평가

⑥ 위탁회사는 정보처리 및 전산설비 위탁과 관련된 적정한 비상계획을 수립하여야 함

가. 위탁회사는 위탁된 모든 서비스에 관한 비상계획을 수립해 두고 정기적으로 모의훈련을 실시

나. 위탁서비스가 중단되는 경우 당해업무의 복구상황을 관리하고 금융이용자 보호에 미치는 영향 등을 평가하는 등 리스크를 관리·통제할 책임 있는 팀(부서) 또는 문제해결을 위한 임시조직을 구성

⑦ 위탁회사는 BCP를 마련하고 이행하여야 하며, 전체 또는 일부를 위탁하는 경우에는 다음 사항을 추가적으로 반영하여야 함

가. (인력) 수탁회사는 적절한 현장 기술지원 자격을 갖춘 직원을 고용하여 복구 장소에서 시의 적절하게 운영이 재개될 수 있도록 해야 함

나. (처리시간 가용성) 수탁회사는 충분한 처리시간, 자원, 보안통제를 배분하여 다수의 고객이 존재할 가능성에 대비해야 하며, 위탁회사는 일정 시간 안에 적정한 양의 업무를 처리할 수 있도록 하여야 함

다. (접근권) 수탁회사는 접근 제한사항을 모두 공개해야 하며, 비상시 또는 위탁회사가 위탁업무 수행 및 점검을 위해 필요로 하는 경우 위탁회사가 site를 사용할 수 있도록 하여야 함

라. (하드웨어와 소프트웨어) 복구 site에 호환성 있는 하드웨어와 소프트웨어를 갖추어야 함

- 위탁회사는 site의 인프라(공급전력, 네트워크 등) 상태가 해당 하드웨어와 소프트웨어 가동에 충분한지 상시 모니터링

- 상시 모니터링을 강화하기 위해 수탁회사는 계약에 따라 복구 site의 하드웨어, 소프트웨어, 장비에 있어서의 변화를 위탁회사에 통지해야 함

마. (보안 통제) 위탁회사는 복구 site에 적절한 물리적, 논리적 보안통제를 유지할 수 있도록 하여야 함

바. (테스트) 주기적 테스트를 위한 복구 site에 대한 접근권을 계약서에 명시하여야 함

- 위탁회사는 복구 site에 대해 적어도 1년에 한번 이상 전면적인 테스트(통신 능력에 대한 확인 등)를 실시할 수 있는 권한이 필요

- 수탁회사가 자체 BCP를 주기적으로 테스트하고 테스트 결과를 위탁회사에 제출하도록 요청

아. (통신) 위탁회사는 위탁회사와 복구 site간 통신 설정 방법 등 복구 site의 통신 용량을 검토

- 수탁회사는 복구 site가 모든 고객에게 충분한 통신 서비스(데이터, 음성 등)를 제공할 수 있도록 조치를 취해야 함

자. (상호 합의) 다른 회사와 복구 site에 관한 계약을 체결하는 위탁회사는 인력, 처리 가용성, 복구 또는 테스트를 위한 접근권, 호환성, 보안, 용량 등의 내용을 고려

- 양 계약당사자는 일방 당사자가 복구작업 수행시 다른 상대방은 복구 목표시간과 최소서비스 수준을 달성할 수 있도록 충분한 용량을 유지

차. (공간) 복구 site는 피해를 입은 위탁회사의 복구 직원에게 제공할 수 있는 충분한 공간을 확보해야 함

카. (인쇄 용량·능력) 복구 site는 충분한 인쇄 용량을 유지하여 피해를 입은 위탁회사에 적절한 수준의 서비스를 제공할 수 있도록 해야 함

타. (연락망) 위탁회사는 재난선언 책임자와 복구 site 가동개시 선언 책임자 등을 포함한 재난선언절차를 구비하고 있어야 함

- 복구 site 제공자의 이름과 연락처를 보유하고 제공자와의 소통 절차

- 위탁회사는 위탁한 재난복구 서비스를 주기적으로(연 1회 이상) 철저히 테스트

6 정보보호 및 보안통제 등

6-1. 위탁회사는 위탁된 정보가 충분히 보호되도록 물리적·기술적·관리적 보호·보안조치와 리스크 통제 및 점검 대책을 마련하고 이행하여야 함

① 위탁회사는 수탁회사 선정시 위탁된 정보가 보호될 수 있는지 수탁회사의 정보 보호 및 보안 통제환경과 안정성 확보조치에 대한 실사를 실시하는 등 충분한 주의의무를 다하여야 함

- 위탁회사는 수탁회사가 영업데이터 및 고객데이터 관리에 있어 철저한 보호조치를 이행하도록 적정한 통제장치를 마련하고 지속 점검하여야 함

② 위탁계약을 체결하기 전과 위탁계약기간 중 위탁회사는 수탁회사의 물리적·기술적·관리적 정보보호 및 보안통제 적용기준이 관련법규 또는 금융감독기관이 요구하는 기준을 충족하거나 더 높은 수준을 유지할 수 있도록 하여야 함

- 위탁회사는 수탁회사가 정보보호 및 보안통제와 관련하여 위탁회사의 내부관리기준과「개인정보보호법」,「신용정보 이용 및 보호에 관한 법률」,「전자금융거래법」 등 관련 법규에서 규정하고 있는 사항 및 금융감독기관의 권고사항에 대하여 충분히 이해하고 있는지 주기적으로 확인 및 교육을 실시하고, 관련된 모든 보호·보안조치를 이행하도록 하여야 함

③ 위탁회사는 수탁회사가 위탁된 업무 수행에 필요한 정보 및 시스템에 대해서만 접근권을 가지도록 통제·관리하고 관련사항에 대한 상시 모니터링 방안을 마련하고 운영하여야 함

가. 위탁회사는 위탁업무와 관련된 수탁회사의 시스템 및 정보에 대해 제한없이 접근이 가능하여야 하며, 정보보호 교육 등을 포함한 정보보호 및 보안 조치를 지속적으로 강구하고 수탁회사가 이를 준수하도록 하여야 함

나. 위탁회사는 수탁회사가 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하도록 하여야 하며, 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 보관하여야 함

다. 위탁회사는 수탁회사의 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우에는 처리일시, 처리내역 등 접속기록을 저장하여 보관·관리하고 이를 월 1회 이상 정기적으로 확인·감독하도록 하여야 하며, 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관토록 하여야 함

라. 위탁회사는 수탁회사로 하여금 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 및 보안통제 절차를 수립·운영하여야 하며, 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관토록 하여야 함

④ 위탁회사는 수탁회사가 위탁된 시스템에 대해 해킹 등 전자적 침해행위로부터 보호될 수 있도록 다음 사항의 대책을 수립·운용하도록 관리하여야함

가. 해킹 등 전자적 침해행위에 기인한 사고를 방지하기 위해 정보보호시스템을 설치 및 운영하되 정보보호시스템에 대한 원격관리를 금지하고 주기적으로 운영 상태를 점검할 것

나. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항을 적시에 실시

다. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지

라. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것

마. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것

바. 해킹 등 전사적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 비상연락망 및 대응체계 등을 갖출 것

사. 정보보호시스템에 대한 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것

6-2. 위탁회사는 위탁 처리되는 정보의 보호를 위한 안전성 확보조치의 구체적 내용을 홈페이지 등을 통해 공시하여야 하며, 특히 민감정보의 처리를 위탁할 경우에는 정보주체에게 서면, 팩스, 전화(휴대전화 문자메시지를 포함), 전자우편 또는 이에 상당하는 방법으로 민감정보의 처리목적, 처리기간, 처리범위, 처리자 등 위탁내용을 개별 고지*하여야 함

*「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제5조②에 따라 위탁회사는 민감정보의 처리 위탁시 정보주체에게 개별 고지하여야 함

6-3. 위탁회사는 전산장비가 위치하는 전산실에 대하여 기본적으로 다음 사항을 확인하고, 전산실의 안정성 및 보안성이 확보될 수 있도록 수탁회사를 통제하여야 함

① (건물) 건물 출입구는 경비원에 의해 통제하고 출입통제 보안대책을 수립·운용하고 번개, 과전류 등 고전압에 의한 피해예방을 위한 피뢰설비를 갖출 것

- 전산장비 및 통신장비 등의 중량을 감안한 적재하중 안전대책을 수립·운용하고 화재발생에 대비하여 자동소화설비, 배연설비 등을 갖출 것

② (전원, 공조 등 설비) 전원실, 공조실 등 주요 설비시설에 출입통제 장치를 설치하고 적절한 감시제어시스템을 갖출 것

가. 전산실의 전력공급 중단에 대비하여 자가발전설비 및 무정전전원장치(UPS)를 갖추고 과전류, 누전에 의한 장애 방지를 위하여 누전경보기 및 일정한 전압 및 주파수 유지를 위한 정전압정주파수장치(CVCF)를 갖출 것

나. 공조 설비 상태 점검을 위한 압력계, 온도계 등을 갖추고 전산실에 24시간 적정한 온도 및 습도를 유지하기 위한 자동제어 항온·항습기를 갖출 것

③ (전산실에 관한 사항) 출입문은 이중 안전장치로 보호하며, 출입자 관리 대장 기록·관리 및 CCTV 설치 등으로 출입자에 대한 사후확인이 가능하도록 할 것

가. 천정·바닥·벽의 침수로 인한 전산장비의 장애가 발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등의 조치를 취할 것

나. 적정온도 유지를 위하여 온도·습도 자동기록장치 및 경보장치를 설치하고 케이블 보호를 위한 전용 통로관 설치 및 정전에 대비하여 조명설비 및 휴대용 손전등을 비치할 것

다. 다수의 기관이 공동으로 이용하는 집적정보통신시설(IDC)에 전산장비를 설치하는 경우 미승인자가 접근하지 못하도록 적절한 접근 통제 대책을 갖출 것

6-4. 국외위탁은 해당 국가의 고유 위험(국가리스크)과 국가간 감독규제의 상충, 정보보호·보안통제, 상시 모니터링·감사 및 정보접근성 저하 등 다양한 리스크를 유발할 수 있으므로 위탁회사는 관련 리스크를 면밀하게 분석, 평가하고 예방 및 통제할 수 있는 리스크 관리시스템을 구축하여야 함

① 국가리스크는 수탁회사 소재 국가의 정치·경제·사회적 상황에 의한 제반 리스크를 의미하며, 관련 리스크는 수탁회사의 위탁서비스 제공수준에 부정적인 영향을 미칠 수 있으므로 위탁회사는 국가리스크에 대한 관리 및 대응방안*을 마련하여야 함

* 위탁회사는 국가리스크를 관리하기 위해 국외의 정치·경제·사회적 상황과 사건에 대한 모니터링 및 평가를 실시하여야 하며, 국가리스크 관리방안에는 예상치 못한 서비스 중단에 대비한 비상대책, 위탁서비스의 연속성 확보, 출구전략 수립 등이 포함되어야 함

② 위탁회사는 국외위탁이 금융이용자 보호에 미치는 영향과 지리적 거리(물리적 시간소요)*, 언어, 사업관행, 법·규제 등과 관련된 리스크를 파악하고, 국외위탁에 따른 관리·감독(상시 모니터링·감사 등) 비용을 포함한 리스크를 고려하여야 함

* 대한민국 감독기관과 위탁회사의 지시·요구사항이 국외 수탁회사에 즉시 전달되어 이행되고, 국외 수탁회사의 이행여부를 점검·확인하는데 소요되는 물리적 시간과 장애를 테스트하고 이를 해소할 수 있는 리스관리 방안(의사소통 채널 확보 등) 을 마련

③ 위·수탁회사는 국외위탁의 경우에도 이 리스크지침에서 규정하고 있는 권리·의무 등 제반 리스크 통제절차를 동일하게 준수하여야 하며, 특히 개인식별정보가 국외로 이전될 경우에는 「개인정보보호법」, 「신용정보 이용 및 보호에 관한 법률」, 「전자금융거래법」 등 관계법규에서 정하고 있는 물리적·기술적·관리적 보호조치 등 요구사항과 개인식별정보 암호화 및 비식별화 등 금융감독기관의 권고사항이 준수·보장되어야 함

④ 위탁회사는 위탁과 관련하여 한글로 번역된 제반 문서를 보관하여야 하며, 동 문서에는 계약서(부속서류 포함), 계약서에 대한 법률검토 의견, 실사보고서, 수탁회사에 대한 상시 모니터링과 감사 및 리스크 통제활동(경영진 및 이사회 보고내용 포함), 수탁회사 재무제표와 기타 중요 보고서가 포함됨

⑤ 위탁회사의 국외 수탁회사 이용이 대한민국 감독기관의 위탁회사 및 수탁회사에 대한 감독·검사권한을 훼손하여서는 안 됨

- 위탁업무와 관련된 수탁회사, 데이터 또는 정보 등에 대한 대한민국 감독기관의 감독·검사권한을 제한하는 위탁계약 체결은 금지됨

- 위탁회사의 국외 위탁과 관련된 법률검토 의견에는 수탁회사 소재지 국가의 법률·규제와 계약내용이 대한민국 감독기관의 감독·검사권한 확보를 제한할 수 있는 지에 대한 검토 내용을 포함하여야 함

⑥ 계약서에는 수탁회사에 대한 대한민국 감독기관의 자료제출 요구, 정보접근 등 위탁업무와 관련된 감독기관의 감독·검사에 대하여 수탁회사의 성실한 협조와 수용(자료제출의 정확성과 적시성 준수 포함) 의무를 포함하여야 함

⑦ 국외 감독기관의 감독 및 규제를 받는 수탁회사는 위탁 서비스와 관련하여 국외의 감독기관에 의한 감독·검사 등 정보를 대한민국 감독기관과 위탁회사에 즉각적으로 제공하여야 하며, 동 내용을 계약서에 포함시켜야 함

⑧ 대한민국 감독기관과 국외 감독기관 간의 협약 등에 따라 수탁회사에 대한 감독·검사 등이 이루어질 경우에도 위탁회사와 수탁회사는 이에 성실하게 협조하여야 하며 동 내용을 계약서에 포함시켜야 함

⑨ 이 조항(6-4 조항)에 따라 계약서에 명시한 국외 수탁회사의 의무가 적정하게 이행되지 않을 경우 위탁회사는 별도의 위약금 등 불이익이 없이 위탁계약을 해지할 수 있도록 계약을 체결하여야 하며, 감독기관의 감독·검사결과 규정과 이 지침 또는 계약상의 의무를 위배하여 수탁회사로서 그 업무를 계속적으로 수행하는데 문제가 있다고 판단될 경우에는 즉시 계약관계를 종료하고 데이터를 회수하는 등 사후관리에 최선을 다하여야 함