대한민국 금융기관을 위한 마이크로소프트 클라우드 컴플라이언스 체크리스트

작성일: 2020 년 3 월

목차

서문: 대한민국 금융기관을 위한 클라우드 컴플라이언스 체크리스트

개요

인공지능(AI)과 빅데이터 애플리케이션의 급격한 발전은 컴퓨팅 능력과 데이터 가용성의 향상과 맞물리면서 산업 전반에 걸쳐 AI 의 도입이 확대되는 결과를 낳고 있습니다. 금융서비스 산업 역시 예외는 아니며 금융회사들이 다양한 분야에서 AI 를 도입하고 있고, 클라우드 컴퓨팅은 이러한 추세에 필수적이며 대한민국 내 금융회사들 사이에서 예외적인 현상이 아닌 표준으로 빠르게 자리를 잡아가고 있습니다.

다른 모든 기술적 진보와 마찬가지로 클라우드 컴퓨팅 역시 상당한 이점을 제공하지만 그와 동시에 금융회사들이 헤쳐 나가야 할 복잡하고 생소한 환경을 만들기도 합니다. 금융회사들은 클라우드로 전환하기에 앞서 클라우드 서비스 제공자로부터 지금껏 유례가 없는 높은 수준의 보장을 당연히 원하고 기대하고 있습니다. 금융감독원(**FSS**)과 금융위원회(**FSC**)는 2018 년 12 월 합동 보도자료를 통해 금융서비스 산업의 디지털 변혁을 도모할 목적으로 클라우드 컴퓨팅을 확대하기 위해 규제를 완화하겠다는 강력한 의지를 보였으며 금융회사들이 클라우드 컴퓨팅을 이용하여 고유식별정보와 개인신용정보가 포함된 필수적인 정보까지도 처리할 수 있도록 허용했습니다.

Microsoft 는 대한민국 내 금융회사들을 상대로 일련의 신뢰받는 클라우드 서비스를 제공하기 위해 최선을 다하고 있습니다. Microsoft 는 방대한 업계 경험과 고객에 대한 이해 그리고 연구와 광범위한 파트너십을 바탕으로 금융회사 고객이 요구하는 수준의 보장을 제공할 수 있는 귀중한 식견과 차별화된 역량을 갖추고 있습니다.

본 체크리스트는 대한민국 내 금융회사들에 대한 Microsoft 의 약속을 담고 있습니다. 즉, 본 체크리스트는 대한민국 내 금융회사들이 관련 규제 요건을 준수하면서 Microsoft 클라우드 서비스를 도입할 수 있게 뒷받침할 목적으로 작성되었습니다.

본 체크리스트에는 어떤 내용이 포함되어 있는가?

본 체크리스트에는 다음과 같은 내용이 포함되어 있습니다.

1. 대한민국 내 관련 규제 요건을 소개하는 **규제 환경에 관한 개요**.
2. 규제 이슈들을 열거하고 그러한 사항들과 관련하여 Microsoft 의 클라우드 서비스를 설명한 **컴플라이언스 체크리스트**.
3. **추가 정보**를 얻을 수 있는 출처에 관한 상세한 설명.

본 체크리스트는 누구를 대상으로 하는가?

본 체크리스트는 Microsoft 클라우드 서비스를 이용하기를 원하는 대한민국 내 금융회사들을 대상으로 삼고 있습니다. '금융회사'에는 금융위원회와 금융감독원의 규제를 받는 모든 기관을 포괄하며, 여기에는 은행, 일반 보험사, 생명보험사가 포함됩니다.

본 체크리스트는 어떤 Microsoft 클라우드 서비스에 적용되는가?

본 체크리스트는 Microsoft 의 Online Services Terms (**OST**)에 명시된 Microsoft Office 365, Microsoft Dynamics 365 Core Services, 그리고 Microsoft Azure Core Services 에 적용됩니다. 이러한 서비스에 관한 관련 정보는 Microsoft Trust Center 를 통해 언제라도 확인할 수 있습니다.

Office 365:	microsoft.com/en-us/trustcenter/cloudservices/office365
Dynamics 365:	microsoft.com/en-us/trustcenter/cloudservices/dynamics365
Azure:	microsoft.com/en-us/trustcenter/cloudservices/azure

본 체크리스트를 반드시 모두 작성해야 하는가?

그렇지 않습니다. 대한민국의 경우 Microsoft 클라우드 서비스를 도입하려는 금융회사가 체크리스트를 반드시 작성할 것을 요구하는 요건은 존재하지 않습니다. 다만, 다수의 대한민국 내 클라우드 고객과 상담을 진행해본 결과 이러한 체크리스트 방식을 적용할 경우 첫째, 규제 요건을 이해하는 수단으로, 둘째, Microsoft 클라우드 서비스가 금융회사의 규제 요건 준수에 어떻게 도움을 줄 수 있는지를 파악하는 수단으로, 셋째, 컴플라이언스를 문서화하는 내부 체제로, 넷째, 필요한 경우 금융감독기관과의 협의 절차를 효율화하는 도구로 유용하였습니다. 본 체크리스트를 검토하고 모두 준수하는 금융회사는 대한민국 내 규제 요건을 준수한다는 확신 하에 Microsoft 클라우드 서비스를 도입할 수 있습니다.

본 체크리스트를 어떻게 활용해야 하는가?

1. 다음 장에 수록된 '규제 환경에 관한 개요'를 검토하는 작업에서부터 시작할 것을 권합니다. 그러면 그에 후속하는 장들에 관한 맥락을 잘 파악할 수 있습니다.

2. 그 다음으로, 컴플라이언스 체크리스트에 수록된 문항과 관련 정보를 규제 준수 현황을 측정하는 도구로서 검토할 것을 권해 드립니다. 본 문건에 포함된 정보는 금융회사의 위험 평가를 지원할 목적으로 제공되는데, 이는 적절한 위험 평가를 수행하는 과정에서 반드시 이행해야 하는 작업을 대신하거나 대체할 목적이라기보다는 그러한 절차를 돕기 위해서 입니다. 그에 추가하여, Microsoft 의 서비스에 대한 지속적인 감독을 유지하는 동시에 금융회사의 위험 평가를 수행하는 업무의 일부로서 관련 정보를 획득할 수 있도록 Microsoft 가 제공하는 다양한 리소스들도

존재합니다. 그러한 정보는 Service Trust Portal 을 통해, 그 중에서도 특히 Compliance Manager 를 이용하여 확인할 수 있습니다.

Microsoft 는 Compliance Manager 를 통해 위험 평가의 성과에 관한 자체 감사와 실사를 지원하는 방대한 정보를 제공합니다. 여기에는 이행에 관한 세부 사항을 포함하여 보안 통제에 관한 다수의 세부 사항과 제 3 자 감사인이 각각의 통제를 어떻게 평가 했는지에 관한 설명이 포함됩니다. 보다 구체적으로, Compliance Manager 는 다음과 같은 역할을 수행합니다.

- Microsoft 클라우드 서비스에 대한 **위험 평가를 수행할 수 있도록 고객을 지원**합니다. 제 3 자가 다양한 기준(ISO 27001:2013, ISO 27018:2014 등)에 입각하여 Microsoft 의 클라우드 서비스에 대해 실시한 감사 절차의 일부로서 Microsoft 가 감사인과 감독기관에 제공한 세부적인 정보 그리고 Microsoft 가 규정(EU GDPR 혹은 기타 필수 통제에 대한 맵핑 등) 준수를 위해 내부적으로 취합한 정보를, 고객의 관련 기준 및 규정 준수 상황에 대한 자체 평가와 종합합니다.
- 고객의 책임지는 부분에 대한 규제 요건을 준수할 수 있도록 뒷받침하는 통제항목(컨트롤)과 역량을 개선할 목적으로 고객에게 세부적인 지도와 **권고사항을 제공합니다**.
- **컴플라이언스 업무절차(work flow)를 단순화**하는 동시에 고객이 부서간 장벽을 초월하여 컴플라이언스 목표를 달성할 수 있도록 지원할 수 있는 컴플라이언스 및 평가 관련 업무를 배정·추적·기록합니다. 또한, 컴플라이언스 활동과 관련된 증거와 그 밖의 아티팩트(artifact)를 업로드하고 관리하는 보안 저장소를 고객에게 제공하고, 그리하여 Microsoft 와 고객 내부 조직이 수행한 컴플라이언스 활동을 문서화한 아주 자세한 보고서를 엑셀로 작성하여 감사인, 감독기관, 기타 컴플라이언스 이해관계자에게 제공할 수 있도록 합니다.

3. 추가적인 지원이 필요하거나 의문 사항이 있는 경우에는 Microsoft 전문가들이, 최초 관계자가 참여하는 가장 초기 단계에서부터 금융 감독기관과의 필수적인 협의를 지원하는 업무에 이르기까지 클라우드 프로젝트 전반에 걸쳐 고객을 지원합니다. 또한, '추가 정보'에 제시된 것처럼 온라인상에서 보다 세부적인 정보를 확인할 수도 있습니다.

본 문서의 목적은 Microsoft 의 클라우드 서비스에 대해 리스크 평가를 포함하여 실사를 수행하는 고객을 위한 지침을 제공하는 것입니다. 적절한 실사를 수행할 책임은 고객에게 있으며, 본 문건은 그러한 실사나 고객의 위험 평가를 대체할 수는 없습니다. 본 문건이 Azure Core Services (이하 "**Azure**"), Office 365 Services (이하 "**Office 365**"), Dynamics 365 Services (이하 "**Dynamics 365**")에 주된 초점을 맞추고 있는 것은 사실이지만 이 원칙들은, 달리 언급된 경우를 제외하고 Microsoft 의 Online Services Terms (OST)에 포함된 Data Protection Terms (**DPT**)에 정의되고 참조된 모든 클라우드 서비스에도 동일하게 적용됩니다.

규제 환경에 관한 개요

클라우드 서비스가 허용되는가?	**그렇습니다.** 이는 귀 금융기관 전반에 걸쳐 Microsoft 클라우드 서비스의 적용을 고려할 수 있음을 의미합니다.
관련 감독기관과 당국은 어디인가?	관련 감독기관은 국무총리실 산하 금융위원회(FSC)(http://fsc.go.kr/)와 FSC 로부터 지시/감독을 받는 금융감독원(FSS)(http://fss.or.kr/)입니다.
어떤 규정과 지침이 적용되는가?	클라우드를 도입하려는 금융회사가 인지해야 할 법규와 지침은 다음과 같습니다. 1. 전자금융거래법 2. 전자금융감독규정(“**감독규정**”) 3. 금융회사의 정보처리 업무 위탁에 관한 규정(“**정보처리위탁규정**”)[1] 4. 금융기관의 업무 위탁 등에 관한 규정(“**업무위탁규정**”) 5. 금융분야 클라우드 컴퓨팅 서비스 이용 가이드라인(“**클라우드 가이드**”)(2019)[2] (http://www.fsec.or.kr/user/bbs/fsec/147/315/bbsDataView/1155.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory) ‘클라우드 가이드’는 법적 구속력이 없으며 금융보안원에서 제시한 권고 사항에 불과하다는 점을 유의하시기 바랍니다.
감독 당국의 승인이 요구되는가?	**그렇지 않습니다.** 다만, 다음의 경우에는 금융회사가 클라우드 컴퓨팅 서비스 이용 예정일로부터 최소한 7 영업일 전에 금융감독원에 **보고**해야 합니다. 1. 고유식별정보 또는 개인신용정보를 처리하는 경우. 2. 사안이 전자금융거래의 보안성과 신뢰성에 중대한 영향을 미칠 것으로 예상되는 경우.

[1] 금융투자업자의 경우 ‘자본시장과 금융투자업에 관한 법률(**자본시장법**)’의 위탁 관련 조항이 업무위탁규정과 정보처리위탁규정(정보처리위탁규정 제 3 조 제 1 항)에 우선합니다. 금융투자업에 종사하지 않는 금융회사의 경우 정보 처리 업무의 위탁과 관련하여 정보처리위탁규정이 업무위탁규정에 우선합니다.

[2] 클라우드 가이드는 금융보안원에서 제작하여 배포했으며 클라우드 컴퓨팅 서비스를 이용하는 금융회사 등이 준수해야 할 사항들을 권고함으로써 금융 이용자를 보호하고 금융 시스템의 안전을 유지·강화하는 것이 그 목적입니다. 클라우드 가이드에는 클라우드 서비스의 도입, 클라우드 서비스의 이용, 클라우드 서비스의 관리 및 사후 관리에 관한 사항들이 수록되어 있습니다.

국외로 정보를 이전하는 것이 허용되는가?	**고유식별정보와 개인신용정보를 제외하고 허용됩니다.** 비중요 정보처리 시스템의 경우 국외 데이터센터를 이용하는 것이 허용됩니다. 고유식별정보와 개인신용정보는 반드시 대한민국 내에 저장되어야(localize) 합니다. 단, 전자금융거래의 안전성과 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내 지점과 국외 사이버 몰을 위한 전자지급결제대행업자는 국외에서도 고유식별정보와 개인신용정보를 처리할 수 있습니다. (금융회사뿐만 아니라 전 산업 분야에 적용되는)일반적인 개인정보보호 관련 법률은 다음과 같은 경우에 위탁의 맥락에서 개인정보의 국외 이전을 허용하고 있습니다. 1. 개인정보 보호법이 적용되는 경우: (i) 서면에 의한 위탁 계약과 (ii) 위탁 계약의 통지/공시로 구성되는 일반적인 위탁 원칙(국외/국내 위탁 간의 차이가 존재하지 않음)이 적용됩니다. 2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률(“**정보통신망법**”)이 적용되는 경우: 원칙적으로 정보 주체의 동의가 요구됩니다. 단, 계약상의 의무를 이행하고 이용자의 편의 증진을 위해 위탁업체의 이용이 필수적이고, 위탁과 국외 이전에 관한 사항을 개인정보처리방침에 공개하거나 기타 방식으로 이용자에게 고지한 경우에는 동의요건이 면제됩니다. 그에 추가하여, 개인정보를 보호하는 기술적·관리적 조치와 고충 처리 조치 등을 포함하여 개인정보 보호에 필요한 조치를 이행할 것을 요구 받습니다. 고유식별정보와 개인신용정보를 제외한 정보를 국외로 이전할 수 있음에도 불구하고 당사의 대한민국 금융서비스 고객 중 상당수는 Azure 와 Office 365 를 포함하여 마이크로소프트 대한민국 데이터센터에서 제공하는 클라우드 서비스를 이용하고 있습니다.
퍼블릭 클라우드 서비스의 안전성은 충분한가?	**그렇습니다.** 퍼블릭 클라우드(Public Cloud) 서비스를 이용하는 국내 금융회사가 갈수록 늘고 있습니다. 실제로, 퍼블릭 클라우드 서비스는 일반적으로 가장 먼저 혁신이 이뤄질 뿐만 아니라 매우 방대한 위협 인텔리전스 데이터를 확보하고 있다는 점에서 통상적으로 고객이 최첨단 보안 기능과 혁신을 활용할 수 있도록 합니다. Microsoft 클라우드 서비스에서 이러한 유형의 혁신 사례로 Office 365 Advanced Threat Protection 과 Azure Web Application Firewall 을 들 수 있는데, 해당 서비스는 기존에 알려지지 않은 멀웨어(malware)를 탐지하여 무력화하는 고도로 정교한 모델을 제공하는 동시에 고객에게 정보 보호 및 분석정보를 제공합니다.

서비스 제공자와의 계약에 반드시 포함시켜야 하는 의무적인 조항이 존재하는가?	**그렇습니다.** 감독규정과 정보처리위탁규정에는 금융회사가 클라우드 서비스 계약에 반드시 포함시켜야 하는 일부 구체적인 사항들이 명시되어 있습니다. 후술하는 제 2 부 컴플라이언스 체크리스트에서는 이러한 사항들을 Microsoft 계약 문서에 대응하여 설명하고 있습니다.
일반적인 개인정보보호 법률은 금융회사의 클라우드 서비스 이용에 어떻게 적용되는가?	금융회사에 적용 가능한 개인정보보호 법률에는 클라우드 서비스 제공자(Microsoft, 수탁자)에게 위탁하는 정보의 유형에 따라 금융회사가 반드시 준수해야 할 신용정보법, 개인정보보호법, 정보통신망법이 포함됩니다. 클라우드 서비스 제공자는 개인정보 처리서비스를 제공하는 수탁자로서 개인정보의 처리와 관련하여 신용정보법(개인신용정보의 경우), 개인정보보호법, 정보통신망법에 따른 여러 요건을 준수해야 합니다. 개인정보보호 감독기관에는 금융위원회, 금융감독원, 행정안전부, 방송통신위원회, 개인정보보호위원회가 있습니다. 그에 추가하여, 2018 년 5 월 25 일을 기해 유럽의 개인정보보호법인 **GDPR(the General Data Protection Regulation)**이 시행되었습니다. 특기할 사실로 GDPR 은 EU 내의 주민에게 재화와 용역을 제공하는 경우 뿐만 아니라 EU 역내에서 일어나는 개인의 행동을 모니터링하는 기업, 정부 부처, 비영리단체, 기타 조직에까지 적용됩니다. 이러한 이유에서, GDPR 은 EU 역내에서 설립된 조직체에 국한되지 않고 법역을 초월하여 적용됩니다. Microsoft 는 클라우드 서비스 전반에 걸쳐 GDPR 컴플라이언스를 추구하고 있으며 계약상의 약정을 통해 GDPR 관련 약속을 하고 있습니다. Microsoft 제품이 GDPR 준수에 어떻게 도움을 줄 수 있는지는 여기에서 자세히 확인할 수 있습니다.

컴플라이언스 체크리스트

본 컴플라이언스 체크리스트는 어떤 방식으로 기능하는가?

'**문항/요건**' 란에는 이행할 필요가 있는 요건이 제시됩니다.

'**지침**' 란에는 Microsoft 클라우드 서비스를 이용하여 관련 요건에 대응할 수 있는 방법이 설명됩니다. 필요한 경우에는 기본 요건의 출처와 그 외에도 고려할 필요가 있는 다른 사항들에 관한 *지침*이 함께 제시됩니다.

컴플라이언스 체크리스트를 어떻게 활용해야 하는가?

각각의 금융회사와 클라우드 서비스는 저마다 차이가 있습니다. Microsoft 는 제공된 지침을 적절히 수정하여 귀 금융회사 및 클라우드 서비스 사정에 따라 스스로의 대응논리를 발전시킬 것을 권해 드립니다.

어떤 부분에 주목해야 하는가?

본 컴플라이언스 체크리스트는 다음과 같은 두 부분으로 구성되어 있습니다.

- **제 1 부**에서는 주요 컴플라이언스 고려 사항을 다룹니다.
- **제 2 부**에서는 반드시 다루어야 하는 계약상의 조항을 열거하고 해당 조항이 Microsoft 계약 문서에서 어디에 위치하는지를 표시합니다.

제 1 부: 주요 고려 사항

본 제 1 부는 누구에게 적용되는가?

본 제 1 부는 대한민국 내 금융회사가 구축하는 모든 Microsoft 클라우드 서비스(그 중에서도 특히 Office 365, Dynamics 365, Azure)에 적용됩니다.

번호	문항/요건	지침
A. 개요 ***본 장에는 Microsoft 클라우드 서비스에 관한 전반적인 개요가 제시되어 있습니다.***		
1.	서비스 제공자는 누구인가?	서비스 제공자는 대한민국마이크로소프트(유)입니다. 대한민국마이크로소프트(유)는 미국에서 상장(NASDAQ: MSFT)되고 전 세계에 정보기술 디바이스와 서비스를 제공하는 기업인 Microsoft Corporation 의 완전 자회사인 동시에 지역 라이선스 법인입니다. Microsoft 의 모든 기업정보는 다음에서 확인할 수 있습니다: microsoft.com/en-us/investor/ Microsoft 의 사업보고서는 다음에서 확인할 수 있습니다: microsoft.com/en-us/Investor/annual-reports.aspx
2.	귀사에서 이용하는 클라우드 서비스는?	Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365 Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365 Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure
3.	서비스 제공자에 위탁할 활동과 업무는 무엇인가?	본 컴플라이언스 체크리스트는 Office 365, Dynamics 365 및/또는 Azure 를 이용하는 금융회사를 대상으로 만들어졌습니다. 각각의 서비스는 저마다 차이가 있으며 동일한 서비스 내에서도 다양한 옵션과 설정이 존재합니다. 이하의 답변은 귀사가 Microsoft

번호	문항/요건	지침
		클라우드 서비스를 어떻게 이용할 계획인지에 따라 적절한 조정이 필요할 것입니다. 필요한 경우 귀사를 담당하는 Microsoft 담당자로부터 조력을 받을 수 있습니다. Office 365 를 이용하는 경우 통상적으로 이하의 항목들이 포함됩니다. • Microsoft Office applications (Outlook, Word, Excel, PowerPoint, OneNote, Access) • Exchange Online • OneDrive for Business, SharePoint Online, Microsoft Teams, Yammer Enterprise • Skype for Business Dynamics 365 를 이용하는 경우 통상적으로 이하의 항목들이 포함됩니다. • Microsoft Dynamics 365 for Customer Service, Microsoft Dynamics 365 for Field Service, Microsoft Dynamics 365 for Project Service Automation, Microsoft Dynamics 365 for Sales, Microsoft Social Engagement • Microsoft Dynamics 365 for Finance and Operations (Enterprise and Business Editions), Microsoft Dynamics 365 for Retail, Microsoft Dynamics 365 for Talent Microsoft Azure 를 이용하는 경우 통상적으로 이하의 항목들이 포함됩니다. • Virtual Machines, App Service, Cloud Services • Virtual Network, Azure DNS, VPN Gateway • File Storage, Disk Storage, Site Recovery • SQL Database, Machine Learning • IoT Hub, IoT Edge • Data Catalog, Data Factory, API Management • Security Center, Key Vault, Multi-Factor Authentication

번호	문항/요건	지침
		• Azure Blockchain Service
4.	어떤 유형의 클라우드 서비스를 이용할 계획인가?	*이용할 클라우드 서비스의 유형에 따른 성격은 위험 프로파일의 차이를 초래합니다. 또한, 클라우드 솔루션의 유형에 대한 이해는 솔루션과 연관된 위험을 파악하는 과정과 관련이 있을 수 있습니다. Microsoft 클라우드 서비스의 경우 퍼블릭 및 하이브리드 클라우드를 포함하여 폭 넓은 옵션이 보장됩니다. 다만, 고객에게 돌아가는 운영상의 이점과 상업적인 이점을 감안할 때, 대부분의 기관들 사이에서 퍼블릭 클라우드가 표준적인 모델로 점차 대두되고 있습니다.* 퍼블릭 클라우드를 이용하는 경우: 대부분의 비즈니스용 Microsoft 클라우드 서비스가 만들어지는 Microsoft Azure 는 데이터의 논리적 분리(logical data isolation)를 통해 고도의 안전성을 보장하는 방식으로 여러 테넌트들을 호스팅합니다. 테넌트의 데이터 저장과 처리는 후술하는 D 장(기술적·운영적 위험 Q&A)에서 설명하는 것처럼 다른 테넌트들로부터 분리됩니다. 하이브리드 클라우드를 이용하는 경우: 고객은 Microsoft 하이브리드 클라우드를 통해 고객 스스로 결정한 시간 계획에 따라 멀티 테넌트 클라우드로 이동할 수 있습니다. 테넌트는 Windows Server 가상 머신을 이용하여 자체 서버에 저장할 데이터의 카테고리를 식별하기를 원할 수 있습니다. 그 외의 다른 모든 카테고리의 데이터는 멀티 테넌트 클라우드에 저장됩니다. 대부분의 비즈니스용 Microsoft 클라우드 서비스가 만들어지는 Microsoft Azure 는 데이터의 논리적 분리를 통해 고도의 안전성을 보장하는 방식으로 여러 테넌트를 호스팅합니다. 테넌트의 데이터 스토리지와 프로세싱은 후술하는 D 장(기술적·운영적 위험 Q&A)에서 설명하는 것처럼 다른 테넌트들로부터 분리됩니다.
5.	금융회사를 대신하여 서비스 제공자에 의해 어떤 데이터가 처리되는가?	*고유식별정보 또는 개인신용정보를 처리하는 경우에는 금융감독원사전 보고와 데이터 국내 보관(localization) 등의 추가적인 요건이 수반됩니다. 그러므로 Microsoft 클라우드 서비스를 통해 어떤 데이터를 처리할 것인지를 이해하는 것이 중요합니다. Microsoft 클라우드 서비스 내에서 어떤 데이터를 저장하거나 처리할 계획인지에 따라 본 장의 내용을 조정하시기 바랍니다.*

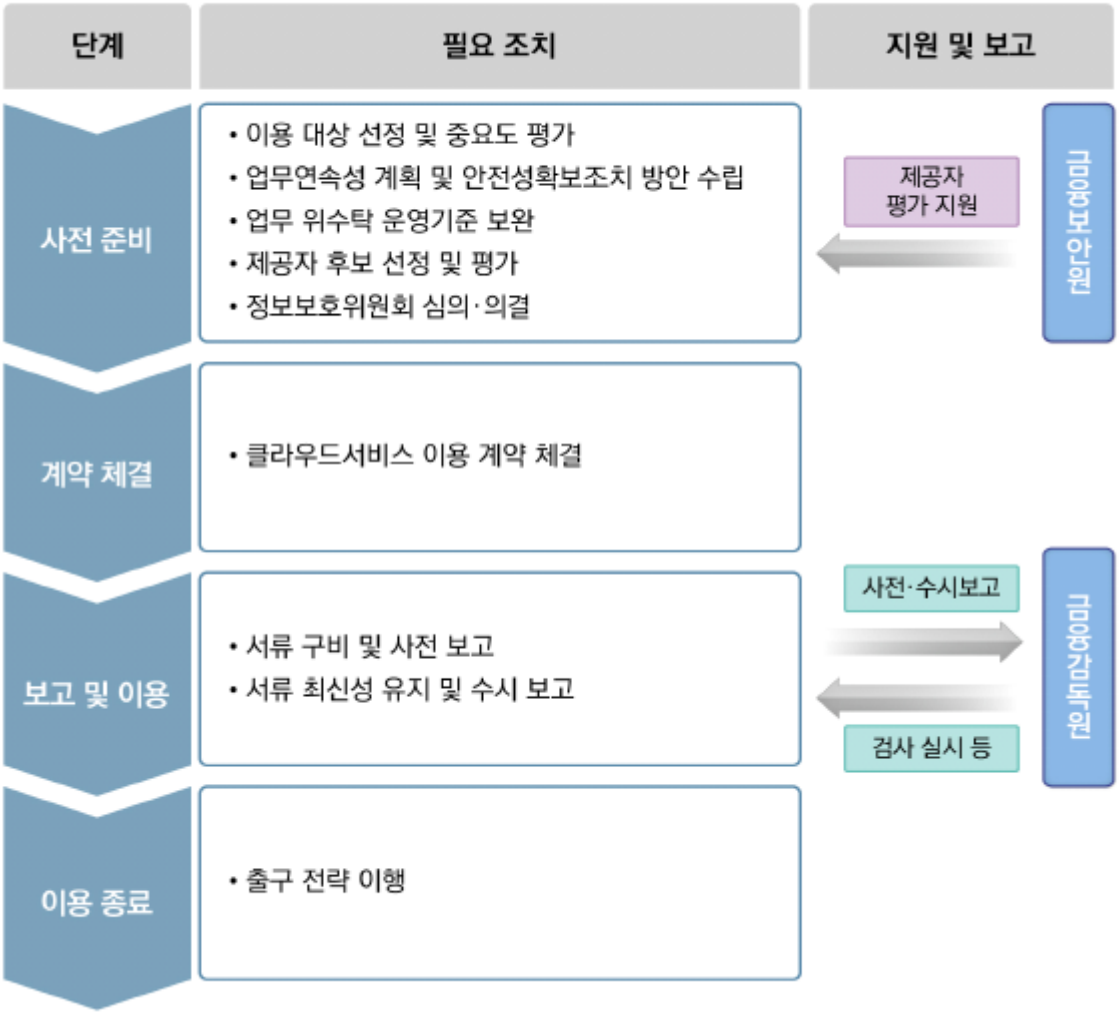
번호	문항/요건	지침
		Microsoft 고객들이 Microsoft 클라우드 서비스 내에서 통상적으로 저장하거나 처리하기를 원하는 데이터 카테고리는 이하와 같습니다. • 고객 데이터(고객 성명, 연락처 정보, 계정 정보, 결제 카드 데이터, 보안 자격 증명, 통신 포함) • 직원 데이터(직원 성명, 연락처 정보, 이메일과 기타 수단을 이용한 사내·외 통신, 고용에 관련된 개인정보 포함) • 거래 데이터(조직이 관여한 거래에 관한 데이터) • 인덱스(예: 시장 데이터) • 금융회사로서의 사업 운영에 관한 기타 개인 및 비개인 데이터 모든 데이터는 Microsoft 와 체결한 계약의 조건에 의거, 귀사가 법적 의무 및 고객과의 약속을 지속적으로 준수할 수 있도록 최고 수준의 보안을 적용하여 취급됩니다. 귀사는 제반 관련 법률과 규정에 따라 사업을 운영하는 데 필요한 데이터만을 수집하고 처리할 것이며 이 원칙은 데이터를 자체 시스템상에서 처리하든 클라우드 솔루션상에서 처리하든 상관없이 마찬가지로 적용됩니다.
6.	어떤 서비스 제공자를 선정하는 경우에 거래상대방으로 인해 발생하는 위험을 해결할 수 있는가?	*감독규정 제 14 조의 2 제 1 항 제 2 호는 금융회사가 클라우드 서비스 제공자의 건전성과 안전성을 평가할 것을 요구하고 있습니다. Microsoft 클라우드 서비스의 건전성과 관련하여, 우리의 고객들이 일반적으로 중요하다고 언급하는 요인들을 요약하면 아래와 같습니다. Microsoft 에 관한 추가적인 정보는 Trust Center 에서 확인할 수 있습니다.* **a. 역량.** Microsoft 는 클라우드 컴퓨팅 산업을 선도하는 기업입니다. Microsoft 클라우드 서비스는 물리적·논리적·프로세스·관리통제에 관한 엄격한 글로벌 기준인 ISO/IEC 27001 및 ISO/IEC 27018 표준에 근거하여 만들어졌습니다. Microsoft 는 다른 어떤 클라우드 서비스 제공자보다 포괄적인 컴플라이언스 서비스를 제공합니다. 현재까지의 인증 현황 리스트는 microsoft.com/ko-kr/trustcenter/compliance/complianceofferings 에서 확인할 수 있습니다. 위험보장의 관점에서, Microsoft 의 기술적·조직적 조치들은 전 세계 금융회사의 요구를 충족시킬 목적으로 수립되었습니다. 또한, Microsoft 는 https://www.microsoft.com/ko-kr/Licensing/product-licensing/products.aspx 에서 확인이 가능한 Online Services Terms 를 통해 클라우드 서비스 전반에 걸쳐 구체적인 약정을 제시합니다. **b. 실적.** 세계적인 기업들 중 상당수가 Microsoft 클라우드 서비스를 이용합니다. customers.microsoft.com 에는 Microsoft 클라우드 서비스 이용에 관련된 다수의 사례연구들이 게재되어 있습니다. 고객들은 (필요한 경우) 규제기관의 승인을 획득했으며 현재 세계 각지에서 클라우드 서비스를 이용하고 있습니다. Office 365 는 세계적인 기업과 금융회사를 포함하여

번호	문항/요건	지침
		1 억 명 이상의 이용자를 거느린 서비스로 성장했고, Azure 는 90% 이상의 성장세를 지속하고 있으며 대규모 금융회사들 가운데 80% 이상이 Azure 서비스를 이미 이용하고 있거나 향후 이용할 것을 약정했습니다. c. **구체적인 금융서비스 경험.** 영국, 프랑스, 독일, 싱가포르, 캐나다, 미국 등 선진 금융시장의 금융회사 고객들이 자체 실사를 수행한 바 있으며, 자국 감독기관과의 협조 하에 Microsoft 클라우드 서비스가 규제 요건에 부합한다는 만족스러운 결론에 도달했습니다. 이를 통해 고객들은 Microsoft 가 엄격한 금융서비스 규정을 준수하는 데 도움을 줄 수 있으며 관련 요건을 이행하는 분야에서 풍부한 경험을 축적하고 있다는 사실을 확신하고 있습니다. d. **Microsoft 의 재무 건전성.** Microsoft Corporation 은 미국의 상장기업이며 시가총액을 기준으로 세계 최대 규모를 자랑합니다. Microsoft 는 안정적인 수익을 기록해온 건실한 실적을 보유하고 있습니다. 시가총액이 1 조 달러(2019 년 12 월 현재)를 웃도는 Microsoft 는 시가총액을 기준으로 세계 3 대 기업에 속하며, 2000 년 이래 세계 10 대 기업 명단에 계속해서 이름을 올리고 있습니다. 실제로, Microsoft 는 지난 20 년간 세계 10 대 기업으로서 꾸준히 자리를 지킨 유일한 기업입니다. Microsoft 의 기업 정보는 microsoft.com/en-us/investor/에서 확인할 수 있고 회사 사업보고서는 microsoft.com/en-us/Investor/annual-reports.aspx 에서 볼 수 있습니다. 따라서 고객은 Microsoft 의 재무 건전성에 대해서는 전혀 걱정할 필요가 없습니다.
B. 해외 위탁 ***Microsoft 는 고객이 특정한 데이터를 대한민국 내에 저장할 수 있는 기회를 제공합니다. 이는 귀사가 선택하는 Microsoft 클라우드 서비스 설정에 달려 있는데, 귀사는 귀사의 상황에 맞춰 대응할 필요가 있습니다.***		
7.	제안된 위탁 서비스에 데이터 국내 보관(localization)이 요구되는가?	*감독규정은 클라우드를 이용하여 고유식별정보와 개인신용정보를 처리하는 모든 시스템이 대한민국 내에 존재할 것을 요구하고 있습니다. Microsoft 는 데이터 위치 투명성을 보장하며 고객이 대한민국 내에 데이터를 저장할 수 있는 선택권을 부여합니다.* 첫째, 가장 중요한 요소로서 고객은 Core online Services 데이터가 대한민국 내에 저장되도록 서비스를 설정할 수 있습니다. *Office 365 및/또는 Dynamics 365 를 이용하는 경우:* 고객은 Core Online Services 데이터가 대한민국 내에 저장되도록 선택할 수 있습니다. 세부적인 사항은 http://aka.ms/dcmap (Office365) 및 o365datacentermap.azurewebsites.net (Dynamics 365)의 인터액티브 데이터센터 맵을 참조하시기 바랍니다. *Azure 를 이용하는 경우:*

번호	문항/요건	지침
		고객은 데이터가 대한민국 내에 저장되도록 서비스를 설정할 수 있습니다. 세부적인 사항은 azure.microsoft.com/ko-kr/regions 의 인터액티브 데이터센터 맵을 참조하시기 바랍니다.
8.	클라우드 서비스 제공자와의 계약을 통해 어떻게 해외위탁으로 인한 위험을 관리할 수 있는가?	국외에서 저장되거나 처리되는 일부 제한적인 데이터 카테고리와 관련하여, 고객은 이하와 같은 이유에서 해외 위탁 위험이 관리된다는 사실에 만족할 수 있습니다. i. 고객은 데이터가 어디에 저장되는지 알 수 있습니다. 국외에서 저장되거나 처리되는 일부 제한적인 데이터 카테고리의 경우 관련위치를 http://aka.ms/dcmap (Office365), o365datacentermap.azurewebsites.net *(Dynamics 365)* 그리고 azure.microsoft.com/ko-kr/regions *(Azure)*에서 각각 확인할 수 있습니다. ii. 관련 데이터 센터들은 다양한 국가 및 사회경제적 요인들을 고려하여 전략적으로 배치되어 있습니다. Microsoft 의 데이터 센터들은 법률 제도, 규제 체제, 기술력, 인프라를 기반으로 안정적이고 안전하며 신뢰할 수 있는 것으로 인정되는 국가에 위치합니다. 해당 국가의 정부 당국이 정보에 대한 접근권을 행사할 수 있는 상황은 부적절한 요인으로 간주되지 않습니다. iii. 국외에 위치한 Microsoft 데이터 센터를 이용한다는 사실은 고객이 Microsoft 를 상대로 계약을 집행할 수 있는 능력에 영향을 미치지 않습니다. Microsoft 는 상당한 인적 및 물적 자원(resources)을 보유한 국제적인 기업입니다. Microsoft 는 (대한민국을 포함하여) 다수의 국가에 진출해 있으며 금융서비스 분야에서 오랜 실적을 보유합니다. iv. 국외에 위치한 Microsoft 데이터 센터를 이용한다는 사실이 금융 감독기관의 규제 감독 및 접근에 영향을 미치지 않습니다. 금융 감독기관이 클라우드 서비스에 관련된 Microsoft 의 시설, 시스템, 프로세스, 데이터를 조사할 수 있도록 보장하는 계약 조항들이 있습니다. v. 국외에 위치한 Microsoft 데이터 센터를 이용한다는 사실이 고객이 데이터에 접근할 수 있는 능력에 영향을 미치지 않습니다. 고객이 Microsoft 클라우드 서비스에 데이터를 저장하면 해당 데이터에 대한 소유권을 보유합니다. 고객은 Microsoft 의 협조 없이 어떤 사유를 불문하고 언제라도 해당 데이터의 사본을 다운로드할 수 있습니다.
9.	데이터 해외 위탁과 관련하여 어떤 위험을 고려했는가?	*고유식별정보와 개인신용정보를 처리하지 않는 한, 데이터의 해외위탁이 허용됩니다. 우리의 고객들이 데이터 해외위탁과 관련하여 일반적으로 중요하다고 강조하는 위험 분야들은 이하와 같습니다.* **a. 정치(국제적 분쟁, 정치적 불안 등)** 고객들은 데이터가 어디에 호스팅 되는지를 알고 있고, 해당 국가들은 정치적으로 안정된 환경을 보장합니다. **b. 국가/사회경제**

번호	문항/요건	지침
		Microsoft 의 데이터 센터들은 다양한 국가 및 사회경제적 요인들을 고려하여 전략적으로 배치되어 있습니다. 해당 위치는 사회경제적으로 안정된 환경을 제공합니다. **c. 인프라/보안/테러** 세계 각지의 Microsoft 데이터 센터들은 위험과 무단 접근으로부터 고객 데이터를 보호할 목적으로 수립된 완전히 동일한 기준으로 보안이 유지됩니다. 이에 관한 사항은 microsoft.com/en-us/trustcenter/security 에 보다 상세하게 기술되어 있습니다. **d. 환경(지진, 태풍, 홍수)** Microsoft 데이터 센터는 지진 안전지대에 건설됩니다. 온도 조절, 난방, 통기 및 공조, 화재 감지 및 방재 시스템과 전력 관리 시스템, 물리적 하드웨어에 대한 24 시간 모니터링, 지진 대비 랙 등 데이터 센터를 보호하는 환경 통제 조치가 시행됩니다. 이러한 요건에는 Microsoft 의 ISO/IEC 27001 인증이 적용됩니다. **e. 법률** 고객은 위탁 서비스와 관련하여 Microsoft 를 상대로 구속력을 갖춘 계약상의 합의에 도달함으로써 직접적인 계약상의 권리를 부여받고 감독기관의 규제 감독을 유지합니다. 그 계약조건들은 제 2 부에 요약되어 있습니다.
C. 클라우드 서비스 이용 절차		

〈클라우드서비스 이용 절차도〉



번호	문항/요건	지침
		감독규정 제14 조의2 (클라우드 컴퓨팅 서비스 이용절차 등)는 금융회사가 클라우드를 이용하고자 하는 경우 필수적인 절차를 수행할 것을 요구하고 있으며 클라우드 가이드에는 상기 절차가 제시되어 있습니다. ***또한, 금융회사는 (i) 클라우드를 이용하여 고유식별정보나 개인신용정보를 처리하거나 (ii) 클라우드 이용으로 인해 전자금융거래의 안전성과 신뢰성에 중대한 영향을 미치는 경우, 금융감독원에 클라우드 이용을 보고해야 합니다. 금융감독원 보고 시 아래 서류가 요구됩니다.*** ***- 정보처리위탁규정 제7 조 제1 항 각 호에 규정된 서류*** ***- 이용대상 정보처리시스템의 중요도 평가에 대한 자체 중요도 평가 기준 및 결과*** ***- 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항*** ***- 클라우드 서비스 이용과 연관된 정보보호위원회의 심의 및 의결 결과*** ***이러한 절차는 개별 금융회사가 처리해야 할 사안이지만 Microsoft 는 과거에 다른 고객들이 채택한 접근방식을 지원했던 경험을 바탕으로 지원을 제공합니다. 이 절차는 최종적으로 귀사의 컴플라이언스 업무를 반영하여 귀사에 맞춰 조정될 필요가 있습니다.***
10.	클라우드 서비스를 이용할 업무를 선정하고 그 중요도를 평가한다.	*금융회사가 (i) 클라우드를 이용하여 고유식별정보나 개인신용정보를 처리하거나 (ii) 클라우드 이용으로 인해 전자금융거래의 안전성과 신뢰성에 중대한 영향을 미치는 경우에는 금융감독원에 클라우드 이용을 보고해야 합니다.* Microsoft 는 Asset Inventory 와 Asset Handling 방식 그리고 OST 에 명시된 기타 보안 약정을 포함하여 Core Online Services 에 포함되는 고객 데이터에 대한 구체적인 보안 조치를 이행해왔으며 그러한 보안 조치를 유지하기 위해 최선을 다하고 있습니다. 그에 추가하여, Microsoft 는 금융회사가 디바이스, 앱, 클라우드 서비스, 온프레미스 전반에 걸쳐 민감한 데이터를 발견·분류·보호·모니터링할 수 있도록 돕기 위해 데이터 분류 및 보호 기술을 활용하는 클라우드 서비스를 제공하고 있습니다. Azure Information Protection, Office 365 Information Protection, Windows Information Protection, Microsoft Cloud App Security 등을 포함하는 Microsoft Information Protection 솔루션의 예시는 여기에서 확인할 수 있습니다.

번호	문항/요건	지침
		Office 365 / Microsoft 365 역시 금융회사가 엄격한 수준의 보장 및 컴플라이언스 요건을 준수할 수 있도록 지원하는 한층 진보된 기능을 제공하고 있습니다. 그 예는 다음과 같습니다. • 첨단 전자적 디스커버리 • 데이터 거버넌스 및 보존 • BYOK (bring-your-own key) 암호화 • Microsoft 지원 엔지니어에 의한 데이터 접근 방식 통제 • 접근 권한 관리 Azure SQL 의 경우, 데이터 마스킹 및 암호화와 함께, 데이터 디스커버리 및 분류를 지원하는 데이터 보안 기능이 존재합니다.
11.	안전성을 보장하는 업무 연속성 계획 및 조치	*이 요건은 Microsoft 와 같은 제 3 자 서비스 제공자에게 업무를 위탁하는지 여부와 상관없이 적용됩니다. 귀사를 담당하는 Microsoft 고객 담당자가 Microsoft 의 재난 복구 계획에 관한 질의 그리고 귀사의 재난 복구 계획과의 상호 작용에 관한 조언을 제공할 수 있습니다.* Microsoft 는 장애를 일으킨 인프라 컴포넌트로부터의 워크로드(workload) 이전이 서비스에 미치는 영향을 체감할 수 없을 정도로 가능하게끔 디스크, NIC, 전력 공급원, 서버 수준에서의 물리적 이중화와 상시적인 콘텐츠 복제, 강력한 백업·복원·대체작동 기능, 실시간 이슈 탐지 및 자동화된 대응을 실시하는 등의 방식으로 서비스 중단을 최소화하기 위해 최선의 노력을 다하고 있습니다. 또한, Microsoft 는 긴급 엔지니어링 지원팀을 1 년 365 일 24 시간 운영하고 있습니다. Financial Services Compliance Program 과 Premier Support 를 참고할 수 있고 또한, Office 365 Support, Premier Support for Enterprise, Azure Support Plans 도 참고가 가능합니다.

번호	문항/요건	지침
		• *이중화*. Microsoft 는 서버, 데이터센터, 서비스 수준에서의 물리적 이중화, 강력한 대체작동(failover) 능력이 적용된 데이터 이중화 그리고 오프라인 기능성이 부여된 기능적 이중화를 유지합니다. 이중화가 적용된 Microsoft 의 스토리지와 데이터 복원 절차는 고객 데이터를 손실 또는 파괴 이전의 원 상태 혹은 직전 복제 상태로 복구할 목적으로 수립되었습니다. ○ Office 365 의 경우, Microsoft 는 이중화를 위해 다수의 데이터센터에 복수의 고객 데이터 사본을 저장합니다. ○ Azure 의 경우, Microsoft 는 데이터 이중화 혹은 기타 운영상의 목적으로 특정한 권역 내에 있는 다수의 리전(region)들 간에 고객 데이터를 복제할 수 있습니다. 일례로, Azure GRS 는 중대한 데이터센터 재난에 대비하여 데이터 지속성을 강화할 목적으로 동일한 권역 내에서 2 개 리전 간에 특정한 데이터를 복제합니다. • *복원력*. Microsoft 의 클라우드 서비스는 데이터 복원력(resiliency)을 확대할 목적으로 액티브 로드 밸런싱(load balancing), 자동화된 대체작동 및 인적 백업, 오류 도메인 전반에 걸친 복구 테스팅을 제공합니다. 일례로, Azure Traffic Manager 는 서로 다른 리전들 간의 로드 밸런싱을 제공하며 고객은 Azure Virtual Networks 내에서 애플리케이션 딜리버리 컨트롤러(ADC/로드 밸런싱) 기능을 위해 네트워크 가상 어플라이언스를 이용할 수 있습니다. 로드 밸런싱은 Power BI Services, Gateway, Azure API Management 기능을 통해서도 제공됩니다. • *분산형 서비스*. 또한, Microsoft 는 어느 한 컴포넌트의 오류로 인한 영향과 범위를 제한할 목적으로 Exchange Online 이나 SharePoint Online 같은 분산형 컴포넌트 서비스를 제공합니다. 오류가 발생할 경우 서비스와 서비스를 단절시킬 목적으로 컴포넌트 서비스 전반에 걸쳐 디렉토리 데이터 역시 복제됩니다. • *모니터링*. Microsoft 의 클라우드 서비스에는 자동 복구를 구동하는 내부 모니터링, 사고를 경고하는 아웃사이드-인 모니터링, 로깅·감사·개별추적(granular tracing)에 대한 방대한 진단 기능이 포함됩니다.

번호	문항/요건	지침
		• *단순화*. Microsoft 는 이슈 분리 복잡성(issue isolation complexities)을 낮출 목적으로 표준화된 하드웨어를 이용하고 또한, 완전 자동화된 구축 모델(deployment model)과 표준 탑재(built-in) 관리 메커니즘을 적용합니다. • *인적 백업*. Microsoft 의 클라우드 서비스에는 1 년 365 일 24 시간 긴급 지원을 제공하는 자동화된 복구 서비스, 신속한 대응과 해결을 보장하는 다양한 역량을 갖춘 긴급 지원팀, 그리고 긴급 지원팀이 습득한 지식에 기반한 지속적인 개선이 포함됩니다. • *지속적 학습*. 사고가 발생한 경우 Microsoft 는 철저한 사후 검토를 실시합니다. 이러한 사후 검토는 발생 사건에 대한 분석, Microsoft 의 대응 및 추후에 유사한 문제의 재발을 방지하기 위한 Microsoft 의 계획으로 구성됩니다. Microsoft 는 서비스 사고로 인한 피해를 입은 고객과 사후 검토 결과를 공유할 것입니다. • *재난 복구 테스트*. Microsoft 는 1 년에 1 회 이상 재난 복구 테스트를 실시합니다.
12.	업무위수탁 운영기준의 보완	*감독규정 별표 2-3 에는 (i) 위탁 및 재위탁 계약의 결정 및 해지 절차에 관한 사항, (ii) 위탁 감독에 관한 사항, (iii) 비상 대응 계획에 관한 사항, (iv) 위탁 서비스와 관련된 조사 및 접근 권한에 관한 사항, (v) 위수탁 계약에 포함될 사항으로 구성된 업무위수탁 운영기준 보충사항이 열거되어 있습니다.* 적합한 기준은 조직의 유형 및 대상이 되는 클라우드 서비스에 의해 결정되며 조직의 위험 프로파일과 클라우드 서비스를 이용하는 구체적인 업무·데이터·목적이 고려되는데, 일반적으로 이하의 요소들이 포함됩니다. • 조직이 예금자나 보험가입자 혹은 기타 이해관계자에 대한 금융 및 서비스 상의 의무를 확실하게 이행하기 위해 위탁에 관련된 위험을 파악·평가·관리·경감·보고하는 체계. • 위탁에 수반되는 위험의 성격과 중대성에 기반한 적절한 위탁 승인 권한(방침 자체는 이사회의 승인을 요함). • 건전하고 대응적인 위탁 위험 관리 방침과 절차를 수립하기 위한 관리 역량에 대한 평가. • 위탁 전략 및 체계의 지속적인 관련성, 안전성, 건전성에 관한 정기적인 검토.

번호	문항/요건	지침
		• 현실적이고 개연성이 있는 파괴적(disruptive) 시나리오에 기초한 비상대응계획의 수립 및 테스트 보장. • 방침의 준수에 관한 외부 검토 및 감사 보장. 예를 들어, 귀사는 서비스 제공자 선정 절차에서 Microsoft 의 평판 및 실적과 관련하여 위에 열거된 요소들에 대한 자체적인 기준 분석을 포함시킬 수 있습니다. 그에 추가하여, 귀사는 Microsoft 인증 요건의 일환으로, Microsoft 가 정기적, 독립적 제 3 자 감사를 받을 것을 요구하는 방침을 포함하는 방안을 고려할 수도 있습니다. 물론, Microsoft 는 이미 매년 감사를 받고 있으며 외부 감사보고서를 고객에게 제공합니다. (i) 위탁 및 재위탁 계약의 결정 및 해지 절차에 관한 사항, (ii) 위탁 감독에 관한 사항, (iii) 비상 대응 계획에 관한 사항은 Service Trust Portal 에서 확인할 수 있습니다. (iii) 비상 대응 계획에 관한 사항은 Q11 을 참조하시기 바랍니다. (iv) 위탁 서비스와 관련된 조사 및 접근 권한에 관한 사항은 Q16 을 참조하시기 바랍니다. (v) 위수탁 계약에 포함될 사항은 <제 2 부: 계약 체크리스트>를 참조하시기 바랍니다.
13.	서비스 후보업체 선정 및 평가	*감독규정 별표 2-2 와 클라우드 가이드에는 '기본 보호조치'와 '금융부문 추가 보호조치'로 구성되는 평가 기준이 열거되어 있습니다. '기본 보호조치'는 클라우드 서비스 제공자가 의무적으로 준수해야 하는 일반적인 보안 기준이며 '금융부문 추가 보호조치'는 금융업계에 국한하여 적용되는 기준입니다. 국내외에서 아래의 보안 인증을 획득하여 유지하고 있는 클라우드 서비스 제공자의 경우 '기본 보호조치' 항목들에 대한 평가를 생략할 수 있습니다. Microsoft 는 클라우드 가이드(https://azure.microsoft.com/ko-kr/overview/trusted-cloud/compliance/) 에 열거된 국외 인증을 취득 했으므로 '기본 보호조치' 항목들에 대한 평가가 생략될 수 있습니다.*

<table>
<tr><th>번호</th><th>문항/요건</th><th>지침</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>분류</th><th>인증 제도</th><th>평가 생략 근거</th></tr>
<tr><td>국내</td><td>CSAP</td><td>- 과학기술정보통신부에서 관장, KISA 에서 평가 및 인증 부여
- 국내 주요 클라우드 서비스 제공자들이 인증 획득
- 약 120 개 평가 항목을 구성</td></tr>
<tr><td rowspan="3">국외</td><td>FedRAMP (높음)(미국)</td><td>- 연방정부(FedRAMP Program Management Office)에서 관장
- 최대 약 400 개 평가 항목으로 구성</td></tr>
<tr><td>CSA STAR (골드)(글로벌)</td><td>- 약 400 개 클라우드 서비스 제공자가 동참하여 CSA*에서 관장
* CSA: Cloud Service Alliance: 최대 약 300 개 평가 항목으로 구성</td></tr>
<tr><td>MTCS (레벨 3) (싱가포르)</td><td>- IMDA (Info-communications Media Development Authority)에서 관장 및 인증 부여</td></tr>
</table>
기본적으로, 클라우드 서비스 제공자에 대한 평가를 수행하는 주된 주체는 금융회사이며 위반 사고에 대응하는 기관들('금융보안원' 등)은 금융회사의 요청이 있는 경우 그러한 평가에 협조할 수 있습니다. Microsoft 는 이미 금융보안원의 평가 절차를 거쳤으며 금융회사의 평가를 지원할 준비가 완료된 상태입니다. 평가 절차와 관련된 지원에 관해서는 귀사를 담당하는 Microsoft 담당자와 상의할 수 있습니다.
</td></tr>
<tr><td>14.</td><td>클라우드 서비스 이용과 관련된 정보보호위원회의 심의 및 의결</td><td>감독규정 제 14 조의 2 제 2 항은 금융회사가 다음 사항들에 대해 정보보호위원회의 심의·의결을 거칠 것을 요구하고 있습니다.

- 이용대상 정보처리시스템의 중요도 평가 결과</td></tr>
</table>

번호	문항/요건	지침
		- *클라우드 서비스 제공자의 건전성 및 안전성 평가 결과* - *자체 업무위수탁 운영기준* 클라우드 서비스 제공자의 건전성에 대한 평가는 Q6 을 참조하시기 바랍니다. 클라우드 서비스 제공자의 안전성에 대한 평가는 Q13 을 참조하시기 바랍니다. 업무위수탁 운영기준은 Q12 를 참조하시기 바랍니다.
15.	금융감독원보고에 요구되는 서류	*금융회사는 (i) 클라우드를 이용하여 고유식별정보나 개인신용정보를 처리하거나 (ii) 클라우드 이용으로 인해 전자금융거래의 안전성과 신뢰성에 중대한 영향을 미치는 경우 금융감독원에 클라우드 이용을 보고해야 합니다.* *금융감독원에 보고하는 경우에는 이하의 서류가 요구됩니다.* *- 정보처리위탁규정 제 7 조 제 1 항 각 호에 규정된 서류* *- 이용대상 정보처리시스템의 중요도 평가에 대한 자체 중요도 평가 기준 및 결과* *- 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항* *- 클라우드 서비스 이용과 연관된 정보보호위원회의 심의 및 의결 결과* *정보처리위탁규정 제 7 조 제 1 항 각 호에 규정된 서류는 이하와 같습니다.* *(a) 위탁계약서 사본* *(b) 업무위탁규정 제 3 조의 2 에 따른 업무위수탁 운영기준* *(c) 업무위탁 계약이 관련 법령에 위반되지 않는다는 준법감시인(준법감시인이 없는 경우, 감사 등 이에 준하는 자)의 검토의견 및 관련자료 사본* *(d) 위탁의 필요성 및 기대효과*

<table>
<tr><th>번호</th><th>문항/요건</th><th>지침</th></tr>
<tr><td></td><td></td><td>
(e) 위탁에 따른 업무처리절차의 주요 변경내용
(f) 정보처리업무 운영에 대한 감독기관의 감독 능력을 확인할 수 있는 서류
(g) 위탁 계약 상대방(재위탁 예정시 재위탁 계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)
(h) 전산사고 및 정보유출 등 발생시 피해자 구제절차
<table>
<tr><td>(a) 위탁계약서 사본</td><td>본 컴플라이언스 체크리스트 제 2 부 참조.</td></tr>
<tr><td>(b) 업무위탁규정 제 3 조의 2 에 따른 업무위수탁 운영기준</td><td>Q12 참조.</td></tr>
<tr><td>(c) 위탁의 필요성 및 기대효과</td><td>Microsoft 클라우드 서비스 이용의 사업성 근거를 작성해야 합니다. 필요한 경우 이하에 수록된 Microsoft 클라우드 서비스의 핵심적인 이점들을 포함시킬 수도 있습니다.

• Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365
• Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365
• Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure

Microsoft 클라우드 서비스 이용의 사업성 근거를 작성할 때 이하에 열거된 요인들을 활용할 수도 있습니다.

• 경제성. Microsoft 클라우드 서비스는 중소기업이 경제적인 비용으로 이용할 수 있는 엔터프라이즈급 기술을 제공합니다.</td></tr>
</table>
</td></tr>
</table>

번호	문항/요건	지침	
			• 보안성. Microsoft 클라우드 서비스에는 고객 데이터를 보호하는 폭넓은 보안 기능이 포함되어 있습니다. • 가용성. Microsoft 의 데이터 센터들은 데이터 가용성을 보장할 목적으로 최상위 수준의 재난 복구 기능을 제공하고 완벽한 이중화를 갖추고 있으며 지리적으로 분산되어 있으므로 자연 재해를 비롯하여 예상치 못한 상황으로부터 데이터를 보호할 수 있습니다. 또한, Microsoft 는 대부분의 클라우드 서비스에 대해 경제적으로 뒷받침되는 99.9% 업타임(uptime)을 보장합니다. • IT 통제 및 효율성. Microsoft 클라우드 서비스는 기업의 IT 직원들이 중요성이 높은 주요 업무에 집중할 수 있도록—보안 업데이트나 백엔드 시스템 업그레이드 등의—기본적인 IT 관리 작업을 수행합니다. IT 담당 직원들은 이용자 관리 및 서비스 설정에 대한 통제를 유지합니다. 업데이트를 관리하고 보안 위협에 대처하며 실시간 서비스 향상을 보장하는 Microsoft 클라우드 서비스의 연속성은 전통적인 레거시 사설 호스팅 클라우드 환경의 추종을 불허합니다. • 이용자 친숙성 및 생산성. Microsoft Office, Outlook, SharePoint 등의 프로그램이 클라우드상에서 호스팅되므로 기업의 직원들은 노트북, PC, 스마트폰을 통해 정보에 원격으로 접근할 수 있습니다.
		(f) 정보처리업무 운영에 대한 감독기관의 감독 능력을 확인할 수 있는 서류	계약에는 감독기관이 서비스에 관련된 Microsoft 의 시설, 시스템, 프로세스, 데이터를 조사하거나 검사할 수 있는 능력을 보장하는 조항이 존재합니다. Microsoft 가 규제대상 금융회사에 제공하는 Financial Services Amendment 의 일부로서, Microsoft 는 감독기관의 요청이 있는 경우 감독기관이 현장 검사를 실시할 수 있는 권리를 포함하여 관련 서비스에 대한 검사를 실시하고 Microsoft

번호	문항/요건	지침	
			직원과 외부 감사인을 면담하며 관련 정보, 기록, 보고서, 서류에 접근할 수 있는 직접적인 권리를 보장합니다. Microsoft 는 위수탁 계약에 의거, 법률에 의해 요구되거나 고객의 지시나 동의가 없는 경우에는 감독기관에 고객 데이터를 공개하지 않을 것임을 확약합니다.
		(g) 위수탁 계약 상대방(재위탁 예정시 재위탁 계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)	대한민국마이크로소프트(유) (우)03142 서울 종로구 종로 1 길 50 더 케이트윈타워 A 동 12 층
		(h) 전산사고 및 정보유출 등 발생시 피해자 구제절차	Azure 및 Office 365 를 위한 사고 관리 이행 가이드는 고객이 Microsoft 클라우드 환경의 보안 태세를 강화할 목적으로 활용할 수 있는 포괄적인 문서에 해당합니다. 이 자료는 제품 내 로깅 기능에 의해 구현되는 예방, 탐지, 경보, 이상 활동 모니터링, 사고 사후 조사 등 최적의 보안 사고 관리를 위한 최선의 테넌트 설정 방법을 제시하고 있습니다. Microsoft 의 Office 365 Security Incident Management 및 Azure Security Response 프로그램 문서 역시 고객이 Microsoft 의 자체 사고 관리 기능·방침·프로세스를 평가할 수 있도록 지원합니다.

D. 기술적·운영적 위험 Q&A

금융회사는 업무 연속성 관리 및 IT 보안 위험 요건(위탁에 특별한 것은 아니지만 그럼에도 위탁의 맥락에서 반드시 고려해야 하는 요건)을 규정한 클라우드 가이드(부록: 금융분야 클라우드 컴퓨팅 서비스 제공 기준)에 명시된 보안 평가 항목들에 근거하여 IT 위험, 보안 위험, IT 보안 위험, 운영 위험에 대처하는 적절한 조치를 시행할 필요가 있습니다. 본 장에는 발생 가능한 다수의 기술적·운영적 문제에 대처하는 Microsoft 클라우드 서비스에 관한 상세한 기술적·운영적 정보가 수록되어 있습니다. 다른 문제가 발생한 경우 Microsoft 담당자에게 즉시 연락하시기 바랍니다.

번호	문항/요건	지침
16.	서비스 제공자가 금융회사 및/또는 감독기관에 의한 감사를 허용하는가?	*감독규정 별표 2-3 및 정보처리위탁규정 제 4 조 제 3 항.* 그렇습니다. Financial Services Amendment 에 의거하여 Microsoft 는 감독기관이 감독 의무를 이행할 목적으로 클라우드 서비스 운영에 대한 검사를 요청한 경우, 감독기관이 현장 검사를 실시할 수 있는 권리를 포함하여 관련 서비스에 대한 검사를 실시하고 Microsoft 직원과 외부 감사인을 면담하며 관련 정보, 기록, 보고서, 서류에 접근할 수 있는 직접적인 권리를 보장합니다. Microsoft 는 개별 Online Service 에 대해 고객 데이터를 처리하는 과정에서 이용하는 컴퓨터, 컴퓨팅 환경, 물리적 데이터센터의 보안에 대한 감사가 수행되도록 조치합니다. 또한, 고객은 클라우드 서비스에 대한 추가적인 모니터링·감독·감사 권리와 추가적인 통제를 목적으로 선택에 의해 Financial Services Compliance Program 에도 참가할 수 있습니다. 업무위수탁 운영기준 제 29(h)항에 관련된 추가적인 내용은 제 2 부를 참조하시기 바랍니다.
17.	서비스 제공자의 서비스가 제 3 자 감사의 대상에 해당하는가?	그렇습니다. Microsoft 의 클라우드 서비스는 SSAE16 SOC1 Type II, SSAE SOC2 Type II, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27018 등 정기적, 독립적 제 3 자 감사의 대상이 됩니다. Deloitte 등이 수행하는 철저한 제 3 자 감사를 통해 클라우드 서비스가 상기 기준의 엄격한 요건을 준수하는지 여부를 검증할 뿐만 아니라, Financial Services Amendment 를 통해 고객에게 Financial Services Compliance Program 에 참가할 수 있는 기회를 부여합니다. 이를 통해 고객은 (여타 활동들에 추가하여) Microsoft 가 개최하는 연례 웹캐스트(webcast)에 참가하여 감사를 통해 확인된 미비점을 시정하기 위해 예정된 조치들에 관한 상세한 정보에 후속적으로 접근하고 또한 감사 결과에 대해 협의할 수 있습니다. 그리고, Financial Services Compliance Program 구성원에게는 웹캐스트 녹화 영상이 제공됩니다.
18.	서비스 제공자의 인프라 내에서 고객 데이터 같은 비밀정보의 전송 및 저장을 보호하기 위해 어떤 보안 통제 조치가 시행되고 있는가?	Microsoft 는 수탁사로서 업계에서 클라우드 보안을 선도하고 있고, 가장 선진화된 조직의 온프레미스 데이터센터와 대등하거나 그보다 더 엄격한 수준의 방침 및 통제를 시행하고 있습니다. Microsoft 클라우드 서비스는 물리적·논리적·프로세스적·관리적 통제를 아우르는 엄격한 국제 기준인 ISO/IEC 27001 과 ISO/IEC 27018 에 근거하여 구축되었습니다.

번호	문항/요건	지침
		Microsoft 클라우드 서비스 보안 기능은 (a) 기본적으로 탑재된 보안 기능, (b) 보안 통제 그리고 (c) 확장형 보안 등 세 부분으로 구성됩니다. 여기에는 24 시간 모니터링되는 물리적 하드웨어, 분리된 고객 데이터, 자동화된 운영 및 록박스(lock-box) 프로세스, 보안 네트워크, 암호화 데이터가 포함됩니다. Microsoft 는 Microsoft 클라우드 서비스의 설계·개발·구축을 포괄하는 모든 단계에 적용되는 종합적인 보안 프로세스로서 Microsoft Security Development Lifecycle (SDL)을 운영합니다. SDL 은 설계요건, 공격 표면(attack surface) 분석, 위협 모델링을 통해 Microsoft 가 서비스 개시시점부터 제품 수명주기 전반에 걸쳐 취약성과 위협을 예측·식별·경감할 수 있도록 지원합니다. Microsoft 데이터센터들 내 네트워크는 주요 백엔드 서버와 스토리지 디바이스를 외부공개 인터페이스로부터 물리적으로 분리할 목적으로 분할되어 있습니다. 엣지 라우터 보안은 침입과 취약성 징후를 탐지할 수 있는 능력을 갖추고 있습니다. 인터넷을 통한 고객의 서비스 접근은, 이용자의 인터넷 가능 위치에서 시작하여 Microsoft 데이터센터에서 종료되고, 이러한 연결은 업계 표준 TLS (transport layer security)를 이용하여 암호화됩니다. TLS 를 이용함으로써 고도의 보안성을 갖춘 클라이언트-서버 연결을 수립하여 데스크톱과 데이터센터 간의 데이터 기밀성과 무결성을 보장할 수 있습니다. 고객은 발신 및 수신 이메일에 대해 Microsoft 클라우드 서비스와 외부 서버 간의 TLS 를 설정할 수 있는데, 이 기능은 기본으로 제공됩니다. 또한, Microsoft 는 서비스 거부 공격을 방지할 목적으로 트래픽 제한을 실시합니다. Microsoft 는 보안 침입을 미연에 예측하고 방지하기 위한 방어전략으로 '공격 예방·탐지·경감' 프로세스를 시행합니다. 여기에는 포트 스캐닝 및 복원, 경계 취약성 스캐닝, 최신 보안 소프트웨어 업데이트를 통한 OS 패칭, 네트워크 수준에서의 DDOS 탐지 및 방지, 서비스 액세스를 위한 멀티 팩터 인증 등을 포함하는 기본적인 보안 기능에 대한 지속적인 개선이 수반됩니다. 강력한 패스워드의 사용이 강제되며 패스워드는 정기적으로 변경해야 합니다. 조직 구성원 및 프로세스의 관점에서, 침입을 방지하기 위해서는 모든 운영자/관리자의 접근과 행동에 대한 감사, 서비스 관리자의 제로 스탠딩 권한, 서비스 장애 해결을 담당하는 엔지니어 권한의 'JIT (Just-In-Time) 접근 및 권한 상승' (즉 필요한 경우에 한하여 필요한 시점에서만 권한 상승이 허용됨), 직원 이메일 환경과 작성 액세스 환경과의 격리가 수반됩니다. 신원 조회를 통과하지 못한 직원은 상위 권한 액세스가 자동으로 거부되며, 직원 신원조회는 엄격한 조사가 수반되는

번호	문항/요건	지침
		자동화 되지 않은 승인(manual-approval) 절차를 따릅니다. 또한, 침입 방지에는 직원이 퇴사하거나 부서를 변경하거나 만료 이전에 계정을 사용하지 않는 경우에 불필요한 계정을 자동으로 삭제하는 작업이 수반됩니다. 또한, 데이터는 암호화됩니다. Microsoft 클라우드 서비스 내에서 고객 데이터는 두 가지 상태로 존재합니다. • 스토리지 미디어에 저장된 상태 • 데이터센터에서 네트워크를 거쳐 고객 디바이스로 전송 중인 상태 Microsoft 는 저장 상태의 데이터를 보호할 목적으로 다양한 기본 암호화 기능을 제공합니다. • Office 365 의 경우, Microsoft 는 고객 데이터의 기밀성과 무결성을 보호하기 위해 TLS/SSL 과 AES 같은 업계의 암호화 표준을 준수합니다. 전송 중인 데이터의 경우 고객 데이터의 보안을 보장할 목적으로 모든 고객 접점 서버가 TLS/SSL 을 이용하여 클라이언트와 보안 세션을 생성합니다. 저장된 데이터의 경우 Office 365 는 이메일과 IM 대화 그리고 SharePoint Online 과 OneDrive for Business 에 저장된 콘텐츠를 포함하여 모든 메시징 데이터가 보관된 서버에 AES 256 비트 암호화에 기반한 BitLocker 를 적용합니다. 그에 추가하여, 일부 시나리오의 경우 Microsoft 는 파일 수준의 암호화를 적용합니다. • Azure 의 경우, 암호화 커뮤니케이션과 운영 프로세스 등의 기술적 안전장치가 고객의 데이터를 안전하게 보호합니다. 또한, Microsoft 는 고객이 추가적인 암호화를 시행하고 자체 키를 관리할 수 있는 유연성을 보장합니다. 전송 중인 데이터의 경우 Azure 는 이용자 디바이스와 Microsoft 데이터센터들 간에 TLS/SSL 같은 업계 표준 보안 전송 프로토콜을 적용합니다. 저장된 데이터의 경우 Azure 는 AES-256 지원과 같은 다수의 암호화 옵션을 제공함으로써 고객의 요구에 가장 부합하는 데이터 스토리지 시나리오를 선택할 수 있는 유연성을 보장합니다.

번호	문항/요건	지침
		이러한 방침과 절차는 Trust Center 와 Service Trust Portal 을 포함하는 Microsoft 의 온라인 리소스를 통해 제공됩니다.
19.	금융회사의 데이터는 서비스 제공자가 보관하는 다른 데이터와 어떻게 분리되는가?	Microsoft 는 모든 클라우드 서비스에 대해 고객 데이터와 Microsoft 가 보관 중인 다른 데이터를 논리적으로 분리합니다. 각 테넌트의 데이터 저장 및 처리는 보안경계('사일로')를 이용하여 고객을 격리하는 '액티브 디렉토리' 구조를 통해 분리됩니다. 사일로는 공유 테넌트(co-tenants)에 의한 데이터 접근이나 침해가 불가능하도록 고객의 데이터를 안전하게 보호합니다.
20.	서비스 제공자의 접근 로그는 어떻게 모니터링하는가?	Microsoft 는 잠재적인 보안공백을 파악할 수 있도록 클라우드 기반 네트워크·애플리케이션·디바이스상에서의 활동에 대한 극대화된 가시성을 보장하기 위해 고객에게 모니터링 및 로깅 기술을 제공합니다. 클라우드 서비스에는 Azure AD Privileged Identify Management 시스템과 Multi-Factor Authentication 을 포함하여 고객이 직원들의 서비스 접근을 제한하고 모니터링할 수 있도록 지원하는 기능들이 포함되어 있습니다. 그에 추가하여, 클라우드 서비스에는 필수적인 접근권과 설정 오류가 발생할 수 있는 노출 영역을 최소화하는 기본 승인(built-in approved) Windows PowerShell Scripts 가 포함됩니다. Microsoft 는 고객 데이터가 저장된 정보 시스템에 대한 접근과 이용에 관한 로그를 직접 작성하거나 고객에 의한 작성을 지원함으로써 접근 ID, 시간, 승인 부여 혹은 거부 상황, 관련 활동을 기록합니다. Microsoft 내부의 독립적인 부서에서 분기에 1 회 이상 로그를 감사하며 고객은 그러한 감사 로그에 접근할 수 있습니다. 그에 추가하여, Microsoft 는 정당한 업무 관련성이 있는 이용자만이 적절한 시스템에 접근할 수 있도록 보장하기 위해 정기적으로 접근 레벨을 검토합니다.
21.	서비스 제공자는 비밀정보에 접근할 수 있는 직원들을 모니터링하기 위해 어떤 방침을 시행하고 있는가?	Office 365 와 Azure 의 일부 주요 서비스의 경우, 고객 데이터 콘텐츠에 접근할 수 있는 인원(직원 및 수급인 포함)에 대해서는 관련 법률에서 허용하는 신원조회, 보안교육, 접근승인이 적용되고, 신원조회는 Microsoft 가 해당 직원에게 고객 데이터 접근권을 부여하기에 앞서 실시됩니다. 법률이 허용하는 범위 내에서, 부정, 배임, 자금 세탁 혹은 직무와 관련된 중대한 허위 진술, 위조,

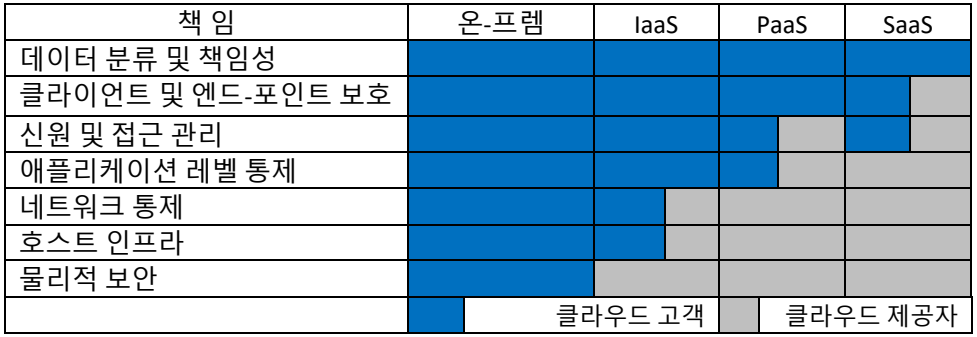
번호	문항/요건	지침
		누락이 관련된 범죄 경력을 이유로 채용 후보자의 입사 자격을 박탈할 수 있으며 이미 채용된 경우에는 후속적으로 해고될 수 있습니다.
22.	고객은 어떻게 인증하는가?	Microsoft 클라우드 서비스는 2-Factor 인증방식을 적용하여 보안을 강화합니다. 리소스 접근에 패스워드만을 요구하는 통상적인 인증 방식은 민감하거나 취약한 정보의 경우 적절한 수준의 보호를 보장할 수 없습니다. 2-Factor 인증은 보다 강력한 이용자 식별 수단을 적용하는 인증 방식입니다. Microsoft 의 전화 기반 2-Factor 인증 솔루션은 이용자가 문자로 PIN 을 수신한 후에 자신의 PIN 을 제 2 패스워드로 입력하여 서비스에 로그인할 수 있도록 합니다.
23.	서비스 제공자가 충분한 정보 보안 역량을 갖추고 있는가?	*감독규정 제 14 조의 2 제 1 항과 클라우드 가이드는 금융회사가 클라우드를 이용하기에 앞서 클라우드 서비스의 안전성을 평가할 것을 요구하고 있습니다. Microsoft 담당자에게 문의하면 Microsoft 클라우드 서비스가 클라우드 가이드의 보안평가 기준 항목을 어떻게 만족시키고 있는지에 관한 상세한 자료를 얻을 수 있습니다.* 금융회사가 Microsoft 의 정보보안 역량을 평가하고 Microsoft 클라우드 서비스의 정보보안 통제체제를 검토할 수 있는 방법에는 여러 가지가 있는데, 금융회사는 이를 통해 규제 요건을 준수하고 클라우드 서비스를 감독할 수 있습니다. 첫째, Microsoft 는 금융회사가 자체적인 보장 프로세스의 일환으로 접근, 통제, 서비스 운영을 검사하고 검증할 수 있는 기본적인 서비스 기능을 제공합니다. 여기에는 다음과 같은 기능들이 포함됩니다. • **Service Trust Portal** – Microsoft 의 서비스에 대한 최근 감사보고서와 국제표준화기구(ISO) 적용성 보고서를 포함하여 심도 깊은 기술적 신뢰 및 컴플라이언스 정보를 제공하는 기능. • **Compliance Manager** – 테스트 상태와 직전 테스트 일자를 포함하여 Microsoft 의 내부 통제에 관한 상세한 정보를 제공하고 금융회사가 자체 평가를 수행하고 내부 통제를 모니터링할 수 있도록 지원하는 도구.

번호	문항/요건	지침
		• **Office 365 Audited Controls** – 국제 기준에 대한 맵핑과 직전 테스트 일자를 포함하여 Microsoft 의 내부 통제 체제에 관한 상세한 정보를 제공하는 기능. • **Office 365 Management Activity API** – Office 365 및 Azure Active Directory 활동 로그 이벤트와 이용자, 관리자, 시스템, 방침 조치에 대한 가시성. • **Office 365 Health Dashboard** – 현재 알려진 서비스 문제점과 상시적으로 추진 중인 해결 계획을 포함하여 서비스 건전성을 즉각적으로 점검하는 기능. • **Azure Security Center** – Azure 리소스의 보안 상태와 위협 및 취약성 대응 능력에 대한 가시성. • **Azure Advisor** – Azure 환경의 보안을 더욱 강화할 수 있는 방법에 대한 지속적인 지능형 제안. • **Microsoft Trust Center** – Microsoft 의 주요 및 백업 데이터센터 위치, 재수탁업체 명단, Microsoft 서비스 관리자가 고객 데이터에 접근할 수 있는 경우에 관한 규칙 등 데이터 보호 및 보안에 관한 정보. 더 나아가, 금융부문 고객을 대상으로 작성된 Microsoft 의 확장 계약조건에는 고객의 사내 준법감시인이 감독 요건을 준수하기 위해 서비스를 보다 심층적으로 검사할 수 있는 권리가 추가되어 있습니다. 고객은 선택에 의해 참가하는 Financial Services Compliance Program 을 통해 서비스의 통제체제를 검사하고 위험관리 체제를 검토하며 Microsoft 의 감사인과 1 대 1 면담을 실시하는 동시에 Microsoft 소속 분야 전문가로부터 직접적인 의견을 구할 수 있는 기회를 가집니다. Microsoft 보안방침 거버넌스 백서는 Microsoft 의 보안방침 체제에 대한 개관과 더불어 주요 Microsoft 보안 방침 문서로의 링크를 제공합니다.

<table>
<tr><th>번호</th><th>문항/요건</th><th>지침</th></tr>
<tr><td></td><td></td><td>고객은 보안, 개인정보보호, 컴플라이언스에 관한 Azure 답변을 참조하여 Azure 그리고 기초가 되는 Office 365 / Microsoft 365 및 Dynamics 365 클라우드 서비스에 대한 Microsoft 보안 역량을 평가할 수 있습니다.</td></tr>
<tr><td>24.</td><td>금융회사가 정보 보안 방침 체제를 갖추고 있는가? 만약 그렇다면 서비스 제공자의 책임을 규정하고 있는가?</td><td>Microsoft 클라우드 서비스는 ISO 27001, PCI- DSS, FedRAMP 등 다수의 보안 체제를 준수합니다. 이러한 체제(framework)들은 알려져 있거나 알려지지 않은 위협을 지속적으로 평가하기 위해 포괄적인 Vulnerability Management Framework 를 운영할 것을 Microsoft 에게 명령합니다. Microsoft 클라우드 보안방침 체제 컴플라이언스 서비스는 Online Services Terms 의 '보안방식 및 방침' 장에 명시되어 있으며 Trust Center Compliance Offerings 페이지에 요약되어 있습니다.

금융회사의 정보보안 방침체제에는 책임공유모델(아래 도표 참조)에 따른 고객 측 및 서비스 측 통제 그리고 Online Services Terms 에 규정된 계약상의 약정에 부합하는 Microsoft 의 클라우드 서비스 제공자로서의 역할이 포함되어야 합니다.

아래 도표는 클라우드 서비스 모델 전반에 걸쳐 책임 공유 모델이 어떻게 작동하는지를 보여줍니다.

보다 자세한 정보는 클라우드 컴퓨팅 책임 공유에 관한 백서와 관련 블로그 포스트에서 확인할 수 있습니다.</td></tr>
</table>

번호	문항/요건	지침
25.	정보 보안 사고를 탐지·대응·보고하는 절차는 어떠한가?	The Azure 및 Office 365 를 위한 사고 관리 이행 가이드는 고객이 Microsoft 클라우드 환경의 보안 태세를 강화할 목적으로 활용할 수 있는 포괄적인 문서에 해당합니다. 본 자료는 제품 내 로깅 기능에 의해 구현되는 예방, 탐지, 경보, 이상 활동 모니터링, 사고 사후 조사 등 최적의 보안사고관리를 위한 최선의 테넌트 설정방법을 제시하고 있습니다. Microsoft 의 Office 365 Security Incident Management 및 Azure Security Response 프로그램 문서 역시 고객이 Microsoft 의 자체 사고관리 기능·방침·프로세스를 평가할 수 있도록 지원합니다. Microsoft 는 Online Services Terms 에 명시된 *'보안사고 통보'* (Security Incident Notification) 약정을 통해서도 고객의 컴플라이언스를 지원합니다. **"보안 사고 통보** Microsoft 가 처리 중인 고객 데이터 또는 개인 데이터의 우연한 혹은 불법적인 훼손, 손실, 변경, 무단 유출, 접근을 초래한 보안 침해(각각 '보안 사고'라 한다)를 인지한 경우 Microsoft 는 지체 없이 신속하게 (1) 고객에게 보안 사고를 통보하고 (2) 보안 사고를 조사한 후 고객에게 그에 관한 상세한 정보를 제공하며 (3) 보안 사고로 인한 영향을 경감하고 피해를 최소화하기 위해 합리적인 조치를 취해야 한다… Microsoft 는 고객이 GDPR 제 33 조 혹은 기타 관련 법률이나 규정에 의거하여 소관 감독기관과 정보 주체에게 그러한 보안 사고를 통보해야 할 의무를 이행하는 과정에 조력하기 위해 합리적인 노력을 기울여야 한다." "Microsoft 는 Core Online Services 상의 고객 데이터에 대해 이하의 보안 조치를 이행해왔으며 추후에도 유지한다…. " **사고 대응 프로세스**

번호	문항/요건	지침
		• Microsoft 는 보안 침해의 내용, 기간, 침해로 인한 결과, 보고자 성명, 피보고자, 데이터 복구 절차가 수록된 보안 침해 기록을 보존합니다. • 보안 사고를 인지한 경우 Microsoft 는 지체 없이 신속하게 (위의 '보안 사고 통보' 장에 규정된 방식으로) 그러한 사고를 통보합니다. • Microsoft 는 어떤 데이터가 누구에게 언제 공개 되었는지를 포함하여 고객 데이터 공개 내역을 자체적으로 추적하거나 고객이 추적할 수 있도록 지원합니다. **서비스 모니터링**. Microsoft 보안 관계자는 로그를 상시적으로 모니터링하여 이상 활동을 탐지하고 필요한 경우에는 시정 방안을 제안합니다. 더 나아가, 고객이 선택에 의해 참가하는 Financial Services Compliance Program 은 그 성격과 공통적인 원인, 해법을 포함하여 정보 보안 사고와 잠재적 위협에 관한 Microsoft 와의 심도 깊은 정보 공유를 제공합니다. Microsoft Threat Protection (**MTP**)을 비롯한 기타 보안 제품과 기능은 금융회사가 이러한 의무를 준수할 수 있도록 지원합니다. MTP 는 신원(identities), 엔드-포인트, 이용자 데이터, 클라우드 앱, 인프라 전반에 걸쳐 보호를 제공합니다. Microsoft 는 아래 제 26 항에 상세하게 기술된 Online Services Terms 상의 '감사 컴플라이언스' 약정을 통해 실효성과 목적 적합성을 보장할 목적으로 Microsoft 클라우드 서비스 정보보안 대응계획을 매년 검토하고 테스트해야 할 의무를 준수할 수 있도록 지원합니다.
26.	서비스 제공자가 적용하는 절차를 포함하여 정보 보안 통제의 실효성을 테스트하고 그에 관한	Microsoft 는 Online Services Terms 상의 '감사 컴플라이언스' 약정을 통해 Microsoft 클라우드 서비스에 대한 테스트에 관련된 이러한 규정을 준수할 수 있도록 지원합니다.

번호	문항/요건	지침
	내부 감사를 실시하기 위해 어떤 절차가 시행되고 있는가?	"**감사 컴플라이언스** Microsoft 는 고객정보와 개인정보를 처리하는 과정에서 이용하는 컴퓨터, 컴퓨팅 환경, 물리적 데이터센터의 보안에 대한 감사를 아래와 같이 실시합니다. • 표준(standard)이나 체제(framework)에서 감사를 규정하고 있는 경우에는 그러한 통제 표준이나 체제에 따른 감사를 최소한 1 년에 1 회 이상 실시한다. • 모든 감사는 각각의 관련 통제 표준이나 체제를 관장하는 감독 또는 인증 기구의 표준과 규칙에 의거하여 실시한다. • 모든 감사는 Microsoft 가 선임하고 비용을 부담하는 적격 있고 독립된 제 3 자 보안 감사인에 의해 실시된다. 모든 감사에는 감사보고서(**Microsoft 감사보고서**)의 작성이 수반되며 Microsoft 는 그러한 감사보고서를 https://servicetrust.microsoft.com/ 혹은 Microsoft 가 지정한 다른 위치에서 제공합니다. Microsoft 감사보고서는 Microsoft 의 비밀정보에 해당하며 감사인이 파악한 중요한 발견사항을 명확하게 공시합니다. Microsoft 는 Microsoft 감사보고서에서 지적된 사항들을 감사인이 만족할 수 있는 방식으로 신속하게 시정합니다." 더 나아가, 금융부문 고객을 대상으로 작성된 Microsoft 의 확장된 계약조건에는 규제요건을 준수하기 위해 고객이 서비스를 보다 심층적으로 검사할 수 있는 능력이 추가되어 있습니다. Financial Services Compliance Program 에 참가를 원하는 규제대상 금융회사 고객(사내·외 감사인 포함)은 Microsoft 사업장에 대한 감사를 실시하고 서비스의 통제체제를 검사하고 위험관리 체제를 검토하며 Microsoft 의 독립 감사인과 1 대 1 면담을 실시하는 동시에 Microsoft 소속 분야 전문가로부터 직접적인 의견을 구할 수 있는 권리를 보유합니다.
27.	컴퓨터 시스템 장애, 전자적인 침해 등이 발생한 경우 침해	*2.1. 클라우드 가이드 보안 평가에 따른 추가적인 금융부문 보호 조치들은 이하와 같습니다.*

번호	문항/요건	지침
	사고에 대응하는 금융회사와 조직에 즉시 통보하고 적절한 방식으로 대처하는 조치가 존재하는가?	*감독규정 제 73 조는 다음 각 호의 경우 금융회사가 금융감독원에 보고할 것을 요구하고 있습니다.* *1. 정보처리시스템 또는 통신회선 등의 장애로 10 분 이상 전산업무가 중단 또는 지연된 경우* *2. 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우* *3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로 인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우* *4. 전자금융거래법 제 9 조 제 1 항의 규정에서 정하는 사고* *전자금융거래법 제 21 조의 5 제 1 항(침해사고의 통지 등)은 전자적 침해행위로 인하여 전자금융시설이 교란·마비되는 등의 사고가 발생한 경우 금융회사가 금융위원회에 지체 없이 알려야 한다고 규정하고 있습니다.* Microsoft 는 위 제 25 항에 발췌된 Online Services Terms 상의 '감사 컴플라이언스' 약정을 통해 컴플라이언스를 지원합니다. Microsoft 가 금융회사에 정보보안사고를 통보한 경우 해당 금융회사는 사고를 '인지하게' 되므로 Microsoft 로부터 통보를 수령하고 해당 사고가 전자금융거래법 제 21 조의 5 에 따른 금융위원회통보 및 감독규정 제 73 조에 따른 금융감독원 통보 대상에 해당하는지 여부를 판단한 후에 최대한 조속한 시간 내에 금융감독원에 통보해야 합니다[3]. 더 나아가, 고객이 선택에 의해 참여하는 Financial Services Compliance Program 은 그 성격과 공통적인 원인, 해법을 포함하여 정보보안사고와 잠재적 위협에 관한 Microsoft 와의 심도 깊은 정보 공유를 제공합니다.

[3] 금융기관 검사 및 제재에 관한 규정 제 42 조(주요 정보사항 보고)는 금융기관이 보고할 필요가 있다고 판단하는 중요한 사항이나 사건을 금융감독원에 보고해야 한다고 규정하고 있습니다.

번호	문항/요건	지침
		보안사고 모니터링은 공동의 책임이라는 점에 유의할 필요가 있습니다. Microsoft 클라우드 고객은 일부 유형의 보안사고를 탐지할 책임이 있으며 그러한 사고를 탐지하는 데 있어서 Microsoft 에 의존하지 않아야 합니다. Microsoft 는 고객이 보안 문제점을 식별하고 보안사고를 탐지할 수 있는 능력을 부여할 목적으로 제 25 항에 기술된 도구와 자원을 제공합니다.
28.	터미널과 호스트 간에 전송되는 PIN 과 기타 민감한 데이터를 보호하기 위해 어떤 방식으로 종단간 애플리케이션 암호화 보안이 적용되는가?	Microsoft 클라우드 서비스는 이용자 디바이스와 Microsoft 데이터센터 사이 또는 데이터센터들 사이에서도 네트워크를 통해 전송되는 데이터에 업계 표준의 보안전송 프로토콜을 적용합니다. Microsoft 는 저장된 데이터를 보호하기 위해 기본적인 암호화 기능을 다양하게 제공합니다. Microsoft 암호화 보안의 3 가지 주된 특징은 이하와 같습니다. 1. **신원 보안:** (이용자, 컴퓨터 혹은 양자 모두의) 신원(identity) 은 다수의 암호화 기술에서 핵심적인 요소입니다. 예를 들어, 공개 키(비대칭) 암호화의 경우 각 이용자에게 공개 키와 개인 키 한 쌍으로 구성된 키 쌍을 발급하는데, 오직 한 쌍의 키를 보유한 자만이 개인 키에 접근할 수 있으므로 해당 키를 사용하는 자를 암호화/복호화 프로세스의 당사자로 식별할 수 있습니다. Microsoft Public Key Infrastructure 는 이용자와 컴퓨터의 신원을 검증하는 인증서에 기반을 두고 있습니다. 2. **인프라 보안:** Microsoft 는 인프라를 통해 이동하는 데이터의 안전한 경로를 확보하는 동시에 인프라에 저장되는 데이터의 비밀을 보호할 목적으로 제품과 서비스 전반에 걸쳐 다양한 암호화 방식, 프로토콜, 알고리즘을 적용합니다. Microsoft 는 데이터에 대한 무단 접근을 방지하는 장벽을 구축할 목적으로 업계에서 가장 강력하고 안전한 암호화 프로토콜을 적용합니다. 적절한 키 관리는 암호화 모범규준의 핵심적인 요소이며 Microsoft 는 암호화 키에 대한 보안을 적절하게 유지하고 있습니다. 관련 프로토콜과 기술의 예는 이하와 같습니다. a. 네트워크를 통과하는 통신을 암호화하는 공유 비밀에 기초한 대칭형 암호화 기술을 적용하는 TLS (Transport Layer Security)

번호	문항/요건	지침
		b. 네트워크를 통해 전송되는 데이터의 인증, 무결성, 기밀성을 IP 패킷 수준에서 보장하는 일련의 업계 표준 프로토콜인 IPsec (Internet Protocol Security) c. 로그 파일과 저장된 고객 데이터가 보관된 디스크 드라이브를 볼륨 수준에서 암호화하는 BitLocker 기술이 적용된 Office 365 서버. BitLocker 암호화는 통제 결함(예: 접근 통제 혹은 하드웨어 재활용)으로 인해 타인이 고객 데이터가 보관된 디스크에 물리적으로 접근하는 위협에 대비할 목적으로 윈도우에 기본적으로 탑재된 데이터 보호 기능입니다. d. Exchange Online, SharePoint Online, Skype for Business 와 관련하여 고객 데이터가 보관된 디스크에 AES (Advanced Encryption Standard) 256 비트 암호화를 기반으로 구축된 BitLocker. AES-256 은 DES (Data Encryption Standard)와 RSA 2048 공개 키 암호화 기술을 대체할 목적으로 미국 정부에서 도입한 대칭형 키 데이터 암호화에 대한 NIST (National Institute of Standards and Technology) 기준입니다. e. AES 를 이용하여 윈도우 서버와 클라이언트 머신 전체 볼륨을 암호화하는 BitLocker 암호화 기능과 가상 TPM (Trusted Platform Module)을 추가할 경우 Hyper-V 가상 머신 암호화에 이용할 수 있습니다. 또한, BitLocker 는 패브릭(fabric) 관리자가 가상 머신 내에서 정보에 접근하지 못하도록 하기 위해 윈도우 서버 2016 의 쉴드 VM 을 암호화합니다. 쉴드 VM 솔루션에는 가상화 호스트 증명과 암호화 키 릴리스에 이용되는 Host Guardian Service 가 포함됩니다. f. Office 365 는 Exchange Online, Skype for Business, SharePoint Online, OneDrive for Business 와 관련하여 2 가지 키 관리 옵션(Microsoft 관리 및 고객 키)을 기반으로 서비스 수준에서 암호화를 제공합니다. 고객 키는 기본적으로 탑재된 서비스 암호화 기능으로서 고객이 Office 365 에 저장된 데이터를 암호화하는 키를 제공하고 통제할 수 있도록 지원합니다.

번호	문항/요건	지침
		g. Microsoft Azure Storage Service Encryption 은 Azure Blob 스토리지에 저장된 데이터를 암호화합니다. Azure Disk Encryption 은 운영체제 및 데이터 디스크에 대해 볼륨 암호화 작업을 수행하는 윈도우 BitLocker 기능과 리눅스 DM-Crypt 기능을 이용하여 윈도우 및 리눅스 IaaS (infrastructure as a service) 가상 머신 디스크를 암호화합니다. h. TDE (Transparent Data Encryption)는 Azure SQL 데이터베이스에 저장된 데이터를 암호화합니다. i. Azure Key Vault 는 FIPS 140-2 인증 클라우드 기반 하드웨어 보안 모듈(HSM)을 통해 클라우드 앱과 서비스에서 이용하는 암호화 키에 대한 통제를 비용효과적으로 쉽게 관리하고 유지할 수 있도록 지원합니다. j. Microsoft 클라우드 서비스 역시 S/MIME (secure/multipurpose Internet mail extensions) 메시지를 전송하고 저장하며 PGP (Pretty Good Privacy) 등의 클라이언트 측 제 3 자 암호화 솔루션을 이용하여 암호화된 메시지를 전송하고 저장합니다. **3. 앱 및 데이터 보안:** 각각의 Microsoft 클라우드 서비스에 대한 구체적인 통제는 microsoft.com/en-us/trustcenter/security/encryption 에 보다 상세하게 기술되어 있습니다.
29.	필요한 경우(예: 계약이 해지된 경우) 데이터를 안전하게 파기하거나 제거하기 위해 수립된 절차가 존재하는가?	*클라우드 가이드 기본 보호조치 세부 평가항목 12.1.6.* 그렇습니다. Microsoft 는 NIST 800-88, ISO/IEC 27001, ISO/IEC 27018, SOC 1 및 SOC 2 를 준수하는 와이핑 솔루션(wiping solution)과 모범규준 절차를 적용합니다. 와이핑이 불가능한 하드 드라이브의 경우 파기(파쇄)한 후에 정보 복구를 불가능하게 만드는 파기 프로세스(예: 해체, 파쇄, 분쇄, 소각)를 적용합니다. 적합한 처분 방식은 자산의 유형에 따라 결정되고 파기 기록은 보존됩니다. 모든 Microsoft 클라우드 서비스는 승인된 미디어 스토리지 및 처분 관리서비스를 활용합니다. 종이서류는 사전에 지정된 수명주기 종료 시점에서 승인된 방식으로 파기됩니다. Microsoft 는 고객과의 계약을 통해 클라우드 서비스가 만료 혹은 해지된 날로부터 180 일 이내에 고객의 계정을 불능화하고 계정에 저장된 고객 데이터를 삭제할 것임을 약정합니다.

번호	문항/요건	지침
		'장비의 안전한 처분 혹은 재사용 및 미디어의 처분'에는 Microsoft 가 인증을 획득한 ISO/IEC 27001 표준이 적용됩니다.
30.	사업장 및 보안 구역을 보호하기 위한 문서화된 보안 절차가 존재하는가? 만약 존재한다면 구체적인 절차는?	*클라우드 가이드 기본 보호조치 세부 평가항목 8.* 그렇습니다. 물리적 접근통제는 신분증(badge) 및 스마트 카드, 생체 스캐너, 사업장 보안요원, 상시 카메라 감시, 2중 인증 등 다양한 인증 및 보안 프로세스를 적용합니다. 동작 감지센서, 카메라 감시, 보안침해 경보를 이용하여 데이터센터에 대한 모니터링을 실시합니다.
31.	데이터센터 내 하드웨어, 소프트웨어, 데이터를 보호하기 위한 문서화된 보안 절차가 존재하는가?	*클라우드 가이드 기본 보호조치 세부 평가항목 8.* 그렇습니다. Microsoft Trust Center (microsoft.com/trustcenter)에 이에 관한 사항이 상세하게 기술되어 있습니다. 추가 정보: • 설계 및 운영 보안은 https://www.microsoft.com/en-us/trustcenter/security/designopsecurity 을 참조. • 네트워크 보안은 https://www.microsoft.com/en-us/trustcenter/security/networksecurity 을 참조. • 암호화는 https://www.microsoft.com/en-us/trustcenter/security/encryption 을 참조. • 위협 관리는 https://www.microsoft.com/en-us/trustcenter/security/threatmanagement 을 참조. • 신원 및 접근 관리는 https://www.microsoft.com/en-us/trustcenter/security/identity 을 참조.
32.	특권 관리자 계정은 어떻게 관리되는가? 이러한 계정의 발급(비상 시 이용 포함), 보호, 유지, 파기를 규율하는 절차는 무엇인가? 특권 계정에 2 중 통제를	*클라우드 가이드 기본 보호조치 세부 평가항목에 다수 존재.* Microsoft 는 고객 데이터 접근을 엄격히 통제합니다. 고객 데이터가 저장된 IT 시스템에 대한 접근은 역할기반 접근 통제(RBAC)와 록 박스(lock box) 프로세스를 통해 엄격하게 통제됩니다. 접근 통제는 업무 분장 원칙과 최소특권부여 원칙에 기반한 자동화된 프로세스에 해당합니다. 동 프로세스는 IT 시스템에 대한 접근을 요청하는 엔지니어가 이력 조회, 보안 교육 이수, 접근 승인 등의 자격 요건을 갖췄는지를 확인합니다. 그에 추가하여, 정당한 업무 관련성이 있는 이용자만이 적절한 시스템에 접근할 수 있도록

번호	문항/요건	지침
	적용하는 방식(예: 패스워드를 둘로 분할하여 각각을 서로 다른 관계자에게 부여)은 무엇인가?	보장하기 위해 정기적으로 접근 레벨을 검토합니다. 이 프로세스는 IT 시스템에 대한 접근을 요청하는 엔지니어가 자격 요건을 갖췄는지를 확인합니다. 그에 추가하여, 클라우드 서비스에는 필수적인 접근권과 설정 오류가 발생할 수 있는 노출 영역을 최소화하는 기본 승인(built-in approved) Windows PowerShell Scripts 가 포함됩니다. Microsoft 신원 및 접근 관리에 관한 보다 자세한 정보는 https://www.microsoft.com/en-us/trustcenter/security/identity 에서 확인할 수 있습니다. Microsoft 는 잠재적인 보안공백을 파악할 수 있도록 클라우드 기반 네트워크·애플리케이션·디바이스상에서의 활동에 대한 극대화된 가시성을 보장하기 위해 고객에게 모니터링 및 로깅 기술을 제공합니다. 클라우드 서비스에는 Azure AD Privileged Identify Management 시스템과 Multi-Factor Authentication 을 포함하여 고객이 직원들의 서비스 접근을 제한하고 모니터링할 수 있도록 지원하는 기능들이 포함되어 있습니다. Microsoft 는 고객 데이터가 저장된 정보 시스템에 대한 접근과 이용에 관한 로그를 직접 작성하거나 고객에 의한 작성을 지원함으로써 접근 ID, 시간, 승인 부여 혹은 거부 상황, 관련 활동을 기록합니다(Online Services Terms 13 페이지 참조). Microsoft 내부의 독립적인 부서에서 분기에 1 회 이상 로그를 감사하며 고객은 그러한 감사 로그에 접근할 수 있습니다. 그에 추가하여, Microsoft 는 정당한 업무 관련성이 있는 이용자만이 적절한 시스템에 접근할 수 있도록 보장하기 위해 정기적으로 접근 레벨을 검토합니다. Microsoft 는 2 가지 주된 소스를 통해 금융 거래를 재구성하고 감사 증적을 작성할 수 있는 정보를 고객에게 제공합니다: Azure Active Directory 는 고객 거래정보에 접근한 자와 그러한 정보에 대해 수행된 작업을 파악할 목적으로 검색이 가능한 감사 로그와 기타 정보가 보관된 저장소이고, Azure Monitor 는 고객이 고객 클라우드 정보의 변경에 관련된 '대상, 주체, 시기'를 파악하고 클라우드 서비스 운영에 관한 정보를 얻을 수 있는 활동 로그와 진단 로그를 각기 제공합니다. 비상 상황에서는 서비스 장애 해결을 목적으로 엔지니어 특권에 대해 'JIT (위의 정의 참조) 접근 및 권한 상승 시스템'이 적용됩니다(즉, 필요한 경우에 한하여 필요한 시점에서만 권한 상승이 허용됨).

번호	문항/요건	지침
33.	특권 계정의 활동을 정기적으로 캡처(예: 시스템 감사 로그)하여 검토하는가? 로그를 검토하는 주체와 검토 빈도는?	*클라우드 가이드 금융부문 추가 보호조치 항목 2.6 은 "(i)정보처리시스템 접속 기록(일시, 접속자, 접근 확인), (ii) 전산자료 접근 기록(일시, 사용자, 자료 내용), (iii) 전산자료 처리 내용 기록(사용자 로그인, 액세스 로그 등)이 접속 성공 여부와 상관없이 자동으로 기록·유지에 협조 및 지원하도록 체계가 마련되어 있는가?" 라고 규정하고 있습니다.* 그렇습니다. Microsoft 내부의 독립적인 부서에서 분기에 1 회 이상 로그를 감사합니다. 추가적인 정보는 microsoft.com/en-us/trustcenter/security/auditingandlogging 에서 확인할 수 있습니다.
34.	감사/활동 로그가 특권 계정 이용자의 부정한 개입으로부터 보호되는가? 시행 중인 안전 조치는 무엇인지?	*클라우드 가이드 기본 보호조치 세부 평가항목 10.1.* 그렇습니다. Microsoft 는 고객 데이터가 저장된 정보 시스템에 대한 접근과 이용에 관한 로그를 직접 작성하거나 고객에 의한 작성을 지원함으로써 접근 ID, 시간, 승인 부여 혹은 거부 상황, 관련 활동을 기록합니다(Online Services Terms 13 페이지 참조). Microsoft 내부의 독립적인 부서에서 분기에 1 회 이상 로그를 감사하며 고객은 그러한 감사 로그에 접근할 수 있습니다. 그에 추가하여, Microsoft 는 정당한 업무 관련성이 있는 이용자만이 적절한 시스템에 접근할 수 있도록 보장하기 위해 정기적으로 접근 레벨을 검토합니다. 모든 로그는 다른 관리자 부서에서 관리하는 로그 관리 시스템에 저장됩니다. 모든 로그는 안전한 방식으로 작성 시스템에서 로그 관리 시스템으로 자동 전송되며 부정한 개입을 방지하는 방식으로 저장됩니다.
35.	민감한 파일, 명령, 서비스에 대한 접근이 조작으로부터 제한되고 보호되는가? 시행 중인 통제는 구체적으로 무엇인지?	*클라우드 가이드 기본 보호조치 세부 평가항목 10.1.* 그렇습니다. 설정 데이터/파일 및 명령 같은 시스템 수준의 데이터는 설정 관리 시스템의 일환으로 관리됩니다. 이러한 데이터/파일/명령이 변경 또는 업데이트 되거나 삭제되면 설정 관리 시스템에 의해 이상 활동으로 간주되어 자동 삭제됩니다. 더 나아가, Microsoft 는 고객 데이터 접근을 엄격히 통제합니다. 고객 데이터가 저장된 IT 시스템에 대한 접근은 역할기반 접근 통제(RBAC)와 록 박스(lock box) 프로세스를 통해 엄격하게 통제됩니다. 접근 통제는 업무 분장 원칙과 최소 특권 부여원칙에 기반한 자동화된 프로세스에 해당합니다. 동 프로세스는 IT 시스템에 대한 접근을 요청하는 엔지니어가 이력 조회, 보안 교육 이수, 접근 승인 등의 자격 요건을 갖췄는지를 확인합니다. 그에 추가하여, 정당한 업무 관련성이 있는 이용자만이 적절한 시스템에 접근할 수

번호	문항/요건	지침
		있도록 보장하기 위해 정기적으로 접근 레벨을 검토합니다. 이 프로세스는 IT 시스템에 대한 접근을 요청하는 엔지니어가 자격 요건을 갖췄는지를 확인합니다. 그에 추가하여, 클라우드 서비스에는 필수적인 접근권과 설정 오류가 발생할 수 있는 노출 영역을 최소화하는 기본 승인(built-in approved) Windows PowerShell Scripts 가 포함됩니다. Microsoft 신원 및 접근 관리에 관한 보다 자세한 정보는 https://www.microsoft.com/en-us/trustcenter/security/identity 에서 확인할 수 있습니다.
36.	서비스 제공자가 재난 복구 혹은 업무 연속성계획을 갖추고 있는가? 그러한 계획과 귀사의 계획 간의 상호의존성을 고려하였는가?	*금융회사에 적용되는 재난 복구 및 업무 연속성 관리에 관한 다양한 의무가 <클라우드 가이드: 업무 연속성 관리>에 규정되어 있습니다. 이 요건은 Microsoft 와 같은 제 3 자인 서비스 제공자에게 업무를 위탁하는지 여부와 상관없이 적용됩니다. 귀사를 담당하는 Microsoft 고객 관리자가 Microsoft 의 재난 복구 계획에 관한 질의 그리고 귀사의 재난 복구 계획과의 상호 작용에 관한 조언을 제공합니다.* 그렇습니다. Microsoft 는 서비스에 체감이 가능할 정도의 영향을 미치지 않는 상태에서 장애를 일으킨 인프라 컴포넌트로부터 워크로드 이동이 가능하게끔 디스크, NIC, 전력 공급원, 서버 수준에서의 물리적 이중화와 상시적인 콘텐츠 복제, 강력한 백업·복원·대체 작동 기능, 실시간 이슈 탐지 및 자동화된 대응을 실시하는 등의 방식으로 서비스 중단을 최소화하기 위해 최선의 노력을 다하고 있습니다. 또한, Microsoft 는 긴급 엔지니어링 지원팀을 1 년 365 일 24 시간 운영하고 있습니다. 금융서비스 컴플라이언스 프로그램과 Premier Support 를 참고하시기 바랍니다. 또한, Office 365 Support, Premier Support for Enterprise, Azure Support Plans 도 참고가 가능합니다. • *이중화*: Microsoft 는 서버, 데이터센터, 서비스 수준에서의 물리적 이중화와 강력한 대체 작동 기능이 적용된 데이터 이중화 그리고 오프라인 기능성이 부여된 기능적 이중화를 유지합니다. 이중화가 적용된 Microsoft 의 스토리지와 데이터 복원 절차는 고객 데이터를 손실 또는 파괴 이전의 원 상태 혹은 직전 복제 상태로 복구할 목적으로 수립되었습니다. ○ Office 365 의 경우, Microsoft 는 이중화를 위해 다수의 데이터센터에 복수의 고객 데이터 사본을 보존합니다.

번호	문항/요건	지침
		○ Azure 의 경우, Microsoft 는 데이터 이중화 혹은 기타 운영상의 목적으로 특정한 권역 내에 있는 복수의 리전(region)들 간에 고객 데이터를 복제할 수 있습니다. 일례로, Azure GRS 는 중대한 데이터센터 재난에 대비하여 데이터 지속성을 강화할 목적으로 동일한 권역 내에서 2 개 리전 간에 특정한 데이터를 복제합니다. • *복원력*. Microsoft 의 클라우드 서비스는 데이터 복원력을 확대할 목적으로 오류 도메인 전반에 걸쳐 액티브 로드 밸런싱, 자동화된 대체 작동 및 인적 백업, 복구 테스팅을 제공합니다. 일례로, Azure Traffic Manager 는 서로 다른 리전들 간의 로드 밸런싱을 제공하며 고객은 Azure Virtual Networks 내에서 애플리케이션 딜리버리 컨트롤러(ADC/로드 밸런싱) 기능을 위해 네트워크 가상 어플라이언스를 이용할 수 있습니다. 로드 밸런싱은 Power BI Services, Gateway, Azure API Management 기능을 통해서도 제공됩니다. • *분산형 서비스*. 또한, Microsoft 는 어느 한 컴포넌트의 오류로 인한 영향과 범위를 제한할 목적으로 Exchange Online 이나 SharePoint Online, Lync Online 과 같은 분산형 컴포넌트 서비스를 제공합니다. 오류가 발생할 경우 서비스와 서비스를 단절시킬 목적으로 컴포넌트 서비스 전반에 걸쳐 디렉토리 데이터 역시 복제됩니다. • *모니터링*. Microsoft 의 클라우드 서비스에는 자동 복구를 구동하는 내부 모니터링, 사고를 경고하는 아웃사이드-인 모니터링, 로깅·감사·개별 추적에 대한 방대한 진단 기능이 포함됩니다. • *단순화*. Microsoft 는 이슈 분리 복잡성을 낮출 목적으로 표준화된 하드웨어를 이용합니다. 또한, Microsoft 는 완전 자동화된 구축 모델과 표준 탑재 관리 메커니즘을 적용하고 있습니다. • *인적 백업*. Microsoft 의 클라우드 서비스에는 1 년 365 일 24 시간 긴급 지원을 제공하는 자동화된 복구 서비스, 신속한 대응과 해결을 보장하는 다양한 역량을 갖춘 긴급 지원팀 그리고 긴급 지원팀이 습득한 지식에 기반한 지속적인 개선이 포함됩니다.

번호	문항/요건	지침
		• *지속적 학습*. 사고가 발생한 경우 Microsoft 는 철저한 사고 사후 검토를 실시합니다. 이러한 사고 사후 검토는 발생 사건에 대한 분석, Microsoft 의 대응, 추후에 유사한 문제의 재발을 방지하는 Microsoft 의 계획으로 구성되고, Microsoft 는 서비스 사고로 인한 피해를 입은 고객과 사고 사후 검토 결과를 공유합니다. • *재난 복구 테스트*. Microsoft 는 1 년에 1 회 이상 재난 복구 테스트를 실시합니다.
37.	서비스 제공자에게 위탁하는 시스템 혹은 애플리케이션의 복구목표시간(RTO)은?	*클라우드 가이드 금융부문 추가 보호조치 항목은 금융회사가 각 업무별로 지정한 복구목표시간(RTO)을 준수할 수 있도록 협조 및 지원 체계가 마련되어 있어야 한다고 규정하고 있습니다. 감독규정 제 23 조 제 9 항은 핵심업무의 복구목표시간은 3 시간 이내로 하되, '보험업법'에 의한 보험회사의 핵심업무의 경우에는 24 시간 이내로 한다고 규정하고 있습니다.* • **Azure:** 이에 관한 사항은 서비스 수준 협약(SLA)을 참고하시기 바랍니다. (http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37) Microsoft 와 고객은 회복력(resilience)를 위하여 애플리케이션을 디자인하는 것에 대한 책임을 공유합니다. Azure 는 다양한 디자인 및 컨피규레이션과 함께 Availability Sets, Availability Zones 및 geo-redundant Azure Regions 을 활용하는 리질리언스 플랫폼을 제공합니다. 그러나 리질리언시 요건을 위해 애플리케이션을 디자인하고 구성하는 것은 고객의 책임입니다. • **Office 365:** Office365 는 액티브/액티브 설정을 적용하여 운용됩니다. 예를 들어, Exchange Online 은 24 시간 지연된 온라인 데이터 사본에 기초하여 액티브:액티브:액티브:액티브 설정을 적용하여 운용됩니다. 이러한 설정을 통해 서비스가 고도의 복원력 설계를 충족하고 데이터센터 전손과 같은 블랙스완 사태에 대처할 수 있습니다. 본 서비스가 즉각적인 대체 작동에 유사한 능력과 데이터 무손실을 목표로 구축되었다는 점에서 RTO/RPO 는 액티브/액티브 설정의 평가 혹은 Exchange Online 과 같은 서비스에 대한 유효한 기준으로 간주되지 않습니다.

번호	문항/요건	지침
38.	서비스 제공자에게 위탁한 시스템이나 애플리케이션의 복구목표지점(RPO)은 어떠한가?	*클라우드 가이드 금융부문 추가 보호조치 항목은 금융회사가 각 업무별로 지정한 복구목표시간(RTO)을 준수할 수 있도록 협조 및 지원 체계가 마련되어 있어야 한다고 규정하고 있습니다. 감독규정 제 23 조 제 9 항은 핵심업무의 복구목표시간은 3 시간 이내로 하되, '보험업법'에 의한 보험회사의 핵심업무의 경우에는 24 시간 이내로 한다고 규정하고 있습니다.* • **Azure:** 이에 관한 사항은 서비스 수준 협약(SLA)을 참고하시기 바랍니다. (http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37) Microsoft 와 고객은 회복력(resilience)를 위하여 애플리케이션을 디자인하는 것에 대한 책임을 공유합니다. Azure 는 다양한 디자인 및 컨피규레이션과 함께 Availability Sets, Availability Zones 및 geo-redundant Azure Regions 을 활용하는 리질리언스 플랫폼을 제공합니다. 그러나 리질리언시 요건을 위해 애플리케이션을 디자인하고 구성하는 것은 고객의 책임입니다. • **Office 365:** Office365 는 액티브/액티브 설정을 적용하여 운용됩니다. 예를 들어, Exchange Online 은 24 시간 지연된 온라인 데이터 사본에 기초하여 액티브:액티브:액티브:액티브 설정을 적용하여 운용됩니다. 이러한 설정을 통해 서비스가 고도의 복원력 설계를 충족하고 데이터센터 전손과 같은 블랙스완 사태에 대처할 수 있습니다. 본 서비스가 즉각적인 대체 작동에 유사한 능력과 데이터 무손실을 목표로 구축되었다는 점에서 RTO/RPO 는 액티브/액티브 설정의 평가 혹은 Exchange Online 과 같은 서비스에 대한 유효한 기준으로 간주되지 않습니다.
39.	서비스 제공자가 보관하는 귀사의 데이터에 대한 데이터 백업과 복구 체제는 어떠한가?	*클라우드 가이드 금융부문 추가 보호조치 항목 2.7 은 이중화 및 백업 체계 구축에 관해 규정하고 있습니다.* **이중화** • 서버, 데이터센터, 서비스 수준에서 물리적 이중화 • 강력한 대체작동 기능이 포함된 데이터 이중화

번호	문항/요건	지침
		• 오프라인 기능이 포함된 기능적 이중화 이중화가 적용된 Microsoft 의 스토리지와 데이터 복원 절차는 고객 데이터를 손실 또는 파괴 이전의 원 상태 혹은 직전 복제 상태로 복구할 목적으로 수립되었습니다. 그에 추가하여, Microsoft 는 복수의 라이브(live) 데이터 사본을 상시 보존합니다. 라이브 데이터는 연속적인 데이터 접근을 보장하는 '폴트 존(fault zone)'으로 구분됩니다. Office 365 의 경우 Microsoft 는 이중화를 목표로 복수의 고객 데이터 사본을 보존하고 Azure 의 경우 Microsoft 는 데이터 이중화 혹은 기타 운영상의 목적으로 특정한 권역 내의 리전들 간에 고객 데이터를 복제할 수 있습니다. 일례로, Azure Globally-Redundant Storage 는 중대한 데이터센터 재난에 대비하여 데이터 내구성을 강화할 목적으로 동일한 권역 내의 두 리전 간에 특정한 데이터를 복제합니다. **복원력** • 액티브 로드 밸런싱 • 자동화된 대체작동 및 인적 백업 • 오류 도메인 전반에 걸친 복구 테스팅 일례로, Azure Traffic Manager 는 서로 다른 지역들 간의 로드 밸런싱을 제공하며 고객은 Azure Virtual Networks 내에서 애플리케이션 딜리버리 컨트롤러(ADC/로드 밸런싱) 기능을 위해 네트워크 가상 어플라이언스를 이용할 수 있습니다. 로드 밸런싱은 Power BI Services, Gateway, Azure API Management 기능을 통해서도 제공됩니다. Office 365 서비스는 데이터의 손상(corruption)을 방지하고 데이터를 서로 다른 폴트존으로 분리하며, 또한 ACID 테스트 부적격 여부를 모니터링하는 동시에 고객의 자체적인 복구를 지원할 목적으로 수립된 구체적인 복원력 원칙들에 근간을 두고 있습니다. **분산형 서비스** • Exchange Online, SharePoint Online, Skype for Business 같은 분산형 컴포넌트 서비스를 통해 특정한 컴포넌트의 오류로 인한 영향 및 범위 제한

번호	문항/요건	지침
		• 컴포넌트 서비스들 간에 복제된 디렉토리 데이터를 통해 오류가 발생한 경우 서비스와 서비스 단절 • 단순화된 운영과 구축 **모니터링** • 자동 복구를 구동할 목적으로 구축된 내부 모니터링 • 아웃사이드-인 모니터링을 통한 사고 경보 발령 • 방대한 진단 기능을 통한 로깅·감사·개별 추적 **단순화** • 표준화된 하드웨어를 통한 이슈 분리 복잡성 경감 • 완전 자동화된 구축 모델 • 기본 탑재 관리 체계 **인적 백업** • 1 년 365 일 24 시간 긴급 지원을 제공하는 자동화된 복구 조치 • 신속한 대응과 해결을 보장하는 다양한 역량을 갖춘 긴급 지원팀 • 긴급 지원팀이 습득한 지식에 기반한 지속적인 개선 **지속적 학습** • 사고가 발생할 때마다 Microsoft 가 철저한 사후 검토를 실시. • Microsoft 의 사후 검토는 발생한 사건에 대한 분석, Microsoft 의 대응 및 추후에 유사한 문제의 재발을 방지하는 계획으로 구성.

번호	문항/요건	지침
		• 고객이 서비스 사고로 인한 피해를 입은 경우 Microsoft 는 해당 고객과 사후 검토 결과를 공유. **재난 복구 테스트** • Microsoft 는 1 년에 1 회 이상 재난 복구 테스트를 실시합니다.
40.	서비스 제공자는 재난 복구 테스트를 어떤 빈도로 실시하는가?	*장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 상황별 대응절차, 재해복구계획, 비상대응조직의 구성 및 운용, 모의훈련, 비상연락체계, 파업 시 비상지원인력, 업무 매뉴얼 등을 포함한 업무지속성 확보방안을 수립·준수하고 주기적으로 점검하는가? (클라우드 가이드 금융부문 추가 보호조치 항목 2.7)* Microsoft 는 1 년에 최소한 1 회 이상 재난 복구 테스트를 실시합니다. 그 배경으로, Microsoft 는 서버, 데이터센터, 서비스 수준에서 물리적 이중화, 강력한 대체 작동 기능이 포함된 데이터 이중화, 오프라인 기능이 포함된 기능적 이중화를 실시합니다. 이중화가 적용된 Microsoft 의 스토리지와 데이터 복원 절차는 고객 데이터를 손실 또는 파괴 이전의 원 상태 혹은 직전 복제 상태로 복구할 목적으로 수립되었습니다. Microsoft 는 복수의 라이브 데이터 사본을 상시 보존합니다. 라이브 데이터는 연속적인 데이터 접근을 보장하는 '폴트 존(fault zone)'으로 구분됩니다. Office 365 의 경우 Microsoft 는 이중화를 목표로 복수의 고객 데이터 사본을 보존하고, Azure 의 경우 Microsoft 는 고객이 동일 국가 내에서 쌍을 이루는 리전에 데이터 사본을 복제할 수 있도록 지원하는 설정 옵션을 제공하고 있습니다. 일부 서비스의 경우 복원력을 목적으로 쌍을 이루는 리전들 간에 메타데이터를 복제할 수 있습니다. 데이터 복원력을 강화할 목적으로, Microsoft 의 클라우드 서비스는 액티브 로드 밸런싱, 자동화된 대체 작동 및 인적 백업, 오류 도메인 전반에 걸친 복구 테스트를 제공합니다. 일례로, Azure Traffic Manager 는 서로 다른 지역들 간의 로드 밸런싱을 제공하며 고객은 Azure Virtual Networks 내에서 애플리케이션 딜리버리 컨트롤러(ADC/로드 밸런싱) 기능을 위해 네트워크 가상 어플라이언스를 이용할 수 있습니다. 로드 밸런싱은 Power BI Services, Gateway, Azure API Management 기능을 통해서도 제공됩니다. Office 365 서비스는 데이터의 손상(corruption)을 방지하고 데이터를 서로 다른 폴트 존으로 분리하며, 또한 ACID

번호	문항/요건	지침
		테스트 부적격 여부를 모니터링하는 동시에 고객의 자체적인 복구를 지원할 목적으로 수립된 구체적인 복원력 원칙들에 근간을 두고 있습니다. 이에 관한 보다 자세한 사항은 Microsoft 에서 발간한 백서 'Microsoft Office 365 의 데이터 복원력'을 https://aka.ms/Office365DR 에서 확인할 수 있습니다.

제 2 부: 계약 체크리스트

계약 서류는 어떻게 구성되는가?

감독규정 별표 2-3 과 정보처리위탁규정 제 4 조는 위수탁 계약에 반드시 구비해야 할 항목들을 열거하고 있습니다. 귀사와 Microsoft 가 체결한 계약은 다양한 부분들로 구성되어 있습니다. 필요한 경우 귀사를 담당하는 Microsoft 고객 담당자로부터 관련 부분들에 관한 설명을 들을 수 있습니다. 관련 Microsoft 서류들이 아래 표에 제시되어 있으니 참고하시기 바랍니다.

Microsoft 핵심 계약 서류	**Microsoft 계약에 통합되는 서류**[4]
Microsoft Business and Services Agreement (**MBSA**) Enterprise Agreement (**EA**) 및 등록 계약 **Enrollment** (Enterprise Enrollment 혹은 Server and Cloud Enrollment)	GDPR 조항을 포함하여 Data Protection Terms (**DPT**)을 통합하는 Online Service Terms (**OST**) **제품 계약서(Product Terms)** Online Services 서비스 수준 협약(**SLA**).
금융회사 고객을 대상으로 핵심 계약 서류에 추가하여 Microsoft 가 제공하는 변경계약서 **Financial Services Amendment**	**계약의 일부를 구성하지 않는 근거 서류 및 정보**[5] **Trust Center** 에서 제공되는 자료

본 제 2 부가 적용되는 대상은?

[4] www.microsoft.com/contracts 에서 확인할 수 있음.

[5] www.microsoft.com/trustcenter 에서 확인할 수 있음.

I. 감독규정 별표2-3과 정보처리위탁규정 제4조는 귀사가 클라우드 서비스 제공자와 체결한 계약서에 특정한 사항들이 반드시 기재되어야 한다고 규정하고 있습니다. 본 제2부는 계약서에 반드시 기재되어야 하는 구체적인 항목들을 제시하고 있으며, 두 번째 세로열에는 Microsoft 계약 서류에서 관련 필수 요건들을 다루고 있는 부분과 방식을 표시하고 있습니다.

전자금융감독규정 [별표2-3]

1. 위수탁 계약서 주요 기재사항

	위수탁 계약서 주요 기재사항	Microsoft 계약에서 관련 사항을 다루고 있는 부분 및 방식	관련 법규
1.	클라우드 컴퓨팅 서비스가 제공되는 물리적 위치	관련 조건은 Microsoft 와 금융회사 고객이 체결한 Microsoft Online Services Terms (OST)에 대한 부칙에 해당하는 Data Protection Addendum (DPA)의 "데이터 전송 및 위치(Data Transfers and Location)" 조항(DPA, 8 면)에 규정되어 있음. 대한민국 내 고객 데이터 저장 위치는 아래 링크에서 확인할 수 있음. http://azuredatacentermap.azurewebsites.net/	
2.	재위탁 또는 재위탁의 변경 등 금융회사 또는 전자금융업자의 동의가 필요한 사항	현재 재수탁자 및 재수탁자가 담당하고 있는 서비스는 Service Trust Portal 에서 확인 가능하며, 고객은 이와 같은 재수탁자를 통한 처리에 동의한 것으로 봄. Microsoft 가 새롭게 재위탁을 하는 경우, Microsoft 는 사전에 고객에게 통보함(재수탁자에게 고객 데이터에 대한 접근을 허용하기 최소 6 개월 전, 재수탁자에게 고객 데이터에 포함된 개인 데이터 외의 개인 데이터에 대한 접근을 허용하는 경우에는 14 일 전). 고객이 새로운 재수탁자를 승인하지 않는 경우 고객은 해지 서면을 제출함으로써 관련 서비스를 해지할 수 있음(DPA, 9 면).	• 신용정보 처리 재위탁의 제한에 관한 사항(신용정보업감독규정 [별표4] 3. 라목) • 수탁자가 위탁 받은 업무를 재위탁하는 경우 위탁자에 대한 보고에 관한 사항(신용정보업감독규정 [별표4] 3. 마목) • 재위탁 제한에 관한 사항(개인정보 보호법 시행령 제28조 제1항 제2호)

3.	위탁하는 업무, 데이터에 관한 사항	[위탁하는 업무] 계약서 일체는 당사자들의 개별적 약정과 합의의 범위를 포괄적으로 규정하고 있음. 클라우드 서비스는 EA Enrollment 에 의거하여 발주되며 주문에는 클라우드 서비스와 관련 요금이 명시됨. Microsoft 는 각각의 금융회사 고객들과 클라우드 서비스에 대한 계약을 체결하며, 여기에는 Financial Services Amendment, Online Services Terms, Data Protection Addendum, Service Level Agreement 이 포함됨. 이러한 계약들은 고객에게 제공될 클라우드 서비스를 명확하게 정의함. 서비스들은 관련 이용권과 함께 Product Terms 와 OST, 그 중에서도 특히 OST "핵심 클라우드 서비스(Core Online Services)" 약정에 광범위하게 기술됨. [데이터에 관한 사항] DPA 에 의거하여, 고객은 가입 기간 그리고 종료일로부터 최소 90 일간의 보유 기간 동안 언제라도 각각의 Online Service 에 저장된 고객 데이터에 접근하고 추출할 수 있는 권리를 가짐. Microsoft 는 DPA 에 저장된 고객 데이터에 대해서도 구체적인 약정을 제공함. 요약하면, Microsoft 는 아래와 같은 약정을 제공함. 1. 고객 데이터에 대한 소유권은 계속해서 고객에게 있음. 2. 고객 데이터는 고객에게 클라우드 서비스를 제공하는 것에 부수되는 "Microsoft 의 적법한 업무처리 (legitimate business operations)"(DPA 의 "처리의 성격, 소유권(Nature of Processing; Ownership)"에 추가로 규정됨)을 위해 고객에게	• 제공되는 신용정보의 범위 및 제공·이용 목적 (신용정보업감독규정 [별표4] 1. 가.) • 제공된 신용정보의 업무 목적외 사용 및 제3자 앞 제공 금지에 관한 사항(신용정보업감독규정 [별표4] 1. 나.) • 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항(개인정보 보호법 제26조 제1항 제1호) • 위탁업무의 목적 및 범위(개인정보 보호법 시행령 제28조 제1항 제1호)

		클라우드 서비스를 제공하는 목적에 한하여 이용할 수 있음. 고객 데이터는 광고나 상업적 목적을 포함하여 다른 어떠한 목적으로도 이용할 수 없음. 3. Microsoft 는 법률에 의해 강제되고 정보 제출 명령을 고객에게 전가할 수 없는 경우가 아닌 한 법집행 기관에 고객 데이터를 공개하지 않음. 4. Microsoft 는 우발적이거나 인가되지 않았거나 위법한 접근·공개·변경·손실·파괴로부터 고객 데이터를 보호할 목적으로 적절한 기술적·조직적 조치, 내부 통제, 정보 보안 절차를 이행하고 유지함. 5. Microsoft 는 보안 사고를 인지한 경우 고객에게 통보하며 보안 사고로 인한 영향을 경감하고 피해를 최소화하기 위해 합리적인 조치를 취함. 6. MBSA 는 비밀유지에 관해 규정하고 있음. Microsoft 는 (법률에 의해 요구되지 않는 한) 비밀정보(고객 데이터 포함)를 제 3 자에게 공개하지 않으며 Microsoft 와 고객과의 비즈니스를 위한 목적으로만 비밀정보를 사용할 것임을 약정함. Microsoft 가 비밀유지 의무를 위반한 경우 고객은 Microsoft 를 상대로 계약 위반을 원인으로 한 클레임을 제기할 수 있음.	
4.	위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 등 금융회사 또는 전자금융업자에 대한 통보가 필요한 사항	현재 재수탁자 및 재수탁자가 담당하고 있는 서비스는 Service Trust Portal 에서 확인 가능하며, 고객은 이와 같은 재수탁자를 통한 처리에 동의한 것으로 봄 Microsoft 가 새롭게 재위탁을 하는 경우, Microsoft 는 사전에 고객에게 통보함(재수탁자에게 고객 데이터에 대한 접근을 허용하기 최소 6 개월 전, 재수탁자에게 고객 데이터에 포함된 개인 데이터 외의 개인 데이터 에 대한 접근을 허용하는 경우에는 14 일 전). 고객이 새로운	• 신용정보 처리 재위탁의 제한에 관한 사항(신용정보업감독규정 [별표4] 3. 라목) • 수탁자가 위탁받은 업무를 재위탁하는 경우 위탁자에 대한 보고에 관한

		재수탁자를 승인하지 않는 경우 고객은 해지 서면을 제출함으로써 관련 서비스를 해지할 수 있음(DPA, 9 면).	사항(신용정보업감독규정 [별표4] 3. 마.) • 재위탁 제한에 관한 사항(개인정보 보호법 시행령 제28조 제1항 제2호)
5.	감독당국 또는 내외부 감사인의 조사 접근(현장방문 포함) 수용 의무	계약에는 금융회사가 서비스에 관련된 Microsoft 의 시설, 시스템, 프로세스, 데이터를 조사하거나 검사할 수 있는 능력을 부여하는 조항이 포함되어 있음. Microsoft 가 규제 대상 금융회사에 제공하는 Financial Services Amendment 의 일부로서, Microsoft 는 감독기관의 요청이 있는 경우 감독기관이 현장 방문을 포함하여 관련 서비스를 조사하고 Microsoft 관계자 및 외부 감사인과 면담을 실시하며 관련 정보, 기록, 보고서, 서류에 접근할 수 있는 직접적인 권리를 부여함. 위수탁 계약에 의거하여, Microsoft 는 법률에 의해 요구되거나 고객의 지시나 동의가 있는 경우를 제외하고 감독기관에 고객 데이터를 공개하지 않을 것임을 약정함.	• 수탁회사에 대한 감독당국의 감독·검사 수용의무(금융회사의 정보처리 업무 위탁에 관한 규정 제4조 제3항)
6.	계약의 파기 또는 종료, 기타 위탁업무의 원활한 이행이 어려운 경우 해당 위탁업무의 이전 및 반환 등에 관한 사항	Microsoft 는 계약 만료 또는 해지 후 90 일 동안 기능이 제한된 계정으로 클라우드 서비스에 그대로 저장된 고객 데이터를 보존함. 준거법에 의해 허용 또는 요구되거나 DPA 에 따라 해당 데이터를 보존할 권한을 부여받는 경우가 아니면 그 후 90 일 이내에 고객의 계정을 비활성화하고 고객 데이터 및 개인 데이터를 삭제함(DPA, 9 면). Microsoft 의 Financial Services Amendment 에는 고객이 Microsoft Consulting Services 로부터 시장 요율로 출구 지원을 받을 수 있는 권리를 포함하여 업무 연속성 (business continuity) 및 출구 규정(exit provisions)이 명시되어 있음. 고객은 Microsoft 와 협조하여 그러한 업무 연속성 및 출구 계획을 수립해야 함. 하이브리드 솔루션을 제공하는 Microsoft 의 유연성은 클라우드에서 온프레미스 솔루션으로의 보다 원활한 전환을 뒷받침함.	• 신용정보의 사용.보관 기간 및 동 기간 경과 후 신용정보의 폐기·반납에 관한 사항(신용정보업감독규정 [별표4] 1. 마.)

7.	위탁 및 위탁업무 관련 준거법 준수의무 및 자율규제에 대한 협조	Microsoft 는 보안 위반 통지법 및 데이터보호요건(Data Protection Requirement)을 포함해 클라우드 서비스의 조항에 적용되는 모든 법률 및 규정을 따를 것임(DPA, 5 면).	
8.	비상대응훈련(재해복구 전환훈련 포함), 취약점 분석, 평가, 침해사고대응 훈련 등의 협조에 관한 사항	Microsoft 는 침해사고 대응 절차 관련하여 공식적이고 문서화된 절차를 수립하여 보급함(DPA, 부록 A – 보안책). 취약점 분석 및 평가에 대한 내용은 https://servicetrust.microsoft.com 의 "데이터 보호 리소스" 중 "Penetration Test Summary" 등의 리포트에서 확인할 수 있음.	
9.	위탁업무 모니터링 지원에 관한 사항	금융회사는 관리 대시보드를 통해 Microsoft 의 SLA 약정 준수에 관한 정보를 포함하여 클라우드 서비스의 이행을 모니터링할 수 있음. DPT 는 클라우드 서비스가 적절한 보안 및 컴플라이언스 기준을 준수하고 있는지 여부를 검증할 목적으로 Microsoft 가 시행하는 감사 및 모니터링 체제를 규정하고 있음. 엄정한 제 3 자 감사를 통해 Microsoft 의 클라우드 서비스가 이러한 엄격한 요건을 준수하고 있는지 여부를 검증함. 요청이 있는 경우 Microsoft 는 DPT 에 따른 보안 의무를 준수하고 있는지 여부를 검증할 목적으로 고객에게 일체의 Microsoft 감사보고서를 제공함. 또한, Microsoft 는 Microsoft 클라우드 전반에 걸쳐 탐지 및 보호 수준을 높일 목적으로 정기적인 침투 테스트를 실시함. Microsoft 는 고객에게 침투 테스트 및 사이버보안 현황에 관한 기타 감사 결과를 제공하며 고객 역시 서비스에 대한 자체 침투 테스트를 실시할 수 있음. 이는 Microsoft 의 ROE (rules of engagement)에 의거하여 행해지며 그러한 테스트에 대한 Microsoft 의 사전 허가를 요하지 않음. 침투 테스트에 관한 보다 자세한 사항은 https://technet.microsoft.com/en-us/mt784683.aspx 에서 확인할 수 있음.	• 수탁자에 대한 관리.감독에 관한 사항(신용정보업감독규정 [별표4] 3. 나.) • 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항(개인정보 보호법 시행령 제28조 제1항 제4호)

		Microsoft 는 고객이 클라우드 서비스에 대한 자체 가상 감사를 실시할 수 있도록 Service Trust Portal 을 통해 특정한 툴을 제공함. 또한, Microsoft 는 2 가지 주된 소스를 통해 금융 거래를 재구성하고 감사 증적을 작성할 수 있는 정보를 고객에게 제공함: Azure Active Directory 는 고객 거래 정보에 접근한 자와 그러한 정보에 대해 수행된 작업을 파악할 목적으로 검색이 가능한 감사 로그와 기타 정보가 보관된 저장소이며 Azure Monitor 는 고객이 고객 클라우드 정보의 변경에 관련된 '대상, 주체, 시기'를 파악하고 클라우드 서비스 운영에 관한 정보를 얻을 수 있는 활동 로그와 진단 로그를 각기 제공함. 그에 추가하여, Financial Services Amendment 는 고객과 감독기관에 부여하는 검사 및 감사 권리를 구체적으로 기술하고 있음. "감독기관 검사권"은 Microsoft 사업장에 대한 검사까지도 포함하는 절차를 규정하고 있음. 고객이 조사·감독·통제·감사 요건을 만족시킬 수 있도록 지원할 목적으로 Microsoft 는 고객에게 정보, Microsoft 관계자, Microsoft 외부 감사인에게 접근할 수 있는 구체적인 권리와 절차를 수립했음. Microsoft 는 고객에게 다음과 같은 권리를 부여함. 1. **클라우드 서비스 정보 방침** Microsoft 는 고객에게 관련 Online Service 에 대해 시행 중인 보안 통제 장치에 관한 설명 그리고 Microsoft 보안 방식 및 방침과 관련하여 고객이 합리적으로 요청하는 기타 정보와 더불어 정보 보안 방침을 제공함. 2. **클라우드 서비스에 대한 감사** Microsoft 는 고객을 대리하여 각각의 Online Service 에 대해 고객 데이터를 처리하는 과정에서 이용하는 컴퓨터, 컴퓨팅 환경, 물리적 데이터센터의 보안에 대한 감사가 실시되도록 조치함. DPA 의 조건에 의거하여, Microsoft 는 고객에게 일체의 Microsoft 감사보고서를 제공함. 3. **Financial Services Compliance Program**	

		또한, 고객에게 Microsoft 를 감사할 수 있는 능력을 지원하는 유료 프로그램인 Financial Services Compliance Program 에 참여할 수 있는 기회를 제공하며 여기에는 (a) 서비스에 대한 통제와 실효성을 평가하고 (b) 서비스 운영에 관련된 데이터를 평가하고 (c) 서비스의 운영상의 위험에 대한 분석을 수행하고 (d) Microsoft 가 서비스를 제공할 수 있는 능력에 중대한 영향을 미칠 가능성이 있는 변경 사항을 통보받고 (e) 서비스에서 개선이 필요한 부분에 대한 의견을 개진할 수 있는 능력이 포함됨. Microsoft 는 Financial Services Amendment 가 규제 대상 회사가 서비스 제공자로부터 조사 및 접근 권리를 확보할 것을 요구하는 운영기준 요건에 부합하는 것으로 판단하고 있음.	
10.	전송 정보에 대한 정보보호 의무 및 서비스 연속성 보장 등의 보안 요구사항	[전송 정보에 대한 정보보호 의무] Microsoft 는 내부 보안 정책 및 ISO 27001, ISO 27002, ISO 27018, SSAE 18 SOC 1 Type II, SSAE 18 SOC 2 Type II 에 따라 데이터를 보호함. 데이터 보안 정책 및 구체적인 보안 조치의 내용에 대해서는 DPA “데이터 보안” 및 “부록 A – 보안책”을 참조. [서비스 연속성 보장] SLA 는 클라우드 서비스에 대한 서비스 레벨 약정과 더불어 Microsoft 가 약정을 준수하지 않을 경우 고객에게 부여되는 서비스 크레딧 구제 조항을 규정하고 있음. 각 Online Service 의 업타임에 관한 정보는 Service Level Agreement for Microsoft Online Services 에서 확인할 수 있음.	• 데이터에 대한 접근통제(금융회사의 정보처리 업무 위탁에 관한 규정 제4조 제3항) • 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항(개인정보 보호법 시행령 제28조 제1항 제3호) • 금융회사 또는 전자금융업자의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서·계약서(입찰 공고 포함)에 인원·장비·자료 등에 대한 보안조치 사항과 정보유출 및

			부정당업자에 대한 손해배상 내용 등을 정확히 기술 (전자금융감독규정 시행세칙 제9조의2 제1항 [별표5-2]) • 신용정보 송수신시 정보유출 방지에 관한 사항(신용정보업감독규정 [별표4] 1. 라.) • 신용정보주체의 신용정보 보호 및 비밀유지에 관한 사항(신용정보업감독규정 [별표4] 3. 다.) • 개인정보의 기술적・관리적 보호조치에 관한 사항(개인정보 보호법 제26조 제1항 제2호)
11	재위탁 관련 클라우드 서비스 제공자의 관리감독 의무에 관한 사항	Microsoft 는 재위탁업체들이 Microsoft 가 의뢰한 서비스를 제공하려는 목적에 한하여 고객 데이터를 취득할 수 있으며 그 외의 다른 어떠한 목적으로도 고객 데이터를 이용하는 것이 금지된다는 점을 약정함. Microsoft 는 재위탁업체의 미준수 행위에 대해 Microsoft 의 행위와 동일한 책임을 부담함. 재위탁업체의 책임성을 보장할 목적으로, Microsoft 는 고객 개인 정보를 취급하는 모든 협력업체가 고객 개인 정보의 취급을 표준화하고 강화할 목적으로 도입된 Microsoft Supplier Security and Privacy Assurance Program 에 참가하는 동시에 협력업체의 업무 프로세스와 시스템이 Microsoft 의 업무 프로세스와 시스템을 준수할 것을 요구함.	• 신용정보 처리 재위탁의 제한에 관한 사항(신용정보업감독규정 [별표4] 3. 라.) • 재위탁 제한에 관한 사항(개인정보 보호법 시행령 제28조 제1항 제2호)

		Microsoft 의 Supplier Security and Privacy Program 에 관한 자세한 사항은 https://www.microsoft.com/en-us/procurement/msp-requirements.aspx 에서 확인할 수 있음. Microsoft 는 고객 데이터를 이전하는 모든 재위탁업체를 상대로 Microsoft 가 고객과 체결한 계약상의 데이터 처리 조항에 비해 정보보호수준이 떨어지지 않는 서면계약을 체결함(DPA, 9 면). 그에 추가하여, Microsoft 의 ISO/IEC 27018 인증은 Microsoft 가 재위탁업체들을 상대로 Microsoft 와 동일한 보안통제가 적용되도록 감독할 것을 요구하고 있음. Microsoft 의 ISO 27001 인증은 민감한 데이터의 취급, 신원 조회, 비밀유지계약 등 재위탁업체가 Microsoft 의 개인정보보호, 보안, 기타 고객 약정을 완벽하게 준수할 것을 요구하는 엄격한 요건이 적용되는 추가적인 통제 계층을 규정하고 있음. Microsoft 는 클라우드 서비스상의 고객 데이터에 대한 접근이 인가된 재위탁업체들과 이들이 제공하는 제한적인 혹은 부수적인 서비스가 열거된 웹사이트를 운영하고 있음. Microsoft 는 신규 재위탁업체에 고객 데이터 접근을 인가하기 최소한 6 개월 전에 해당 웹사이트를 업데이트하고 고객이 그러한 업데이트에 관한 통보를 받을 수 있는 방법을 제공해야 함. 고객이 신규 재위탁업체를 승인하지 않은 경우 해당 고객은 통보 기간이 종료되기 전에 승인 거부의 근거에 관한 설명이 포함될 수 있는 서면 해지 통지를 전달함으로써 관련 클라우드 서비스를 벌칙 없이 해지할 수 있음. 대상이 되는 클라우드 컴퓨팅 서비스가 스위트(suite) (혹은 그와 유사한 1 회성 서비스 구매)의 일부를 구성하는 경우 스위트 전체에 해지의 효력이 적용됨. Microsoft 는 해지 이후에는 해지된 클라우드 서비스에 대한 대금 결제 의무를 후속적인 고객 청구서상에서 배제함. (DPA, 9 면)	
12	재위탁 또는 재위탁 변경에 따른 보안 리스크 증가 등 서비스에 악영향을 미칠 수 있는	Microsoft 는 클라우드 서비스상의 고객 데이터에 대한 접근이 인가된 재위탁업체들과 이들이 제공하는 제한적인 혹은 부수적인 서비스가 열거된 웹사이트를 운영하고 있음. Microsoft 는 신규 재위탁업체에 고객 데이터 접근을 인가하기 최소한 6 개월 전에 해당 웹사이트를 업데이트하고 고객이 그러한 업데이트에 관한 통보를 받을 수 있는 방법을	• 신용정보 처리 재위탁의 제한에 관한 사항(신용정보업감독규정 [별표4] 3. 라.)

	경우 원위탁자의 계약해지 권한 보유에 관한 사항	제공해야 함. 고객이 신규 재위탁업체를 승인하지 않은 경우 해당 고객은 통보 기간이 종료되기 전에 승인 거부의 근거에 관한 설명이 포함될 수 있는 서면 해지 통지를 전달함으로써 관련 클라우드 서비스를 벌칙 없이 해지할 수 있음. 대상이 되는 클라우드 컴퓨팅 서비스가 스위트(혹은 그와 유사한 1 회성 서비스 구매)의 일부를 구성하는 경우 스위트 전체에 해지의 효력이 적용됨. Microsoft 는 해지 이후에는 해지된 클라우드 서비스에 대한 대금 결제 의무를 후속적인 고객 청구서상에서 제거함. (DPA, 9 면)	• 재위탁 제한에 관한 사항(개인정보 보호법 시행령 제28조 제1항 제2호)

II. I 에 포함된 항목을 제외한 위수탁 계약서 주요 기재사항

1. 금융회사의 정보처리 업무 위탁에 관한 규정 제4조 제3항

	위수탁 계약서 주요 기재사항	Microsoft 계약에서 관련 사항을 다루고 있는 부분 및 방식
1	보안사고 등에 따른 이용자 피해에 대한 위·수탁회사간의 책임관계	MBSA 에는 책임에 관한 사항을 다루는 조항이 포함되어 있음. MBSA 는 Microsoft 가 제 3 자 권리 침해 청구로부터 규제대상 회사(regulated entity)를 방어할 의무를 규정하고 있음.
2	수탁회사의 분쟁해결 과정에서의 재판관할	금융회사와 Microsoft 간에 분쟁이 발생한 경우 준거법 선택 및 분쟁 해결 조항은 Microsoft 와 금융회사 간의 계약에 명확하게 규정됨. MBSA 에는 관할지역을 포함하여 계약에 따라 분쟁을 처리하는 방식을 기술한 규정이 포함되어 있음.

2. 전자금융감독규정 제60조 제1항 제7호 및 동 규정 시행세칙 제9조의2 제1항 [별표5-2]

	위수탁 계약서 주요 기재사항	Microsoft 계약에서 관련 사항을 다루고 있는 부분 및 방식
1	용역사업에 투입되는 자료·장비 등에 대해 대외보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서 작성 * 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시	고객의 요청이 있는 경우 별도의 비밀유지계약서를 작성할 수 있음.
2	용역사업 참여인원은 금융회사 또는 전자금융업자의 사전 동의 없이 용역업체가 임의로 교체할 수 없도록 명시	DPA 는 고객의 구체적인 혹은 일반적인 사전 서면 동의 없이 다른 업체에 용역을 의뢰할 수 없다고 규정하고 있음.
3	금융회사 또는 전자금융업자의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서·계약서(입찰 공고 포함)에 인원·장비·자료 등에 대한 보안조치 사항과 정보유출 및 부정당업자에 대한 손해배상 내용 등을 정확히 기술	표 I. 10. 항목, II. 1. 1. 항목 참조

3. 신용정보업감독규정 [별표4] 신용정보제공계약에 포함될 신용정보 보안관리 대책(제21조 관련), 신용정보의 이용 및 보호에 관한 법률 제17조 제5항 및 동법 시행령 제14조 제5항

	위수탁 계약서 주요 기재사항	Microsoft 계약에서 관련 사항을 다루고 있는 부분 및 방식
1	1. 다. 제공된 신용정보의 이용자 제한 및 전담 관리자 지정에 관한 사항	DPA 에는 시설에 대한 물리적 접근과 접근 인가를 포함하는 보안 조치가 규정되어 있음.
3	3. 사. 위 사항을 위반한 경우의 책임소재 및 제재에 관한 사항	표 II. 1. 1. 항목 참조
※신용정보의 이용 및 보호에 관한 법률 제 17 조 제 5 항 및 동법 시행령 제 14 조 제 5 항		
	연 1 회 이상 수탁자의 소속 임직원에 대한 교육 실시	Microsoft 는 보안 교육을 통해 임직원을 대상으로 관련 보안 절차 및 각자의 역할을 교육함. 또한, Microsoft 는 임직원을 대상으로 보안 수칙 및 절차 위반에 따른 결과를 교육함. (DPA, 부록 A – 보안책)

4. 개인정보 보호법 제26조 제1항 및 동법 시행령 제28조 제1항

	위수탁 계약서 주요 기재사항	Microsoft 계약에서 관련 사항을 다루고 있는 부분 및 방식
1	법 제 26 조 제 2 항에 따른 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항	표 II. 1. 항목 참조

추가 정보

- **Korea Regulatory Compliance for Financial Services Customers: https://www.microsoft.com/en-sg/apac/trustedcloud/korea-financial-service.aspx**
- **Asia Regulatory Compliance for Financial Services Customers: aka.ms/asiafs**
- **Trust Center: microsoft.com/trust**
- **Service Trust Portal: aka.ms/trustportal**
- **Customer Stories: customers.microsoft.com**
- **Online Service Terms: microsoft.com/contracts**
- **Service Level Agreements: microsoft.com/contracts**
- **SAFE Handbook: aka.ms/safehandbook**

© Microsoft Corporation 2019. 본 문건은 법률적 혹은 규제적 조언에 해당하지 않으며 Microsoft 에 의한 보증이나 계약상의 약정을 구성하지 않습니다. 귀사의 클라우드 서비스 프로젝트와 법률적·규제적 의무에 관해서는 외부의 법률적 자문을 구해야 합니다.