



Tencent Cloud 한국 금융 산업 규제 요구사항 준수 가이드

2026 년 4 월

【저작권 고지】

©2013-2026 Tencent Cloud 저작권 소유

본 문서의 저작권은 Tencent Cloud 에 단독으로 귀속됩니다. Tencent Cloud 의 사전 서면 허가 없이 어떠한 주체도 본 문서 내용의 전부 또는 일부를 어떠한 형식으로도 복제, 수정, 표절, 배포할 수 없습니다.

【상표 고지】



및 기타 Tencent Cloud 서비스와 관련된 모든 상표는 Tencent Cloud Computing (Beijing) Co., Ltd. 및 그 계열사에 귀속됩니다. 본 문서에 언급된 제 3 자의 상표는 해당 권리자에 의해 법적으로 소유됩니다.

【서비스 고지】

본 문서는 참고용으로만 제공됩니다. 본 문서의 정보에 대해서 Tencent Cloud 는 명시적 또는 묵시적인 보증을 하지 않습니다. 본 문서는 현 상태를 기반으로 작성되었습니다. 본 문서의 정보와 의견(URL 및 기타 인터넷 웹사이트 참조 포함)은 사전 통지 없이 변경될 수 있습니다. 귀하는 이를 사용함에 따른 모든 위험을 부담합니다.

본 파일은 귀하에게 Tencent 제품의 지식재산권에 관한 어떠한 법적 권리도 부여하지 않습니다. 본 문서 내용은 귀하 내부 참고용으로만 복제 및 사용할 수 있습니다.

본 문서에 기술된 일부 예시는 설명 목적으로만 제공되며 허구입니다. 이를 기반으로 어떠한 사실상의 관련성이나 연관성을 추론하거나 예상해서는 안 됩니다.

STANDARDS CONTENTS

01	개요	
02	Tencent Cloud 보안 및 프라이버시 컴플라이언스	
2.1	국제 권위 인증	4
2.2	ISO/IEC 체계 인증	5
2.3	지역 및 업계 인증	7
03	Tencent Cloud 보안 책임 공유 모델	
04	Tencent Cloud 글로벌 인프라	
05	Tencent Cloud 「전자금융거래법」을 어떻게 준수하고 고객이 이를 충족하도록 지원하는가	
06	Tencent Cloud 「전자금융감독규정」을 어떻게 준수하고 고객이 이를 충족하도록 지원하는가	
6.1	전자금융거래의 안전성 확보 및 이용자 보호	30
6.1.1	인력, 조직 및 예산 부문	30
6.1.2	시설부문	32
6.1.3	정보기술부문	35
6.1.4	정보보호부문	48
6.1.5	업무지속성 부문	59
6.1.6	취약점 분석 및 사고 대응 등	66
6.2	허가 및 등록의 세부요건	70
6.3	전자금융업무의 감독	75
6.4	클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가기준	79
6.4.1	정보보호 정책 및 법규 준수	79
6.4.2	인적보안	82
6.4.3	위험평가 및 관리	84
6.4.4	서비스 공급망 관리	86
6.4.5	업무연속성 계획 및 재해복구	87
6.4.6	침해사고 대응 및 관리	93
6.4.7	사용자 인증 및 접근통제	96

CONTENTS

6.4.8 가상화 및 인프라 보안	100
6.4.9 개발 및 운영 보안	108
6.4.10 암호화 및 데이터 보호	109
6.4.11 물리적 보안	115
6.5 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획	118
6.6 클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치	128
6.7 클라우드컴퓨팅서비스 위수탁 계약서 주요 기재사항	145
07 Tencent Cloud 「금융회사 업무 위탁 규정」 을 어떻게 준수하고 고객이 이를 충족하도록 지원하는가	
08 Tencent Cloud 「금융회사의 정보처리 업무 위탁에 관한 규정」을 어떻게 준수하고 고객이 이를 충족하도록 지원하는가	
09 결론	
10 버전 히스토리	

01 개요

한국 금융위원회(Financial Services Commission, FSC)는 국무총리 산하 중앙행정기관으로, 한국의 금융 법규를 기초 및 개정하고 금융회사에 대한 감독 허가를 부여할 법적 권한을 보유하여, 금융 산업 발전 촉진, 금융 시장 안정 유지, 공정 시장 관행 이행 및 금융 소비자 보호에 전념하고 있습니다. 한국 금융감독원(Financial Supervisory Service, FSS)은 FSC의 집행 기관으로, FSC의 지시에 따라 금융 정책의 이행을 추진하고 금융회사에 대한 현장 점검 및 비현장 모니터링을 담당합니다.

금융업무의 디지털 전환 가속화와 함께, 한국 금융회사의 클라우드 컴퓨팅, 빅데이터, 인공지능 등 디지털 신기술에 대한 수요가 지속적으로 증가하고 있습니다. 금융 디지털화 발전 수요에 부응하고, 새로운 위험과 문제에 대응하며, 한국 금융 분야의 안전과 안정을 보장하기 위해, 한국 금융위원회는 전자금융거래, 아웃소싱, 정보처리 등 다양한 측면을 포괄하는 일련의 법률 및 규정을 제정하여, "금융회사"¹ 및 "전자금융 서비스 제공자" 등이 클라우드 서비스를 안전하고 합리적으로 사용하도록 요구사항과 지침을 제시했습니다.

Tencent Cloud는 한국 금융위원회의 최신 감독 요구사항을 면밀히 주시하며, 한국 금융 기관 고객이 감독 요구사항을 충족하도록 지원하기 위해 노력하고 있습니다. 본 문서는 다음 네 가지 감독 법률 규정을 대상으로, Tencent Cloud가 어떻게 고객이 감독 요구사항을 준수하도록 지원하는지 설명합니다:

- [「전자금융거래법」](#)
- [「전자금융감독규정」](#)
- [「금융기관의 업무위탁 등에 관한 규정」](#)
- [「금융회사의 정보처리 업무 위탁에 관한 규정」](#)

¹ "금융회사"란 다음 각 목의 어느 하나에 해당하는 기관이나 단체 또는 사업자를 말한다.

가. 「금융위원회의 설치 등에 관한 법률」 제 38 조제 1 호부터 제 5 호까지, 제 7 호 및 제 8 호에 해당하는 기관

나. 「여신전문금융업법」에 따른 여신전문금융회사

다. 「우체국예금·보험에 관한 법률」에 따른 체신관서

라. 「새마을금고법」에 따른 새마을금고 및 새마을금고중앙회

마. 그 밖에 법률의 규정에 따라 금융업 및 금융 관련 업무를 행하는 기관이나 단체 또는 사업자로서 대통령령이 정하는 자

02

Tencent Cloud

보안 및

프라이버시

컴플라이언스

규정 준수는 Tencent Cloud 발전의 기초입니다. Tencent Cloud 는 선진적인 국제 및 업계 보안 표준을 식별 및 채택하고, 다양한 국가/지역 및 업계의 규정 준수 요구사항을 준수하며, 내부 관리 체계를 지속적으로 개선하고 Tencent Cloud 의 보안 통제 수준을 향상시켜 고객이 신뢰할 수 있는 클라우드 서비스를 제공하기 위해 노력하고 있습니다. 동시에 Tencent Cloud 는 업계 보안 표준의 제정 및 확산에 적극적으로 참여하고, "규정 준수即서비스"를 고수하며 안전하고 신뢰할 수 있는 클라우드 생태 환경을 구축 및 운영하고 있습니다.

현재까지 Tencent Cloud 는 제 3 자 독립 감사 또는 평가 방식을 통해 다수의 보안 및 개인정보 보호 규정 준수 인증 또는 자격을 취득하여, Tencent Cloud 의 보안 관리 및 개인정보 보호 구축이 관련 인증 기준 또는 업계 모범 사례를 충족함을 입증했습니다. Tencent Cloud 의 규정 준수 정보에 대해 더 자세히 알아보려면 [Tencent Cloud Compliance](#) 페이지를 참조하십시오. 관련 규정 준수 인증서나 보고서가 필요한 경우, [Compliance Document Center](#) 를 통해 신청하여 다운로드하십시오.

Tencent Cloud 의 일부 국제 권위 인증, 지역 및 업계 인증 예시는 다음과 같습니다:

2.1 국제 권위 인증

CSA STAR 클라우드 보안 인증 STAR 클라우드 보안 평가는 국제적으로 권위 있는 비영리 기관인 클라우드 보안 연합(Cloud Security Alliance)이 제정한, 클라우드 보안 특성에 대한 국제적 인증입니다. 이는 ISO/IEC 27001 정보 보안 관리 체계를 확장하고, 클라우드 제어 매트릭스(Cloud Control Matrix, CCM)와 결합하여 클라우드 보안의 특수 문제를 시각화함으로써, 사용자에게 직관적인 보안 아키텍처 평가 개요를 제공합니다.

Tencent 회사의 다년간 축적된 보안 실무를 기반으로, Tencent Cloud 는 CSA STAR 글로벌 골드 클라우드 보안 인증을 획득하여 Tencent Cloud 의 보안 통제 체계가 국제적 권위의 클라우드 보안 표준을 충족함을 입증했습니다.

SOC 감사 시스템 및 조직 통제 보고서(SOC 보고서)는 전문 제 3 자 회계법인에 의해 미국 공인회계사회(AICPA)의 관련 기준에 따라 발행되는 서비스 기관 내부 통제 관련 일련의 보고서입니다. SOC 보고서는 독립적인 감사 보고서로서 Tencent Cloud 플랫폼의 보안성, 가용성 및 기밀성 관련 통제 항목을 다룹니다.

다양한 보증 서비스 유형에 따라 SOC 보고서는 클라우드 사용자와 그 감사인에게 제공될 수 있으며, Tencent Cloud 사용자에게 서비스 기관 관련 위험을 평가하고 해결하기 위한 가치 있는 정보를 제공합니다.

2.2 ISO/IEC 체계 인증

ISO/IEC 22301: 2019 인증
ISO/IEC 22301: 2019 는 업무 연속성 관리(Business Continuity Management, 약칭 BCM)를 주제로 하는 국제 표준으로, 완전하고 보편적인 BCM 방법론을 제공하여 기업이 잠재적인 중단 사건을 식별하고 대응하며, 핵심 운영의 연속성을 보장하여 위험을 줄이고 조직이 중대한 영향을 받지 않도록 하는 것을 목표로 합니다.

Tencent Cloud 는 ISO/IEC 22301: 2019 인증을 획득하여, Tencent Cloud 가 공식적인 업무 연속성 관리 프로세스를 구축하여 자체 업무의 연속성과 안정성을 보장하고 있음을 입증했습니다.

ISO/IEC 27001: 2022 인증
ISO/IEC 27001: 2022 정보 보안 관리 체계는 국제적으로 정보 보안 분야에서 가장 권위 있고 엄격하며, 가장 광범위하게 수용 및 적용되는 체계 인증 기준입니다. 이 인증을 획득한다는 것은 기업이 과학적으로 효과적인 정보 보안 관리 체계를 구축하여 기업 발전 전략과 정보 보안 관리를 조화시키고, 해당 정보 보안 위험이 적절하게 통제되고 올바르게 대응되도록 보장함을 의미합니다.

ISO 27001: 2022 인증을 통해 Tencent Cloud 의 보안에 대한 약속을 더 잘 입증할 수 있으며, Tencent Cloud 가 과학적으로 효과적인 관리 체계를 구축하여 사용자에게 안전하고 신뢰할 수 있는 클라우드 제품 및 서비스를 제공할 수 있음을 나타냅니다.

ISO/IEC 20000-1: 2018 인증
ISO/IEC 20000-1: 2018 는 IT 서비스 관리를 위해 제정된 국제 표준입니다. 이 체계는 기업의 정보 기술 서비스 관리를 규정하며, 구축, 시행, 운영, 모니터링, 검토, 유지 및 개선 모델을 통해 기업이 관련 정보 기술 문제를 지속적으로 식별 및 관리하고, 사용자와의 의사 소통을 강화하며, 자체적으로 개선되는 표준화된 서비스 체계를 구축하도록 돕습니다.

Tencent Cloud 는 ISO/IEC 20000-1: 2018 인증을 획득하였으며, 클라우드 컴퓨팅 서비스, 관리형 서비스 및 재해 복구 서비스 등에 대한 인증 범위를 포함합니다. Tencent Cloud 는 서비스를 최우선으로

하는 태도로 고객과의 정보 기술 서비스 및 의사 소통 메커니즘을 완비하고 있습니다.

ISO/IEC 9001: 2015 인증
ISO/IEC 9001: 2015 는 국제적으로 널리 인정받고 성숙된 품질 관리 체계입니다. 이 체계는 기업 제품 또는 서비스 제공 전 과정의 품질 관리 프레임워크와 지침적 규정을 중심으로 하며, 기업이 제품 또는 서비스를 유지하고, 제공되는 품질이 안정적이고 일관되도록 보장하기 위해 사용됩니다.

Tencent Cloud 는 ISO/IEC 9001 인증을 획득하여 범위에 클라우드 컴퓨팅 서비스, 관리형 서비스 및 재해 복구 서비스 등을 포함합니다. Tencent Cloud 는 품질 관리 체계를 사용하여 효과적이고 효율적으로 예상된 품질 목표를 달성하며, 클라우드 제품과 서비스의 품질 및 운영을 보장합니다.

ISO/IEC 27017: 2015 인증
ISO/IEC 27017: 2015 는 ISO/IEC 27002: 2013 의 보완으로, 클라우드 서비스 정보 보안의 실용적 표준이며, 클라우드 서비스 제공자와 고객에게 특정 보안 통제 및 그 이행 지침을 제공하여 클라우드 컴퓨팅 취약점의 위협과 위험에 대한 통제를 강화합니다.

Tencent Cloud 는 ISO/IEC 27017: 2015 인증을 획득하여, Tencent Cloud 가 국제적으로 인정받는 최적의 실무를 항상 채용할 뿐만 아니라, 더 포괄적인 클라우드 보안 관리 체계를 구축하여 전체적인 클라우드 보안 서비스 역량을 향상시켰음을 증명합니다.

ISO/IEC 27018: 2014 인증
ISO/IEC 27018: 2014 는 개인 식별 정보(PII)가 공공 클라우드 환경에서 처리될 때의 전 세계적으로 가장 포괄적인 보안 표준입니다. 이 표준은 클라우드 서비스 제공자에게 사용자 개인정보 보호를 위한 실무 지침을 제공하여, 클라우드 컴퓨팅 환경에서 개인 데이터의 안전을 보장하는 것을 목표로 합니다.

Tencent Cloud 가 ISO/IEC 27018: 2014 인증을 획득한 것은, Tencent Cloud 의 개인정보 관리 체계가 국제적으로 엄격한 개인정보 보호 법률 규정을 준수함을 의미하며, Tencent Cloud 고객에게 클라우드 보안에 대한 더 많은 신뢰와 보장을 제공합니다.

ISO/IEC 29151: 2017 인증
ISO/IEC 29151 는 개인 식별 정보(PII) 처리와 관련된 통제 조치를 이행하기 위한 국제 표준으로, PII 보호와 관련된 위험 및 프라이버시 영향 평가로 결정된 요구사항을 충족시키기 위한 것입니다.

Tencent Cloud 는 ISO/IEC 29151: 2017 인증을 획득하여, Tencent Cloud 가 자사의 PII 목표와 비즈니스 요구에 기반하여 적절한 보안

통제 체계를 개발하였으며, 클라우드 상의 사용자 PII 에 대해 높은 수준의 프라이버시 보호 통제를 제공함을 나타냅니다.

ISO/IEC 27701: 2019 는 ISO/IEC 27001 및 ISO/IEC 27002 의 프라이버시 정보 관리에 대한 확장 요구사항과 지침으로, 프라이버시 정보 관리 체계의 수립, 이행, 유지 및 지속적 개선을 위한 지침을 제공하며, 프라이버시 위험을 지속적으로 관리하는 이정표입니다.

Tencent Cloud 가 ISO/IEC 27701: 2019 인증을 획득한 것은, Tencent Cloud 가 항상 사용자 개인정보 보호를 서비스의 핵심으로 삼고 있음을 증명하며, Tencent Cloud 제품의 개인정보 보호가 표준화되고 신뢰할 수 있음을 충분히 보여줍니다.

2.3 지역 및 업계 인증

독일 C5 클라우드 컴퓨팅 규정 준수 기준 카탈로그(Cloud Computing Compliance Criteria Catalogue, 약칭 C5)는 독일 연방 정보보호청(BSI)이 제정한 것으로, 표준화된 점검 및 보고를 통해 클라우드 서비스 제공자의 정보 보안 규정 준수성을 검증하는 것을 목표로 합니다. C5 는 클라우드 서비스 분야에서 업계가 크게 인정하는 높은 수준의 보안 표준입니다.

Tencent Cloud 는 독일 C5:2020 기본 및 추가 심사 기준을 통과하여, Tencent Cloud 가 데이터 보호 및 정보 보안 측면에서 독일 정부가 설정한 높은 기준에 도달했음을 의미합니다.

독일 TISAX TISAX 는 독일 자동차 산업 협회(VDA)와 유럽 자동차 산업 보안 데이터 교환 협회(ENX)가 공동으로 제정한 자동차 업계 정보 보안 평가 및 데이터 교환 보안 표준입니다. TISAX 는 자동차 업계 내 정보 보안 평가의 상호 인정을 가능하게 하며, 공통의 평가 및 교류 메커니즘을 제공합니다.

현재 Tencent Cloud 의 다수의 인터넷 데이터센터(IDC)(베이징, 선전 등지에 위치한)가 TISAX 3 단계 평가 심사를 통과했으며, 이는 해당 지역에 배포된 서비스가 모두 TISAX 요구사항을 충족하고 완벽한 정보 보안 관리 체계를 구축 및 유지하고 있음을 의미합니다.

싱가포르 MTCS T3 싱가포르 다계층 클라우드 보안(MTCS) 표준은 싱가포르 정보통신개발청(IDA) 정보기술 표준 위원회(ITSC)의 지도 하에 수립되었습니다. MTCS 는 클라우드의 공통 표준으로, 클라우드 서비스

제공자는 이 표준을 채택하여 고객의 클라우드 데이터 보안성과 기밀성, 그리고 클라우드 서비스 사용이 비즈니스에 미치는 영향에 대한 우려를 해결할 수 있습니다.

Tencent Cloud 는 싱가포르 다계층 클라우드 보안(MTCS) T3 수준 표준 인증을 성공적으로 획득했습니다. 이 인증은 Tencent Cloud 가 건전한 위험 관리 메커니즘과 안전한 클라우드 서비스를 구축하여 클라우드 고객 데이터의 보안성, 기밀성 및 검증 가능한 운영 투명성을 보장함을 의미합니다.

싱가포르 OSAPR 외주 서비스 제공자 감사 보고서(OSPAR)는 싱가포르 금융 업계 외주 서비스의 진입 기준입니다. 이 표준은 싱가포르 SSAE 3000 을 기반으로 하며, 싱가포르 금융 기관의 서비스 제공자에 대해 실제 수준 통제, 일반 정보기술 통제 및 서비스 통제 세 분야의 관련 통제 설계와 운영 유효성을 검증하는 것을 목표로 합니다.

Tencent Cloud 의 여러 제품과 서비스는 싱가포르 OSAPR 감사를 통과했으며, 그 통제가 ABS 지침을 준수하도록 지속적으로 노력하고 있습니다. 이 감사를 통과한 것은 Tencent Cloud 의 보안 역량이 싱가포르 및 동남아시아의 금융 서비스에 대한 엄격한 요구사항을 충족함을 나타냅니다.

DPTM 싱가포르 데이터 보호 신뢰 마크(DPTM)는 싱가포르 개인정보 보호 위원회(PDPC)와 정보통신미디어개발청(IMDA)가 제정하여, 조직이 책임 있는 데이터 보호 관행을 입증하도록 하는 것을 목표로 합니다.

싱가포르 데이터 보호 신뢰 마크 Tencent Cloud 는 싱가포르 데이터 보호 신뢰 마크(DPTM) 인증을 획득하여, Tencent Cloud 가 고객, 비즈니스 파트너 및 규제 기관에 대해 책임 있는 데이터 보호 관행을 채택하고, 수집한 개인 데이터를 보호할 역량이 있음을 나타냅니다.

싱가포르 사이버 트러스트 마크 사이버 트러스트 마크(CTM)는 싱가포르 사이버 보안청(CSA)에서 시행하는 국가 수준 사이버 보안 인증입니다. CTM 프레임워크는 위험 기반 방법론을 채택하며, 거버넌스 및 위험 관리, 사이버 보안 운영, 복원력, 공급망 및 인력 보안, 그리고 지속적인 개선 및 우수 사례라는 4 대 핵심 분야의 22 개 세부 분야에 대한 평가를 포괄합니다.

텐센트 클라우드는 싱가포르 사이버 보안청으로부터 최고 등급(티어 5) 사이버 트러스트 마크를 획득했습니다. 본 인증은 텐센트 클라우드의 사이버 보안 거버넌스, 위험 관리 및 운영 복원력 분야의 우수한 역량을 입증하며, 아시아 태평양 지역 규제 대상 산업 및

고수요 산업에서 신뢰할 수 있는 클라우드 서비스 제공업체로 자리매김하게 합니다.

한국 K-ISMS 인증 한국 정보보호 관리체계(K-ISMS) 인증은 한국 정부가 지원하는 정보 보안 인증으로, 한국 기업 및 조직이 해당하는 한국 정보통신기술 법률에 따라 일관되게 정보 자산을 안전하게 보호하도록 돕는 것을 목표로 합니다.

Tencent Cloud 가 K-ISMS 인증을 획득했다는 것은, 한국의 클라우드 고객이 현지 법적 요구사항을 더 쉽게 준수하고 있음을 증명하여 핵심 디지털 정보 자산을 보호할 수 있다는 의미이며, 또한 Tencent Cloud 의 정보 보안 대응 조치 및 위협 대응 절차 역량이 더욱 향상되어 보안 취약점의 영향을 보다 효과적으로 줄일 수 있음을 의미합니다.

말레이시아 금융 업계 IT 규정 준수 감사 말레이시아 국가 은행(BNM), 말레이시아 증권 위원회(SC) 등 말레이시아 금융 규제 기관은, 말레이시아 은행, 보험, 증권 등 금융 서비스에서 정보 기술의 적용을 규제하고 금융 정보 시스템의 신뢰성, 안전성, 안정성을 보장하기 위해 금융 서비스 업계에 대한 관련 법규를 반포했습니다.

Tencent Cloud 는 독립된 제 3 자 감사를 통해, 말레이시아 금융 업계 고객에게 제공하는 클라우드 서비스가 말레이시아 금융 업계의 규제 요구사항을 엄격히 준수함을 입증할 수 있습니다.

홍콩 금융 업계 IT 규정 준수 감사 홍콩 특별행정구 금융관리국(HKMA), 증권선물사무감독위원회(SFC) 및 보험업감독국(HKIA)은 금융, 보험 및 증권 기관의 정보 기술 적용을 규제하기 위해 다수의 핵심 감독 요구사항을 발표했습니다.

Tencent Cloud 는 독립된 제 3 자 감사를 통해, Tencent Cloud 가 금융 업계에서 신뢰할 수 있는 클라우드 서비스 제공자이며, Tencent Cloud 가 가장 엄격한 규정 준수 의무를 이행하기 위해 적극적이고 선제적인 접근 방식을 취하고 있어 금융 기관이 Tencent Cloud 를 기반으로 차세대 금융 서비스를 안심하고 구축할 수 있음을 입증합니다.

태국 금융 업계 IT 규정 준수 감사 태국 금융 업계 기관은 태국 중앙 은행(BoT), 증권거래위원회 사무국(OSEC), 보험위원회 사무국(OIC) 등 금융 규제 및 관련 법정 기관이 반포한 관련 법규를 준수해야 하며, 그 규제 요구사항은 정보 기술 활용의 위험 관리, 개인정보 보호, 정보 기술이 은행, 보험, 전자

정부 시스템, 전자 화폐, 결제 시스템 인프라, 결제 서비스 제공자 등에서의 적용 및 보안 통제 등을 포함합니다.

Tencent Cloud는 독립된 제3자 감사를 통해, Tencent Cloud가 태국의 엄격한 금융 업계 규제 요구사항을 준수하는 역량과, 태국 금융 업계 고객에게 고품질의 규정을 준수하는 클라우드 서비스를 제공하기 위한 Tencent Cloud의 헌신을 입증할 수 있습니다.

인도네시아 금융 업계 IT 규정 준수 감사 인도네시아 중앙은행(Bank Indonesia), 금융 서비스 감독청(Otoritas Jasa Keuangan, OJK) 등 인도네시아 금융 규제 기관은 금융 서비스 업계에 대한 관련 법규를 반포했으며, 그 규제 요구사항은 정보 기술 활용의 위험 관리, 개인정보 보호, 정보 기술이 은행, 보험, 전자 정부 시스템, 전자 화폐, 결제 시스템 인프라, 결제 서비스 제공자 등에서의 적용 및 보안 통제 등을 포함합니다.

Tencent Cloud는 독립된 제3자 감사 기관에 의해 수행된 인도네시아 금융 규정 준수 감사를 통과하여, Tencent Cloud가 인도네시아에서 금융 고객에게 제공하는 클라우드 서비스가 인도네시아 금융 업계의 규제 요구사항을 엄격히 준수함을 입증합니다.

필리핀 금융 업계 IT 규정 준수 감사 필리핀 금융 업계 기관은 필리핀 중앙은행(BSP) 등 금융 규제 및 관련 법정 기관이 제정한 관련 법규를 준수해야 하며, 그 규제 요구사항은 정보 기술 활용의 위험 관리, 개인정보 보호, 정보 기술이 은행, 보험, 전자 정부 시스템, 전자 화폐, 결제 시스템 인프라, 결제 서비스 제공자 등에서의 적용 및 보안 통제 등을 포함합니다.

Tencent Cloud는 독립된 제3자 감사를 통해, Tencent Cloud가 필리핀의 엄격한 금융 업계 규제 요구사항을 준수하는 역량과, 금융 업계 고객에게 고품질의 규정을 준수하는 클라우드 서비스를 제공하기 위한 Tencent Cloud의 헌신을 입증할 수 있습니다.

미국 영화 협회 MPAA 미국 영화 협회(MPAA)는 보호된 미디어 콘텐츠의 안전한 저장, 처리 및 전송을 위한 일련의 모범 사례 기준을 수립했습니다. 본 이행 지침은 MPAA 협회 회원과 협력 관계를 유지하는 애플리케이션 및 클라우드 서비스 제공업체가 콘텐츠 보안 측면에서 따라야 할 요구사항을 이해하도록 하는 것을 목표로 합니다. MPAA 콘텐츠 보안 템플릿의 구성 요소는 관련 ISO 표준(27001-27002), 보안 표준(예: NIST, CSA, ISACA 및 SANS) 및 업계 모범 사례를 참조합니다.

Tencent Cloud는 ISO 27001, ISO 27017, ISO 27018, PCI DSS 및 CSA STAR 등의 관련 인증을 이미 획득했습니다. 또한 Tencent Cloud는

자체 평가 방식을 통해 고객 콘텐츠 관리 절차가 미국 영화 협회(MPAA) 콘텐츠 보안 모델 지침을 준수하도록 보장했습니다.

미국 HIPAA 미국 HIPAA 법의 목적 중 하나는 전자 건강 기록의 사용을 촉진하여 정보 공유를 강화함으로써 의료 시스템의 효율성과 질을 향상시키는 것입니다. HIPAA 는 기관 및 그 비즈니스 파트너가 생성, 수신, 유지 및 전송 등의 과정에서 보호된 건강 정보(Protected Health Information, PHI)의 안전성(가용성, 무결성 및 기밀성 포함)과 개인정보를 보호 및 보장하는 것에 중점을 둡니다. HIPAA 의 규제를 받는 기관 및 그 비즈니스 파트너는 PHI 를 처리, 유지 및 저장하는 등의 상황에서 상응하는 보안 조치를 제공해야 합니다.

Tencent Cloud 는 자체 평가 방식을 통해, Tencent Cloud 의 사용자 개인정보 보호 역량 및 통제 조치의 유효성이 HIPAA 의 규정 준수 요구사항을 준수하도록 보장합니다.

미국 SEC Rule 17a-4 Tencent Cloud 객체 저장 서비스(COS)는 미국 증권거래위원회(SEC), 금융업 규제국(FINRA) 및 상품선물거래위원회(CFTC)의 기술적 요구사항에 따라, 기록 관리 및 정보 거버넌스에 전문적인 독립 제 3 자 평가 회사에 의해 인증되었습니다.

해당 인증은 높은 수준의 규제 환경(예: 금융 서비스 업계)에서 운영되는 고객에게 Tencent Cloud 객체 저장 서비스(COS)의 재기록 불가능, 삭제 불가능한 보존 방법과 객체 잠금 기능을 보장하여, Tencent Cloud 가 고객에게 안전하고 업계 표준에 부합하는 클라우드 제품을 제공하기 위한 약속을 보여줍니다.

일본 FISC 금융 기관의 보안성을 향상시키기 위해, FISC 은행 및 관련 금융 기관 컴퓨터 시스템 보안 가이드라인은 일본 은행과 금융 기관이 안전한 정보 시스템을 구축하고 정보 시스템의 운영을 보장하는 데 효과적인 지침을 제공합니다.

Tencent Cloud 는 독립된 서비스 감사관에 의해 감사를 받고, 이를 바탕으로 해당 시스템 및 기관 통제(SOC) 보고서를 작성하여, Tencent Cloud 플랫폼의 보안성, 가용성 및 기밀성 관련 통제 항목을 다루어, Tencent Cloud 의 관련 조치가 FISC 은행 및 관련 금융 기관 컴퓨터 시스템 보안 가이드라인의 요구사항을 충족함을 입증합니다.

영국 BS10012: 2017 BS10012: 2017 는 영국 표준 협회가 발표한 것으로, 조직에 개인정보 보호 규정 준수 프레임워크와 모범 사례를 제공하여 기업이 개인정보 관리 체계(PIMS)를 수립 및 유지하고, 조직이 개인정보를 보호하기

위한 충분하고 적절한 통제 조치를 보유하도록 안내하는 것을 목표로 합니다. 이 체계는 일반 개인정보 보호법(GDPR)에 부합하도록 업데이트 및 개정되었습니다.

Tencent Cloud 는 BS10012: 2017 인증을 획득하여, Tencent Cloud 의 개인정보 관리 체계가 국제 표준 및 업계 모범 사례의 요구사항을 충족함을 나타내며, 고객이 GDPR 의 개인정보 보호 요구사항을 더 잘 준수할 수 있도록 합니다.

**유럽연합
CISPE** CISPE 행동 강령은 유럽연합 일반 개인정보 보호법(GDPR) 제 40 조에 따라 클라우드 인프라 서비스 제공자를 위한 범유럽 업계별 지침으로, 유럽 전역의 조직이 소비자, 기업 및 기관을 위한 GDPR 을 준수하는 클라우드 기반 서비스 개발을 가속화하도록 돕습니다.

Tencent Cloud 는 CISPE 행동 강령 "후보" 마크를 부여받았으며, 이는 Tencent Cloud 가 CISPE 행동 강령 요구사항에 따라 자체 평가를 완료하여 Tencent Cloud 의 문서 체계 및 이행 수준의 규정 준수성을 입증하는 데 사용됨을 의미합니다.

**NIST CSF
인증** NIST CSF 는 비즈니스 동인을 사용하여 사이버 보안 활동을 안내하고, 사이버 보안 위험을 조직 위험 관리 프로세스의 일부로 간주하는 데 중점을 둔 프레임워크로, 조직이 비즈니스 요구, 위험 감수 능력 및 자원에 따라 사이버 보안 활동을 조정 및 우선순위를 결정하고, 또한 조직은 해당 프레임워크의 위험 관리 원칙 및 지침을 적용하여 보안성과 탄력성을 향상시킬 수 있습니다.

Tencent Cloud 는 제 3 자 기관으로부터 인증받은 NIST CSF 인증을 획득하여, 이는 Tencent Cloud 의 사이버 보안 방어 체계 역량에 대한 인정일 뿐만 아니라, Tencent Cloud 가 보안 위험을 효과적으로 식별, 방어, 대응 및 처리하여 고객의 클라우드 자산과 데이터를 보호할 수 있음을 나타내며, 고객의 Tencent Cloud 보안 안정성에 대한 신뢰를 강화합니다.

**PCI DSS
인증** 지불 카드 업계 데이터 보안 표준(PCI DSS)은 지불 카드 업계 보안 표준 위원회(PCI SSC)에 의해 생성 및 유지 관리됩니다. 카드 소지자 데이터의 보안성을 강화하기 위해, PCI DSS 는 계정 데이터를 보호하기 위한 기술 및 운영 요구사항에 대한 글로벌 통일 기준을 제공하며, 적용 범위는 모든 지불 카드 처리를 포함하는 실체, 즉 상인, 처리업체, 매입자, 발행자 및 서비스 제공자, 그리고 카드 소지자 데이터를 저장, 처리 또는 전송하는 기타 실체를 포괄합니다.

Tencent Cloud 는 PCI DSS 인증 심사를 통과하여 PCI DSS 1 급 서비스 제공자 자격을 획득했습니다. 이는 Tencent Cloud 가 고객에게 안전하고 신뢰할 수 있는 지불 서비스를 제공하고, 카드 소지자의 데이터 보안을 보호할 수 있음을 입증합니다.

GxP 규정 준수 의료 보건 업계에서 GxP 는 광범위한 규정 준수 관련 활동을 포괄하며, 일반적으로 의약품, 의료 기기 및 의료 소프트웨어 애플리케이션 등 의료 제품의 개발, 제조 및 판매를 규제하는 일련의 규정, 지침 또는 업계 모범 사례를 지칭합니다.

Tencent Cloud 는 GxP 규정 준수 백서를 발표하여, 의료 업계 고객에게 Tencent Cloud 의 관리 프로세스 및 기술 조치가 고객이 GxP 컴퓨터화 시스템의 요구사항을 충족하도록 돕고, Tencent Cloud 에 호스팅된 고객 비즈니스 데이터의 기밀성, 무결성 및 가용성을 보장할 수 있음을 설명합니다.

03

Tencent Cloud

보안 책임 공유
모델

현재 점점 더 많은 고객이 클라우드 컴퓨팅 서비스 제공자 및 그들이 제공하는 제품과 서비스를 선택할 때, 보안을 주요 고려 사항 중 하나로 삼고 있습니다. Tencent Cloud 는 클라우드 컴퓨팅 서비스의 개방 및 공유 특성을 견지하며, 지속적으로 클라우드 플랫폼과 클라우드 서비스의 보안 능력을 향상시키고, 고객과 함께 클라우드 비즈니스와 데이터를 위해 더 좋고 완벽한 보안 보장 체계를 구축합니다. Tencent Cloud 는 클라우드 서비스 제공자로서 데이터센터의 인프라와 클라우드 플랫폼의 보안을 책임집니다. 고객이 서로 다른 클라우드 서비스 범주(예: IaaS, PaaS 및 SaaS 서비스)를 선택할 때 다양한 구성 요소에 대한 통제권 또한 다르다는 점을 고려하여, Tencent Cloud 는 서로 다른 클라우드 서비스 범주에 기반한 클라우드 보안 책임 공유 모델을 구축했습니다. 아래 다이어그램에서 연한 파란색 부분은 Tencent Cloud 가 책임지며, 연한 회색 부분은 고객이 책임지고, 연한 녹색 부분은 Tencent Cloud 와 고객이 상응하는 책임을 공동으로 부담함을 나타냅니다.

	IaaS	PaaS	SaaS	
고객의 책임	클라우드 고객의 데이터 보안	클라우드 고객의 데이터 보안	클라우드 고객의 데이터 보안	서비스/사나리 다양한 의 다양한 책임 Tencent Cloud가 책임
	클라우드 고객의 계정 및 접근 통제 정책	클라우드 고객의 계정 및 접근 통제 정책	클라우드 고객의 계정 및 접근 통제 정책	
	클라우드 보안 구성 정책	클라우드 보안 구성 정책	클라우드 보안 구성 정책	
	클라우드 애플리케이션 보안	클라우드 애플리케이션 보안	클라우드 애플리케이션 보안	
	클라우드 가상화 네트워크 및 호스트 보안	클라우드 가상화 네트워크 및 호스트 보안	클라우드 가상화 네트워크 및 호스트 보안	
	클라우드 플랫폼 및 클라우드 제품 자체 보안 및 규정 준수	클라우드 플랫폼 및 클라우드 제품 자체 보안 및 규정 준수	클라우드 플랫폼 및 클라우드 제품 자체 보안 및 규정 준수	
	물리적 및 기반 아키텍처 보안	물리적 및 기반 아키텍처 보안	물리적 및 기반 아키텍처 보안	

그림 1: Tencent Cloud 정보 보안 책임 공유 모델

Tencent Cloud 는 위 그림의 다양한 보안 속성에 대해 다음과 같이 설명합니다:

- 클라우드 고객의 데이터 보안: 고객의 클라우드 컴퓨팅 환경 내 비즈니스 데이터 자체의 보안 관리로, 업로드, 저장, 배포, 가공 및 기타 방식으로 처리된 고객 비즈니스 데이터 등을 포함합니다.

- 클라우드 고객의 계정 및 접근 통제 정책: 고객이 등록한 Tencent Cloud 계정 정보와, 클라우드 계정 하의 모든 권한 부여 행위로, 계정 정보, 비밀번호, 접근 통제 정책, 신원 인증 등의 정보를 포함합니다.
- 클라우드 보안 구성 정책: 클라우드 제품(보안 제품 포함)을 올바르게 개발하거나 사용하기 위해, 다양한 시나리오와 비즈니스 보안 요구사항에 부합하는 보안 제품과 보안 구성 정책입니다.
- 클라우드 애플리케이션 보안: 클라우드 컴퓨팅 환경 내 비즈니스 관련 애플리케이션 시스템의 보안 관리로, 애플리케이션의 설계, 개발, 릴리스, 운영, 모니터링 운영 등을 포함합니다.
- 클라우드 가상화 네트워크 및 호스트 보안: 클라우드 컴퓨팅 환경 내 호스트 및 네트워크 보안 관리로, 네트워크 계층은 가상 네트워크, 로드 밸런싱, 보안 게이트웨이, VPN, 전용선 링크 등을 포함하고, 호스트 계층은 클라우드 컴퓨팅, 클라우드 스토리지, 클라우드 데이터베이스 등의 클라우드 제품의 기반 관리(예: 가상화 제어 계층, 데이터베이스 관리 시스템, 디스크 어레이 네트워크 등)와 사용 관리(예: 가상 호스트, 이미지, CDN, 파일 시스템 등)를 포함합니다.
- 클라우드 플랫폼 및 클라우드 제품 자체 보안 및 규정 준수: 클라우드 컴퓨팅 환경 내 클라우드 플랫폼 및 제공된 클라우드 제품/서비스 자체의 보안 및 규정 준수를 의미합니다.
- 물리적 및 기반 아키텍처 보안: 클라우드 컴퓨팅 환경 내 데이터센터의 안전한 운영, 물리적 서버 및 물리적 네트워크 장비의 보안 관리 등을 의미합니다.

보안 책임 공유 모델에 관한 자세한 정보는 [Tencent Cloud Security White Paper](#) 를 참조하시기 바랍니다.

04

Tencent Cloud 글로벌 인프라

Tencent Cloud 는 전 세계적으로 다수의 데이터 센터를 배치하여 방대한 인프라 네트워크를 형성했으며, 이를 통해 글로벌 고객에게 빠르고 안정적이며 지능적이고 신뢰할 수 있는 근접 서비스를 제공할 수 있습니다. Tencent Cloud 는 중국 본토, 아시아 태평양 지역, 북미 지역, 유럽 지역에서 20 개 이상의 지리적 리전(Region)을 개방하고 60 개 이상의 가용성 존(Availability Zone)을 운영하여 더 많은 기업에 강력한 기술 지원을 제공하고 비즈니스의 급속한 확장을 지원하며, 고객이 다양한 지역의 규정 요구사항에 유연하게 대응하고, 금융 산업 기업의 데이터 현지화 저장 및 비즈니스 글로벌화 수요를 충족시키며, 데이터 처리의 규정 준수성, 안전성 및 효율성을 보장합니다.

- 리전(Region) 은 물리적 데이터 센터의 지리적 영역을 의미합니다. Tencent Cloud 의 서로 다른 리전 간은 완전히 격리되어 있어 서로 다른 리전 간 최대의 안정성과 내결함성을 보장합니다. 액세스 지연 시간을 줄이고 다운로드 속도를 높이기 위해 고객은 가장 가까운 리전을 선택하는 것이 좋습니다.
- 가용성 존(Zone) 은 Tencent Cloud 가 동일 리전 내에서 전력과 네트워크가 서로 독립된 물리적 데이터 센터를 의미합니다. 그 목표는 가용성 존 간 고장이 상호 격리되도록(대형 재해 또는 대형 전력 장애 제외) 하여 장애 확산이 발생하지 않도록 하고, 사용자의 비즈니스가 지속적으로 온라인 서비스를 제공할 수 있도록 하는 것입니다. 사용자는 독립적인 가용성 존 내 인스턴스를 시작함으로써 애플리케이션이 단일 위치 장애의 영향을 받지 않도록 보호할 수 있습니다.

Tencent Cloud 는 현재 중국 국내에 2300 개 이상의 가속 노드를 배치하여 다중 통신사를 커버하고, 해외에 900 개 이상의 가속 노드를 배치하여 전 세계 70 개 이상의 국가 및 지역을 커버하며, 서비스 콘텐츠를 전 네트워크 가속 노드에 분배하고 글로벌 스케줄링 시스템을 활용하여 사용자가 근처 노드에서 필요한 콘텐츠를 획득할 수 있도록 하여 액세스 지연 시간을 줄입니다.

Tencent Cloud 는 또한 독립 사이트를 설립하고 데이터 암호화, 접근 제어, 감사 추적 등의 기술적 수단을 채택하여 데이터의 격리성과 안전성을 강화하고 데이터 유출 및 불법 접근을 방지하며, 데이터의 지리적 격리와 규정 준수 처리를 강화합니다.

Tencent Cloud 인프라에 대한 자세한 정보는 [Tencent Cloud 글로벌 인프라](#) 페이지를 참조하시기 바랍니다.

05

Tencent Cloud

「전자금융거래법」을
어떻게 준수하고 고객이
이를 충족하도록
지원하는가

「전자금융거래법」은 전자금융 거래의 법률적 관계를 명확히 하고, 동시에 전자금융 산업의 건전한 발전 기반을 마련하여 국민의 금융 편의를 도모하고 국민 경제의 발전에 기여하기 위해 제정되었습니다. 전자금융 거래의 안전성과 신뢰성을 보장하기 위해, 본 법은 금융회사 및 전자금융 서비스 제공자 등에게 정보보호 기술 관련 계획 수립, 정보보호 최고 책임자 임명, 전자금융 인프라에 대한 정기적 취약성 분석 및 평가, 침해 사건에 대한 신속한 대응 및 보고 등의 관련 요구사항을 명시하고 있습니다.

본 장에서는 Tencent Cloud 가 「전자금융거래법」에서 클라우드 서비스 제공자와 관련된 통제 요건을 정리 및 요약하고, Tencent Cloud 가 클라우드 서비스 제공자로서 어떻게 금융회사, 전자금융 서비스 제공자 등이 관련 요건을 준수하도록 지원하는지 설명합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
21	안전성의 확보의무	① 금융회사등은 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다. ② 금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다. ③ 금융위원회는 제 2 항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니 되며, 보안기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다. ④ 대통령령으로 정하는 금융회사 및 전자금융업자는 안전한 전자금융거래를 위하여 대통령령으로 정하는 바에 따라 정보기술부문에 대한 계획을 매년 수립하여 대표자의	고객은 금융위원회가 정한 정보기술 분야, 전자금융 업무 및 전자서명인증서 관련 기준을 준수하여 전자금융 거래의 안전을 관리하고 보호해야 하며, 매년 정보기술 분야 관련 계획을 수립하여 대표자의 확인과 서명을 거친 후 금융위원회에 제출하여야 합니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 사업장 소재 관할권의 법률 및 규정을 엄격히 준수하며, 정보 보안 운영이 관련 법률, 규정, 표준 및 절차 요건에 부합하도록 보안 및 규정 준수 관련 절차를 마련하였습니다. Tencent Cloud 법무팀은 Tencent Cloud 의 비즈니스와 관련된 규제 요건을 지속적으로 파악하고 수집하여 해당 법률 및 규정 목록을 작성하며, 이를 정기적으로 관리하고 갱신합니다. Tencent Cloud 는 매년 독립된 제 3 기관의 전문 감사를 받으며, 검증보고서 성격의 시스템 및 조직 통제 보고서를 제공하여 클라우드 이용 기관, 독립 감사인, 규제 기관,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		확인·서명을 받아 금융위원회에 제출하여야 한다.	회사 주주 및 기타 이해관계자에게 Tencent Cloud 서비스 조직의 최신 내부 통제 현황을 투명하게 공개하고 있습니다. 정보 보안 관리 계획 측면에서 Tencent Cloud는 정보 보안 관리 정책을 수립하였으며, 이는 정보 보안 종합 전략, 보안 조직 구조 및 보안 관리 체계로 구성되어 클라우드 플랫폼의 안전한 운영과 위험 관리를 효과적으로 지원합니다. Tencent Cloud의 정보 보안 정책은 매년 정기적으로 검토되어 클라우드 보안 관리 체계의 통제 목표, 통제 절차 및 통제 조치가 관련 보안 전략, 표준, 절차 및 법적 요구사항에 부합하는지 확인하며, 정보 보안 정책의 적절성과 유효성을 보장합니다. Tencent Cloud는 또한 수용 가능한 사용 정책을 수립하여 직원 및 제 3자가 Tencent Cloud 회사 자원(IT 시스템, 네트워크, 장비, 데이터 등을 포함하되 이에 국한되지 않음)을 사용할 때의 책임과 의무를 명확히 하고, 합리적인 사용 행위를 규정하며 잠재적 위험을 방지합니다. Tencent Cloud는 ISO/IEC 27001 정보 보안 관리 체계, ISO/IEC 27017 클라우드 서비스 정보 보안 관리 체계, ISO/IEC 22301 업무 연속성 관리 체계, ISO/IEC 20000 정보 기술 서비스 관리 체계 등의 국제 보안 관련 표준 인증을 획득하였습니다.
21-2	정보보호 최고책임자 지정	① 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하여야 한다. ② 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자는	고객은 자사의 총 자산 및 직원 수 등의 요인을 기반으로 정보 보호 최고 책임자를 임명하여, 전자금융 업무 및 이를 지탱하는 기초 정보 기술 부분의 보안 관리 업무를 총괄하게 하여야 합니다. 이는 정보 보안 전략 계획 수립, 보안 관련 인적 자원 및 예산 관리, 사고 예방 및 비상 대응 등을 포함합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		정보보호최고책임자를 임원(「상법」 제 401 조의 2 제 1 항제 3 호에 따른 자를 포함한다)으로 지정하여야 한다. ③ 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자의 정보보호최고책임자는 제 4 항의 업무 외의 다른 정보기술부문 업무를 겸직할 수 없다. ④ 제 1 항에 따른 정보보호최고책임자는 다음 각 호의 업무를 수행한다. - 제 21 조제 2 항에 따른 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립 - 정보기술부문의 보호 - 정보기술부문의 보안에 필요한 인력관리 및 예산편성 - 전자금융거래의 사고 예방 및 조치 - 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항 ⑤ 정보보호최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다.	고객의 규제 요구사항 준수를 지원하기 위해 Tencent Cloud 는 정보 보안 관리 체계를 구축하고 정보 보안 최고 책임자를 임명하여 정보 보안 거버넌스 업무를 총괄하게 하였습니다. 주요 책임은 다음과 같습니다: (1) Tencent Cloud 의 정보 보안 관리 체계의 수립, 이행 및 지속적 개선을 주도하여 회사가 국가 법률, 규정, 규제 요구사항 및 업계 정보 보안 표준을 엄격히 준수하도록 보장합니다. (2) 회사의 정보 보안 관리 체계 성과 평가 및 개선을 감독하고 보안 역량의 지속적 발전을 추진합니다. (3) 정보 보안 관리에 필요한 충분한 자원을 보장하고 직원의 보안 의식 및 역량 교육을 조직하여 정보 보안 관리 요구사항을 충족시킵니다. (4) 부서 간 및 분야 간 정보 보안 조정 업무를 담당하여 체계의 효율적인 운영을 보장합니다.
21-3	전자금융기반 시설의 취약점 분석·평가	① 금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자금융기반시설²에 대한 다음 각 호의 사항을 분석·평가하고	고객은 전자금융 기반시설에 대한 취약성 분석 및 평가를 수행하고, 그 결과에 기반하여 필요한 보완 조치 이행 계획을 수립 및 시행해야 합니다. 고객은 평가 결과와 보완 조치 이행 계획 등을 금융위원회에 신속히 보고해야 합니다.

² “전자금융기반시설”이란 전자금융거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 2 조제 1 항제 1 호에 따른 정보통신망을 말한다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		그 결과 ³ (「정보통신기반보호법」 제 9 조에 따른 취약점 분석·평가를 한 경우에는 그 결과를 말한다)를 금융위원회에 보고하여야 한다 ⁴ .	취약성 스캔 측면에서 Tencent Cloud 는 고객에게 Vulnerability Scanning Service (VSS) 를 제공하여 기업 네트워크 자산을 탐지하고 그 위험을 식별할 수 있도록 지원합니다. Tencent 의 다년간 축적된 보안 경험과 위협 인텔리전스를 기반으로, VSS 는 풍부하고 포괄적인 취약성 규칙 데이터베이스를 구축하였으며, 전문적이고 효율적인 0Day/1Day/NDay 취약성 탐지 능력을 보유하고 있습니다. 이를 통해 고객 자산의 가용성, 안전성 및 규정 준수 여부에 대해 정기적인 보안 스캔, 지속적인 위험 경고 및 취약성 탐지를 수행하여 고객에게 전문적인 수정 권고를 제공함으로써 보안 위험을 줄일 수 있습니다. VSS 는 또한 호스트 보안, 웹 애플리케이션 방화벽 등의 클라우드 제품과 연동을 지원하여 위험 모니터링부터 위험 처리까지의 폐쇄형 루프를 실현합니다.
		1. 정보기술부문의 조직, 시설 및 내부통제에 관한 사항	
		2. 정보기술부문의 전자적 장치 및 접근매체에 관한 사항	
		3. 전자금융거래의 유지를 위한 침해사고 대응조치에 관한 사항	
		4. 그 밖에 대통령령으로 정하는 사항	
		② 금융회사 및 전자금융업자는 제 1 항에 따른 전자금융기반시설의 취약점 분석·평가 결과에 따른 필요한 보완조치의 이행계획을 수립·시행하여야 한다.	침투 테스트 측면에서 Tencent Cloud 는 고객에게 Penetration Testing Service (PTS) 를 제공합니다. 이 서비스는 해커가 사용할 수 있는 공격 기술과 취약점 발견 기술을 완전히 모방하여, 통제 가능하고 비파괴적인 방법과 수단으로 대상 시스템의 보안을 심층적으로 탐색합니다. 이를 통해 대상 및 네트워크 장비에 존재하는 취약점을 발견하고, 시스템 보안성을 강화하는데 도움이 되는 보안 강화 권고를 제공하며, 취약점 수정 후 검증을 지원합니다.
		③ 금융위원회는 소속 공무원으로 하여금 제 1 항에 따른 전자금융기반시설의 취약점 분석·평가 결과 및 제 2 항에 따른 보완조치의 이행실태를 점검하게 할 수 있다.	고객의 규제 가이드라인 준수를

³ 이 법 시행령 제 11 조의 6 제 2 항에 따라, 전자금융 기반시설의 취약성 분석 및 평가는 최소한 매 사업연도마다 한 차례 실시해야 합니다.

⁴ 이 법 시행령 제 11 조의 6 제 3 항에 따라, 취약성 분석 및 평가 종료 후 30 일 이내에 금융위원회에 결과 보고서 및 보완 조치 이행 계획을 제출해야 합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			지원하기 위해, Tencent Cloud는 내부적으로 정기적인 취약성 스캔과 침투 테스트 메커니즘을 구축했습니다. Tencent Cloud 내부의 취약성 스캔은 일반적으로 웹 취약점, 구성 요소 취약점, 설정 스캔 등을 포함하며, 취약성 스캔 시스템을 통해 자동 생성된 스캔 작업으로 클라우드 환경 내 자산에 대한 취약성 스캔을 수행하고 발견된 취약점을 분석, 분류 및 수정 처리합니다. 침투 테스트 측면에서는 Tencent Cloud 보안팀이 정기적으로 전체 링크 대규모 침투 테스트를 진행하며, 신제품 출시 전이나 중대 변경과 같은 상황에서 유연하게 표적 침투 테스트를 수행합니다. 테스트 결과는 보안 작업 티켓 형태로 관련 책임 부서에 통보되며, 책임 부서는 취약점 패치 또는 기타 보완적 통제 조치를 신속히 시행하여 침투 테스트에서 발견된 악용 가능한 취약점이 적절히 처리되었는지 확인합니다. 또한 Tencent Cloud는 정기적으로 레드팀/블루팀 대항 훈련을 통해 네트워크 공격에 대응하는 실전 훈련을 수행합니다. 정보 기술 관련 조직 및 내부 통제 등에 대해 Tencent Cloud 보안팀은 매년 최소 한 차례 이상 내부 보안 감사를 실시하며, 클라우드 플랫폼 및 내부 시스템의 상황을 지속적으로 모니터링하여 양호한 보안 태세를 유지하고 관련 법률 규정 및 보안 관리 표준의 규정과 요구사항을 준수하도록 합니다. Tencent Cloud는 매년 독립된 제 3 기관의 전문 감사를 받으며, 검증보고서 성격의 시스템 및 조직 통제 보고서를 제공하여 클라우드 이용 기관, 독립 감사인, 규제 기관, 회사 주주 및 기타 이해관계자에게 Tencent Cloud 서비스

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			조직의 최신 내부 통제 현황을 투명하게 공개하고 있습니다.
21-5	침해사고의 통지 등	① 금융회사 및 전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 “침해사고”라 한다)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 한다. ② 금융회사 및 전자금융업자는 침해사고가 발생하면 그 원인을 분석하고 피해의 확산을 방지하기 위하여 필요한 조치를 하여야 한다.	고객은 침해 사건 발생 시, 사고 원인을 분석하고 피해 확산을 방지하기 위한 필요 조치를 취하며, 즉시 금융위원회에 보고해야 합니다. 고객이 사고를 탐지하고 신속히 대응할 수 있도록 지원하기 위해, Tencent Cloud는 일원화된 보안 관리 플랫폼인 Cloud Security Center (CSC)를 제공합니다. CSC는 자산 센터, 위험 센터, 경보 센터, 고급 보안 관리 등의 기능을 통해 사전 위협 탐지, 사건 발생 시 대응 및 처리, 사후 추적 분석의 보안 운영 폐쇄 루프를 실현하도록 도와 보안 운영 효율성을 향상시킵니다. 고객의 규제 지침 준수를 지원하기 위해, 사건 대응 및 처리 측면에서 Tencent Cloud는 정보 보안 사건 관리 규정을 수립하고, 정보 보안 보고, 대응 및 처리 메커니즘과 관련 절차를 마련하였으며, 사건 처리 절차에서 각 팀의 역할과 구체적인 책임을 명확히 하였습니다. Tencent Cloud는 내부 보안 운영 시스템을 사용하여 보안 사건을 기록합니다. 탐지 및 식별된 보안 사건에 대해 Tencent Cloud는 사건의 성격, 데이터 민감도, 영향 범위 등의 요소를 고려하여 보안 사건을 분석 및 등급 분류하고, 적시에 해당 책임자에게 알려 사건을 추적 처리하도록 합니다. 사건 대응 절차의 효과성과 신속성을 보장하기 위해 Tencent Cloud 내부 비즈니스 부서는 정기적으로 보안 사건 비상 대응 훈련을 진행하며, 보안 기술 발전과 상황 변화에 따라 보안 팀 직원들에게 기술 교육을 제공하여 최신 보안

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			규정과 운영 절차를 이해하고 준수하며, 최신 정보 보안 기준과 모범 사례를 숙지하도록 합니다. 고객이 커뮤니케이션 및 고지 의무를 효과적으로 이행할 수 있도록 지원하기 위해 Tencent Cloud는 정보 보안 사건 대응, 사건 에스컬레이션, 사건 통지 등의 관련 절차를 구축하여 사고의 영향을 받을 수 있거나 이미 받은 회사 내부 인원 및 고객 등 이해관계자들에게 적시에 경보 또는 통지를 제공하고, 모든 당사자가 질서 있고 적시에 효율적으로 소통과 협업을 할 수 있도록 합니다. 고객에게 영향을 미칠 수 있는 보안 사건의 경우 Tencent Cloud는 정보 보안 사건의 영향 범위와 정도에 따라 내부 검토를 거친 후, 적절한 방법으로 고객에게 정보 보안 사건 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.
26	전자금융거래정보의 제공 등	전자금융거래와 관련한 업무를 수행함에 있어서 다음 각 호의 어느 하나에 해당하는 사항을 알게 된 자는 이용자의 동의를 얻지 아니하고 이를 타인에게 제공·누설하거나 업무상 목적 외에 사용하여서는 아니된다. 다만, 「금융실명거래 및 비밀보장에 관한 법률」 제 4 조제 1 항 단서의 규정에 따른 경우 그 밖에 다른 법률에서 정하는 바에 따른 경우에는 그러하지 아니하다. 1. 이용자의 인적 사항 2. 이용자의 계좌, 접근매체 및 전자금융거래의 내용과 실적에 관한 정보 또는 자료	Tencent Cloud는 사업을 운영하는 관할권의 사용자 개인정보 보호 및 데이터 보안 법규를 엄격히 준수하며, 완벽한 정보 보안 및 개인정보 보호 관리 체계를 구축하고 다수의 국제 표준 인증을 획득했습니다. 고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. 서비스 제공 또는 문제 해결의 필요성이 있고, 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 부처의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 상황이 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 직접 접촉하지

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			않습니다. 또한 Tencent Cloud의 개인정보 수집, 처리 및 공유에 관한 자세한 정보는 개인 정보 처리 방침 을 참조하시기 바랍니다.

06

Tencent Cloud

「전자금융감독규정」을
어떻게 준수하고 고객이
이를 충족하도록
지원하는가

「전자금융감독규정」은 금융위원회(FSC)가 발포하며, 주로 다음 세 가지 사항을 명확히 합니다.

1. 「전자금융감독규정」 및 그 시행령에서 금융위원회에 위임된 사항
2. 「전자금융감독규정」 및 그 시행령의 관련 요구사항 이행
3. 기타 법률·규정에서 정한, 금융감독원의 감독을 받는 기관의 정보기술 부문이 그 안전성을 확보하는 데 필요한 사항

본 규정 제 14 조의 2 는 한국의 금융회사 또는 전자금융업자가 클라우드 컴퓨팅 서비스를 사용하고 평가하는 요건을 명시하며, <별표 2 의 2> 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가기준, <별표 2 의 3> 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획, <별표 2 의 4> 클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치, 등을 통해 관련 평가 항목 및 상응하는 평가 기준을 제공합니다.

본 장에서는 Tencent Cloud 가 「전자금융감독규정」에서 클라우드 서비스 제공자와 관련된 조항을 정리 및 요약하고, Tencent Cloud 가 클라우드 서비스 제공자로서 어떻게 금융회사 및 전자금융업자가 관련 요건을 준수하도록 지원는지 설명합니다.

6.1 전자금융거래의 안전성 확보 및 이용자 보호

6.1.1 인력, 조직 및 예산 부문

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
8	인력, 조직, 교육 및 예산	① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것 2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에	고객은 교육 계획을 수립하고 이행하여 임원 및 직원의 정보 보호 역량을 강화해야 하며, 계획의 이행 상황과 직원의 정보 보안 관련 법규 준수 여부를 평가하고 필요에 따라 계획을 보완하거나 갱신해야 합니다. 고객은 정보 보안 관련 법규를 위반한 직원에 대한 제재를 위한 절차를 수립 및 이행해야 합니다. 또한 고객은 정보 기술 및 정보 보안 분야의 전문 지식을 갖춘 인력과 충분한 예산을 보유해야 합니다. 정보 보안 관리 조직 구조 측면에서 Tencent Cloud 는 클라우드 보안 및 정보

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		조직과 인력을 갖추는 것	보안 관련 조직 구조를 구축하여 각 계층의 보안 기능 역할과 관련 책임을 명확히 하고, 정보 보안 감사 및 정보 보안 위험 평가 등 작업 메커니즘을 정의했습니다. Tencent는 보안 기술 위원회와 다양한 기능 및 분야별 전문 보안 팀을 설립했으며, 내부적으로 완비된 인적 자원 관리 기준과 절차를 구축하여 직무 요구사항에 따라 인력을 채용 및 배치하도록 하고 있습니다. Tencent Cloud는 업계의 베테랑 전문가 서비스 팀을 결집하여 고객에게 안전하고 신뢰할 수 있으며 전문적이고 규정을 준수하는 제품과 서비스를 제공하기 위해 노력하고 있습니다.
		3. 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 매년 교육계획을 수립·시행할 것	교육과 훈련 측면에서 Tencent Cloud는 내부적으로 완비된 정보 보안 교육 메커니즘을 구축하여 정규직 직원, 컨설턴트, 인턴, 외주 직원 등이 정보 보안 교육 과정을 이수하도록 요구하고 있습니다. 관련 교육 과정에는 전 직원 필수 교육, 핵심 직무 특화 교육 및 선택적 전문 과정 교육 등이 포함되며, 내용은 기본 보안 의식, 업무 환경 보안, 취약점 식별 및 방어, 개인정보 보호, 비상 대응, 개발 보안 규범 및 데이터 보안 요구사항 등을 포괄합니다.
		4. 최고경영자는 전년도 교육계획 시행 결과를 평가하고, 정보보호최고책임자는 그 결과를 금년도 교육계획에 반영할 것	
		5. 정보보호최고책임자는 임직원이 정보보안 관련법규를 준수하고 있는지 정기적으로 점검하고 그 점검결과 및 보완계획을 최고경영자에게 보고할 것	
		6. 최고경영자는 임직원이 정보보안 관련법규를 위반할 경우 그 제재에 관한 세부기준 및 절차를 마련하여 운영할 것	
		② 금융회사 또는 전자금융업자는 정보기술 및 정보보호 분야별 전문성을 갖춘 인력과 충분한 예산을 확보해야 한다.	Tencent Cloud는 완비된 징계 메커니즘을 구축하여 회사 규정을 위반하거나 어떠한 방식으로든 무단 공개를 시도한 직원에 대해서는 징계 절차에 따라 처리하며, 위반 행위의 경우 상황에 따라 노동 계약 해지, 법적 소송 제기, 형사 책임 추적을 포함한 적절한 제재 조치를 취합니다.
8-3	직무의 분리	금융회사 또는 전자금융업자는 정보기술부문의 내부통제를 위한 직무분리 기준을 수립·운용하여야 한다.	고객은 정보기술 부서 내부 통제를 위한 직무 분리 기준을 수립하고 이행해야 합니다. 고객의 규제 요구사항 준수를 지원하기 위해 Tencent Cloud는 클라우드 보안 및 정보 보안 관련 조직 구조를 구축하고,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			직무 분리 등의 원칙에 기반하여 각 계층의 보안 기능 역할과 관련 책임을 명확히 하여 상호 모순되는 직무가 분리, 견제, 감독되도록 보장합니다. 여기에는 시스템 개발과 운영 업무의 분리, 업무 운영과 시스템 승인의 분리 등이 포함되나 이에 국한되지 않습니다.

6.1.2 시설부문

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
9	건물에 관한 사항	금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 안전대책 및 출입통제 보안대책을 수립·운영해야 한다.	고객은 컴퓨터실이 위치한 건물의 안전과 출입 통제를 보장하기 위한 조치를 수립하고 이행해야 합니다. Tencent Cloud는 전 세계의 각 데이터센터를 관련 국제 표준 및 현지 안전 요구사항에 따라 입지 선정, 건설 또는 임대하여 환경적 위험을 충분히 고려하고 높은 확률의 환경 위험 지역을 피합니다. 현재 Tencent Cloud는 한국에 두 개의 임대형 데이터센터를 구축했습니다. 데이터센터의 탄력성과 안전성을 보장하기 위해 Tencent Cloud는 데이터 공급업체 선정, 계약상의 제약부터 지속적인 감독에 이르기까지 전 과정에 걸쳐 엄격한 관리 체계를 구축했습니다. Tencent Cloud는 고객에게 안전하고 안정적이며 지속적이고 신뢰할 수 있는 물리적 시설 기반을 제공하기 위해 노력하며, Tencent Cloud는 물리적 보안 관리 제도를 수립하여 운영 안전을 규제하고, 위험을 적시에 식별하며, 물리적 보안 관리를 강화하고 있습니다. 물리적 접근 통제 측면에서 Tencent Cloud는 데이터센터 운영사에 인원 범주와 접근 권한에 따라 출입 통제 승인 시스템 내 완전한 인력 접근 통제 보안 매트릭스를 구축하여, 각종 인원의 접근 및 운영 행위를 효과적으로 관리

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			및 통제하도록 요구합니다. Tencent Cloud는 운영사에 데이터센터에 출입하는 각종 방문객이나 직원에 대한 신원 확인과 휴대품 검사를 실시하고, 그들이 휴대한 물품을 등록하도록 요구합니다. 보안 및 모니터링 측면에서 Tencent Cloud는 운영사에 보안 요원을 배치하여 엄격히 점검 목록과 점검 계획에 따라 각 기기실 및 장비 상황을 순찰하며, 각 검사 지점에서 서명 및 점검 시간을 기록하도록 요구하고, 기반 시설 장애나 보안 사건이 발견될 경우 즉시 데이터센터 비상 사건 대응 절차를 가동하도록 합니다. Tencent Cloud는 또한 운영사에 데이터센터에 7*24 시간 사각지대 없는 비디오 모니터링 경보 시스템을 설치하고, 보안실에서 이를 감시하며, 모니터링 기록을 안전하게 저장하고 충분한 시간 동안 보관하도록 요구합니다.
10	전원, 공조 등 설비에 관한 사항	금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비의 안전성을 위한 기준을 수립·운용해야 한다.	고객은 전산실 소재 건물 내 전력, 공조 등 설비에 관한 보안 기준을 수립·이행하여야 합니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud는 물리적 보안 관리 제도를 수립하여 운영 안전을 규제하고, 위험을 적시에 식별하며, 물리적 보안 관리를 강화하고 있습니다. Tencent Cloud는 전 세계의 각 데이터센터를 관련 국제 표준 및 현지 안전 요구사항에 따라 입지 선정, 건설 또는 임대하여 환경적 위험을 충분히 고려하고 높은 확률의 환경 위험 지역을 피합니다. 현재 Tencent Cloud는 한국에 두 개의 임대형 데이터센터를 구축했습니다. Tencent Cloud는 데이터센터 운영사에 고안정성과 완전한 이중화를 갖춘 전력 공급 시스템 및 공조 시스템 등을 사용하도록 요구하여, 단일 장애 지점이 데이터센터의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			지속성과 가용성에 영향을 미치지 않도록 합니다.
11	전산실 등에 관한 사항	금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 포함한 대책을 수립·운영하여야 한다. - 국내에 본점을 둔 금융회사 또는 전자금융업자의 전산실 및 재해복구센터는 국내에 설치할 것(단, 제 50 조제 2 항에 따라 등록한 국외 사이버물을 위한 전자지급 결제대행업자는 제외) - 무선통신망을 설치하지 아니할 것 - 그 밖에 재해 및 위해방지, 출입·접근통제 등 전산실의 안전 및 보안에 관한 사항	고객은 전산실과 재해복구센터를 한국 국내에 설치하고, 재해 예방 및 접근 통제 등의 조치를 통해 전산실 보안을 보호하여야 합니다. Tencent Cloud 는 전 세계 여러 지역에서 관련 국제 표준과 현지 안전 요구사항에 따라 데이터센터를 건설하거나 임대하여, 고객에게 다중 지역(region) 및 다중 가용 영역(zone) 선택을 제공합니다. 또한, 사업 운영 관할권의 사용자 개인정보 보호 및 데이터 보안 관련 법률 규정을 엄격히 준수하며, 지속적으로 현지 규제 동향을 주의 깊게 모니터링합니다. 고객은 사업 발전 요구와 데이터 보안 요구사항에 따라 데이터와 시스템을 다른 지역 또는 다른 가용 영역에 자유롭게 유연하게 배포할 수 있습니다. 현재 Tencent Cloud 는 한국에 두 개의 데이터센터를 보유하고 있으며, 클라우드 서버, 클라우드 데이터베이스, 클라우드 스토리지 등을 포함한 다양한 클라우드 컴퓨팅 서비스를 제공합니다. 한국 고객은 한국 현지에서 자신의 데이터를 저장, 처리 및 백업할 수 있습니다. 재해 예방 측면에서 Tencent Cloud 는 운영사에 데이터센터에 완전한 소방 시스템(지정 구역 화재 감지 시스템, 자동 소화 시스템, 비상 사용용 수동 소화 장치 등)을 설치하도록 요구합니다. Tencent Cloud 는 또한 운영사에 데이터센터에 피뢰 시스템, 방사선 차단 시스템, 전력 공급 시스템, UPS 시스템, 조명 시스템 등 컴퓨터실 정상 작동에 필요한 시설을 설치하도록 요구하며, 데이터센터 유지보수 인력이 교대로

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			근무하여 24 시간 유지보수 및 장비 장애 신속 해결을 보장하도록 합니다. 또한 생산 환경에서는 무선 통신망 설치가 금지됩니다. 물리적 접근 통제 측면에서 Tencent Cloud는 데이터센터 운영사에 인원 범주와 접근 권한에 따라 출입 통제 승인 시스템 내 완전한 인력 접근 통제 보안 매트릭스를 구축하여, 각종 인원의 접근 및 운영 행위를 효과적으로 관리 및 통제하도록 요구합니다. Tencent Cloud는 운영사에 데이터센터에 출입하는 각종 방문객이나 직원에 대한 신원 확인과 휴대품 검사를 실시하고, 그들이 휴대한 물품을 등록하도록 요구합니다.

6.1.3 정보기술부문

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
12	단말기 보호대책	금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다. 1. 단말기는 인가된 사용자만 사용할 수 있도록 관리할 것 2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것 3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지, 정기적인 악성코드 감염여부 확인 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것 4. 정보유출 및 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 등에	고객은 시스템 접근 기록 유지, 인가된 사용자만 기기를 사용할 수 있도록 제한, 중요 단말에 강화된 보호 조치 실시, 단말의 보조 저장 매체에 대한 접근 통제 등의 방식으로 단말을 보호하여야 합니다. 고객은 Cloud Workload Protection Platform (CWPP)을 채택하여 클라우드 호스트에 보안 보호를 제공할 수 있습니다. CWPP는 축적된 방대한 위협 데이터를 기반으로 머신러닝을 활용하여 고객에게 해킹 침입 탐지, 취약점 위험 경보 등 보안 보호 서비스를 제공하며, 비밀번호 해킹 차단, 비정상 로그인 알림, 트로이 목마 파일 탐지, 고위험 취약점 탐지 등 보안 기능을 포함하여 현재 서버가 직면한 주요 네트워크 보안 위험을 해결합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		접근하는 것을 통제할 것	고객의 규제 준수를 지원하기 위해, 호스트 단말 보호 측면에서 Tencent Cloud 는 엔드포인트 탐지 및 대응(EDR) 도구를 배포하여 전체 네트워크 서버 단말 자산에 대한 포괄적인 모니터링 및 제어를 수행합니다. Tencent Cloud 가 사용하는 EDR 도구는 바이러스 백신 및 침입 탐지, 보안 기준선 및 취약점 스캔, 그리고 명령 작업, 로그인 행위에 대한 보안 규정 준수 감사 등의 기능을 지원하며, 악성 프로그램이나 비정상적 행위를 식별할 때 경보를 발생시킵니다. Tencent Cloud 는 작업 티켓 시스템을 통해 경보 사건을 추적 및 처리합니다. 사무 단말 보호 측면에서 Tencent Cloud 는 내부적으로 소프트웨어 보안 규정을 수립하여 사무 단말(노트북 및 워크스테이션 포함)의 소프트웨어 사용 제한을 명확히 하고, 애플리케이션 허용 목록 기술을 활용하여 알려졌고 신뢰할 수 있는 프로그램만 실행하도록 허용하여 악성 소프트웨어 침입 위험을 줄입니다. Tencent Cloud 는 또한 제로 트러스트 보안 관리 시스템을 통해 사무 단말을 제어하며, 바이러스 제거, 취약점 수리, 사전 대응 방어 등의 보안 능력을 통해 랜섬웨어 방지, 피싱 공격 방지, 내부 횡적 이동 방지 등 포괄적인 보안 보호를 실현합니다.
13	전산자료 보호대책	① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 1. 사용자 인증 수단을 개인별로 부여하고 접근권한은 최소한으로 부여하는 등 적절한 접근권한 관리 및 통제 절차를 수립·운용할 것 2. 전산자료의 보유현황을	고객은 접근 통제 절차, 데이터 저장 모니터링 및 보호 조치, 데이터 전송 보호 조치, 데이터 안전 폐기 조치, 관련 비상 대응 계획, 저장 매체 보호 조치, 백업 및 백업 검증 조치, 시스템 운영 기록 등을 포함한 전산 데이터 보호 조치를 수립·이행하여야 하며, 테스트에서 이용자 정보를 사용하지 않아야 합니다. 또한, 고객은 단말 및 전산 데이터에 접근할 수 있는 정보처리시스템 관리자에 대한 적절한 통제 조치를 수립·이행하고, 관리자의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		관리하고 책임자를 지정·운영할 것	주요 업무 활동을 검토·감독하여야 합니다.
3.	전산자료 및 전산장비의 반출·반입을 통제할 것	데이터 접근 관리 측면에서, Cloud Access Management (CAM) 는 고객이 Tencent Cloud 제품 및 자원에 대한 접근을 안전하고 세밀하게 관리할 수 있도록 도와주며, 서로 다른 자원에 대해 서로 다른 인력에 특정 권한을 부여합니다. 고객은 CloudAudit 를 통해 Tencent Cloud 계정 활동에 대한 감독, 규정 준수 점검, 운영 검토 및 위험 검토를 수행할 수도 있습니다. Tencent Cloud 는 또한 Bastion Host (BH) 를 제공하여 사용자, 자산, 계정, 운영 권한 등의 차원에 기반한 세분화된 권한 부여를 지원하여, 사용자가 보유한 권한이 자산 접근 및 업무 수행에 필요한 최소한의 권한임을 보장합니다.	
4.	비상시에 대비하여 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것	고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. Tencent Cloud 는 고객 콘텐츠에 접근하거나 공개하려고 시도하지 않습니다. 직원의 클라우드 환경 및 인프라 접근을 통제하기 위해 Tencent Cloud 는 생산 환경에 베스천 호스트(Bastion Host)를 전면 배포하여, 이를 통해 Tencent Cloud 백엔드 시스템 구성 요소의 관리자 계정 권한과 계정 활동을 중앙 집중식으로 관리합니다. 백엔드 운영 작업 기록은 모두 로깅 플랫폼에 집중 저장되며, Tencent Cloud 내부 감사팀이 정기적으로 기록을 검토합니다.	
5.	정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것	데이터 저장 보호 측면에서 Tencent Cloud 의 여러 저장 및 데이터베이스 제품은 데이터 암호화 기능을 지원하며, 안전한 고강도 암호화 알고리즘을 사용하고 키의 전 생애 주기 관리 및 보호를 지원하여 데이터 기밀성을	
6.	중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것		
7.	주요 백업 전산자료에 대하여 정기적으로 검증할 것		
8.	이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)		
9.	정보처리시스템의 가동기록은 금융감독원장이 정하는 사항을 접속의 성공여부와 상관없이 자동적으로 기록·유지하고 1년 이상 보존할 것		
10.	단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할		

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)	보장합니다. Tencent Cloud 는 데이터 저장 시 다중 복사본 중복 저장 및 삭제 코드 기술을 사용하고 무결성 오류가 감지될 경우 필요한 복구 조치를 취하여 데이터의 내결함성을 크게 향상시킵니다.
		11. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것	컴퓨터 장비 수출입 측면에서 Tencent Cloud 는 데이터센터 운영사에 데이터센터의 물리적 접근을 위한 공식적인 접근 절차를 설정하고, 데이터센터에 들어가는 인원의 신원을 확인하며, 휴대품을 검사 및 등록하고, 장비의 기계실 출입(예: 설치 운용 또는 폐기, 반출)에 대한 승인 및 검사 절차를 설정하도록 요구합니다.
		② 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.	데이터 전송 보호 측면에서, 고객의 Tencent Cloud 콘솔 상의 모든 통신은 HTTPS 보안 프로토콜의 암호화 보호를 받습니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스는 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 고객의 비즈니스에 포트 수준의 통신 보안을 제공합니다. Key Management Service (KMS) 는 또한 엔벨로프 암호화를 통해 프로토콜 통신 내용 등에 암호화 서비스 및 키 보호와 권한 관리를 지원합니다. 또한, 고객은 다음과 같은 Tencent Cloud 서비스를 사용하여 다양한 시나리오에서의 데이터 안전한 전송을 실현할 수 있습니다:
		③ 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제 28 조 제 2 항에 따라 이중확인 및 모니터링을 하여야 한다.	• Direct Connect (DC): 전용성과 높은 보안성을 갖춘 대역폭 네트워크 연결을 제공합니다. 사용자가 네트워크 링크를 독점하여 데이터 유출 위험이 없습니다. • VPN Connection: 네트워크 터널링 기술을 기반으로, 온프레미스 데이터센터와 Tencent Cloud 상의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			자원 간의 안전한 전송 연결을 실현합니다. VPN 터널은 IKE(키 교환 프로토콜) 및 IPsec 을 사용하여 전송되는 데이터를 암호화하고, 인터넷 상에 안전하고 신뢰할 수 있는 데이터 터널을 구축하여 전송 과정 중 데이터의 안전을 보장합니다. 데이터 삭제 및 파기 측면에서, 고객의 서비스가 종료된 후 Tencent Cloud 는 엄격한 데이터 삭제 방식을 따릅니다. 보존 기간 만료 후 복제본 및 백업을 포함한 고객 데이터를 완전히 삭제하며, 삭제된 데이터는 복원할 수 없습니다. 매체 관리 측면에서, Tencent Cloud 는 매체 관리 관련 절차를 구축하여 매체 보관과 매체 처분의 구체적인 프로세스 및 표준을 명확히 했습니다. 매체 처분 전 관련 승인이 필요하며, 매체 처분에 대한 기록을 작성합니다. 물리적 매체를 사용하여 정보를 전송할 때, Tencent Cloud 는 작업 티켓 형태로 매체의 출고, 운송 및 반입 전 과정을 추적합니다. 데이터 백업 측면에서 Tencent Cloud 는 백업 관리 절차를 수립하여 관련 법률 및 규범 요구사항에 따라 수집 및 처리된 중요한 데이터를 백업합니다. 내부 중요 정보의 경우 Tencent Cloud 는 데이터 등급에 따라 서로 다른 데이터의 백업 전략을 수립하고 정기적으로 복구 테스트를 수행합니다. 클라우드 고객 데이터의 경우 Tencent Cloud 는 클라우드 제품 또는 서비스의 기능에 따라 고객에게 다중 저장 복사본 및 백업 서비스를 제공하며, 제품 서비스 수준 계약에 명시된 바에 따라 제공하는 데이터 백업 서비스에 대한 책임을 집니다. Tencent Cloud 가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 저장 서비스,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			데이터베이스 서비스, 컨테이너 및 미들웨어 서비스 등 다양한 클라우드 제품/서비스는 모두고가용성 특성을 갖추고 있어 고객이 시스템 또는 서비스의고가용성을 실현하는 데 도움을 줍니다. 예를 들면: • Cloud Load Balancer (CLB) 는 안전하고 빠른 4/7 계층 트래픽 분산 서비스를 제공하여, 트래픽 분산을 통해 애플리케이션 시스템의 외부 서비스 역량을 확장하고 단일 장애점을 제거합니다. CLB 는 클러스터 배포를 채택하며, 장애 인스턴스를 신속히 제거하여고가용성을 실현합니다. • Cloud Virtual Machine (CVM) 은 서비스고가용성과 데이터 고신뢰성의 특성을 갖추고 있습니다. CVM 에 탑재된 클라우드 디스크는 3 중 복사본 저장 전략을 제공하여 데이터가 어느 한 복사본에 장애가 발생할 경우 빠르게 데이터를 이전하고 복구할 수 있도록 보장합니다. • Cloud Object Storage (COS) 은 데이터의 다중 아키텍처, 다중 장치 간 중복 저장을 제공하여 사용자 데이터에 재해 복구 및 자원 격리 기능을 제공하여 데이터 지속성을 실현합니다. • Cloud Native Database TDSQL-C: Tencent Cloud 의 자체 연구 개발 차세대 클라우드 네이티브 관계형 데이터베이스로서,고가용성 클러스터 아키텍처를 채택하여 장애 노드를 자동 감지할 수 있으며, 초 단위 장애 전환 및 복구를 지원합니다. • TencentDB for MySQL 은

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			데이터의 고신뢰성과 서비스의 고가용성을 실현하며, 완벽한 데이터 자동 백업 및 무손실 복구 메커니즘을 보유하고 있습니다. <u>Tencent Kubernetes Engine (TKE)</u> 는 분산 서비스 아키텍처를 채택하여 서비스의 장애 자동 복구 및 빠른 이전을 보장합니다. 상태 유지 서비스 백엔드의 분산 저장과 결합하여 서비스와 데이터의 안전 및 고가용성을 실현합니다. 테스트 데이터의 보안 관리 측면에서 Tencent Cloud 는 개발/테스트 환경과 프로덕션 환경이 서로 격리되도록 보장하며, 개발/테스트 환경에서 탈식별화되지 않은 프로덕션 환경 데이터의 사용을 금지합니다. 시스템 운영 또는 작업 기록에 대해서 Tencent Cloud 는 고객에게 <u>Cloud Log Service (CLS)</u> 를 제공합니다. 일원화된 로그 서비스 플랫폼으로서 CLS 는 로그 수집, 로그 저장, 로그 검색 분석, 실시간 소비, 로그 전달 등 다양한 서비스를 지원하여 고객이 비즈니스 운영, 보안 모니터링, 로그 감사, 로그 분석 등의 문제를 해결하는 데 도움을 줍니다. CLS 는 사용자가 로그의 저장 기간을 사용자 정의할 수 있도록 지원하며, 표준 저장 유형의 로그 주제는 1 일부터 3600 일까지 또는 영구적으로 저장할 수 있고, 저빈도 저장 유형의 로그 주제는 7 일부터 3600 일까지 또는 영구적으로 저장할 수 있습니다. 단말 관리 측면에서 Tencent Cloud 는 직원 사무 단말에 데이터 외부 유출을 제한할 수 있는 데이터 유출 방지(DLP) 도구를 배포하여, 잠재적인 데이터 도난 활동을 모니터링, 탐지 및 방지합니다. 계정 권한 변경 측면에서 Tencent

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			Cloud 는 직위 역할에 대응하는 인원 신상 정보와 각 비즈니스 시스템 권한 수준의 기록을 유지 관리하며, 정기적으로 내부 권한 심사 작업을 조직하여 권한이 남용되거나 오용되지 않도록 보장합니다. 더 이상 필요하지 않은 접근 권한에 대해서는 적절한 후속 조치를 취하여 불필요한 접근 권한을 적시에 철회합니다.
14	정보처리 시스템 보호대책	금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 운영매뉴얼, 유지보수관리대장, 책임자명부 및 장애상황기록부 등 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 1. 다음 각 목을 작성·보관 할 것 가. 주요 정보처리시스템에 대한 운영매뉴얼 나. 주요 정보처리시스템에 대한 정기적인 유지보수 실시 내용을 기록한 유지보수관리대장 다. 정보처리시스템에 대한 책임자명부 및 장애상황기록부 2. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능하도록 모니터링시스템을 갖출 것 3. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것 4. 정보처리시스템의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할	고객은 주요 정보처리시스템에 대한 운영 매뉴얼, 유지보수 관리 대장, 책임자 명단, 장애 현황 기록부를 수립·유지하고, 시스템 자원 상태를 지속적으로 모니터링하며 중요 패치를 적시에 처리하여야 합니다. 고객은 또한 정보처리시스템의 구성 등을 백업하고, 정보처리시스템 관리자 로그인 등에 이중 인증(2FA) 및 운영 감사 등의 통제 조치를 실시하여야 합니다. 고객의 포괄적 정보 자산 관리를 지원하기 위해, Tencent Cloud 는 Cloud Workload Protection Platform (CWPP)을 제공하여 자산 지문의 자동 수집을 지원하고, 계정, 포트, 프로세스, 애플리케이션 등 자산 지문 데이터를 통합 관리합니다. 고객은 또한 Tencent Cloud 의 일원화된 보안 관리 플랫폼인 Cloud Security Center (CSC)를 활용하여 정보 자산 보안 관리를 수행할 수 있습니다. CSC 는 자산 보안 센터 기능을 포함하여, 클라우드 서버, 객체 저장소, 클라우드 데이터베이스, 로드 밸런서 등 클라우드 자산의 자동화된 동적 재고 파악을 실현하고, 클라우드 설정 위험, 취약점 및 보안 사건 등 다양한 보안 차원을 통해 자산 보안 위험을 통합 관리하여 클라우드 상의 "새도 IT" 위험을 낮춥니다. Tencent Cloud 는 또한 고객에게 Bastion Host (BH)를 제공하여, 특권 계정 접근 제어에 활용되며 사용자

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		것	관리, 권한 부여 관리, 인증 관리 및 종합 감사를 지원하고, 시나리오에 따라 정적 패스워드, LDAP 등 다양한 인증 방식을 제공하며, 보안성 강화를 위한 이중 요소 인증을 지원합니다.
5.	중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1 년 이상 기록·관리할 것		Tencent Cloud 는 내부적으로도 정보 자산 관리 규정 및 전 생애 주기 관리 프로세스를 수립하여, 전자 데이터, 하드웨어 및 그 가상 장비, 인프라, 애플리케이션 시스템 및 소프트웨어 등 자산에 대해 분류 및 등급별 관리 및 보호를 수행합니다. Tencent Cloud 는 자산 관리 시스템을 통해 하드웨어 장비 및 소프트웨어 구성 요소를 관리하며, 자산 등록 및 바인딩, 자산 재고 파악 및 정보 업데이트, 자산 폐기 및 교체 등을 포함하여, 클라우드 플랫폼의 기반 시스템이 안정적으로 운영되도록 보장하고 비즈니스 시스템에 신뢰할 수 있는 지원을 제공합니다.
6.	정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 이중인증 절차를 시행하고, 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하며, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것		클라우드 제품/서비스의 서비스 수준 및 모니터링 측면에서, Tencent Cloud 가 고객에게 제공하는 클라우드 서비스는 각 서비스별로 약정된 서비스 수준 계약에 기반하여 제공되며, 각 서비스의 성능 지표, 측정 기준 및 보고 요구사항은 각 제품의 서비스 수준 계약에 명확히 기재되어 Tencent Cloud 공식 웹사이트에 게시됩니다. 각 클라우드 서비스의 성능과 가용성은 지속적으로 추적되며, 관련 지표는 관리 콘솔을 통해 고객이 실시간으로 모니터링할 수 있습니다. Tencent Cloud 는 또한 고객에게 Tencent Cloud Observability Platform (TCOP) 을 제공하여 클라우드 제품/서비스 모니터링을 지원합니다. TCOP 는 클라우드 서버, 클라우드 데이터베이스 등 클라우드 제품이 자체 보고하는 다양한 모니터링 지표와 고객이 사용자

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			정의 구성하여 보고하는 모니터링 지표를 수집 및 시각화 차트로 표시하여, 고객이 클라우드 제품 자원 사용률, 애플리케이션 성능 및 클라우드 제품 운영 상태를 실시간으로 파악할 수 있도록 돕습니다. TCOP 는 지표에 대한 경보 설정을 지원하며, 설정된 경보 규칙에 따라 메시지 푸시 등을 통해 비즈니스 이상 상황을 고객에게 적시에 통지합니다. 변경 및 운영 관리 측면에서 Tencent Cloud 는 운영 관리 규정을 수립하여 운영 담당자의 일상 운영 행위에 대한 운영 지침과 요구사항을 제공합니다. Tencent Cloud 는 성숙한 도구화, 자동화된 운영 관리 플랫폼을 사용하여 운영 작업을 관리하며, 내부 운영 관리 메커니즘을 통해 변경 시간 창을 엄격히 통제하여 운영 요청이 지정된 시간 내에 완료되도록 보장합니다. Tencent Cloud 는 또한 상세한 운영 보안 기준선을 설정하고 정기적으로 내부 운영 보안 검토를 수행합니다. 생산 환경 내 작업이 통제 및 추적 가능하도록 하기 위해, 백엔드 운영 작업 기록은 상세히 기록되며 로깅 플랫폼에 중앙 집중식으로 저장되고, Tencent Cloud 내부 감사팀이 정기적으로 운영 과정 중의 의심스러운 작업에 대한 문제 조사 및 추적을 수행합니다. 패치 관리 측면에서 Tencent Cloud 는 최신 패치를 식별하고, 패치 설치 전 충분한 보안 테스트를 수행하여 패치 설치의 안전성을 보장합니다. Tencent Cloud 는 정기적으로 내부 각 비즈니스 팀에 패치 업그레이드 및 설치를 알리고, 엔드포인트 검사 도구를 사용하여 패치 설치 상태를 정기적으로 스캔하며, 기한 내에 패치가 설치되지 않은 장치에 대해서는 자동으로 경보

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			작업 티켓을 생성합니다. 이중화 백업 및 재해 복구 요구사항에 대해, Tencent Cloud 의 서로 다른 지역은 완전히 격리되어 있어 지역 간 최대의 안정성과 내결함성을 보장합니다. Tencent Cloud 는 또한 각 지역을 다시 여러 개의 상호 격리된 가용 영역으로 구분하여 고객의 비즈니스 연속성을 보장합니다. 현재 Tencent Cloud 는 한국에 두 개의 임대형 데이터센터를 배치했습니다. 고객은 비즈니스 발전 요구와 데이터 보안 요구사항에 따라 데이터와 시스템을 서로 다른 지역 또는 다른 가용 영역에 자유롭게 유연하게 배포하고, 서로 다른 비즈니스 연속성 모드를 채택하여 비즈니스 재해 복구 요구사항을 충족할 수 있습니다.
14-2	클라우드 컴퓨팅 서비스 이용절차 등	① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제 2 조제 3 호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다. 1. 다음 각 목의 기준에 따른 이용업무의 중요도 평가 가. 규모, 복잡성 등 클라우드컴퓨팅서비스를 통해 처리되는 업무의 특성 나. 클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향 다. 전자적 침해행위 발생 시 고객에게 미치는 영향 라. 여러 업무를 같은 클라우드컴퓨팅서비스	고객은 클라우드 컴퓨팅 서비스 이용 전, 클라우드 컴퓨팅 서비스를 통해 처리하는 업무의 중요성, 특성, 서비스 중단 영향, 집중 위험, 클라우드 서비스 제공자의 보안성 등을 평가하고, 클라우드 컴퓨팅 서비스 이용 관련 업무연속성 계획 및 안전성 확보 조치를 수립·이행하여야 합니다. 또한, 고객은 클라우드 서비스 제공자와 신규 사업 계약 체결 시, 그리고 클라우드 서비스 제공자에게 중대한 변경 또는 문제가 발생한 경우 금융감독원에 적시에 보고하여야 합니다. 고객의 클라우드 서비스 공급자 평가에 부합하기 위해, Tencent Cloud 는 고객의 요청 시 관련 정보를 제공하고, 전담 인력을 배치하여 고객의 실사 활동에 적극적으로 대응 및 협조합니다. 다음은 Tencent Cloud 가 클라우드 서비스 공급자로서 실사 관련 요구사항에 대응하는 다양한 측면의 개요적 실천사항입니다: • 평판 및 업계 경험: 중국 인터넷

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		제공자에게 위탁하는 경우 해당 클라우드컴퓨팅서비스 제공자에 대한 종속 위험 마. 클라우드컴퓨팅서비스 이용에 대한 금융회사 또는 전자금융업자의 내부통제 및 법규 준수 역량 바. 그 밖에 금융감독원장이 정하여 고시하는 사항 2. 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가(단, 제 1 호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 3. 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획 및 안전성 확보조치의 수립·시행(단, 제 1 호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 <별표 2 의 3> 및 <별표 2 의 4>의 필수 사항만 수립·시행할 수 있다.) ② 금융회사 또는 전자금융업자는 제 1 항 각 호에 따른 평가결과, 업무연속성 계획 및 안전성 확보조치에 대하여 제 8 조의 2 에 따른 정보보호위원회의 심의·의결을 거쳐야 한다. ③ 금융회사 또는 전자금융업자는 제 1 항제 2 호의 평가를 직접 수행하거나 제 37 조의 6 제 1 항의 침해사고대응기관이 수행한 평가 결과를 활용할 수 있다. ④ 금융회사 또는 전자금융업자는 다음 각 호의	업계 선도 기업인 Tencent 의 클라우드 컴퓨팅 브랜드로서, Tencent Cloud 는 다수의 업계 기관으로부터 전문 인증을 획득하고 포괄적인 클라우드 컴퓨팅 솔루션을 제공하며, 전 세계 수많은 기업 및 정부 기관 고객에게 신뢰할 수 있는 클라우드 컴퓨팅 서비스를 제공하여 전 세계 다양한 업계 고객의 인정을 받았습니다. • 전문성 및 기술 역량: Tencent Cloud 는 강력한 클라우드 컴퓨팅 기술, 빅데이터 처리 능력, 인공지능 응용, 네트워크 보안 방어, 클라우드 네이티브 기술, 글로벌 데이터센터 네트워크, 업계 솔루션을 통해 업계 선도자의 포괄적 기술 역량을 보여줍니다. 이러한 기술 역량은 Tencent Cloud 서비스의 안정성과 신뢰성을 보장할 뿐만 아니라 고객에게 안전하고 신뢰할 수 있는 클라우드 컴퓨팅 환경을 제공합니다. Tencent Cloud 의 완비된 운영 보안 역량 또한 고객에게 클라우드 제품에 대한 7*24 기술 지원을 제공할 수 있습니다. • 규정 준수 능력: 고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 사업장 소재 관할권의 법률 및 규정을 엄격히 준수하며, 정보 보안 운영이 관련 법률, 규정, 표준 및 절차 요건에 부합하도록 보안 및 규정 준수 관련 절차를 마련하였습니다. Tencent Cloud 는 매년 정보 시스템에 대한 보안 테스트, 위험 평가 및 내부 감사를 수행하여 보안 방어 역량이 항상 적정 수준에 있도록 하고 관련 보안 관리 및 표준의 규정과

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		어느 하나에 해당하는 사유가 발생한 날로부터 3 개월 이내에 금융감독원장에게 보고하여야 하고, 관련 서류를 최신상태로 유지하여야 한다.	요구사항을 준수합니다. 보안팀은 매년 지속적으로 Tencent Cloud 의 보안 관리 체계에 대해 내외부 보안 감사를 수행하여 정보 보안 조치의 효과성과 규정 준수를 보장합니다. 한국의 경우, Tencent Cloud 는 한국 정보보호 관리체계(K-ISMS) 인증을 획득했으며, 매년 정기적으로 KISA 의 감사를 받습니다.
		1. 클라우드컴퓨팅서비스 이용계약을 신규로 체결하거나, 기존 클라우드컴퓨팅서비스 이용계약을 통해 신규 업무를 처리하는 경우	• 비즈니스 연속성 및 재해 복구: Tencent Cloud 는 이미 ISO/IEC 22301 비즈니스 연속성 관리 체계의 국제 표준 인증을 획득했습니다. 고객 비즈니스의 지속적 가용성을 보장하기 위해, Tencent Cloud 는 클라우드 제품에 대해 상세한 재해 복구 계획을 수립하고, 엄격히 요구사항에 따라 정기적인 훈련을 수행하여 재해 복구 계획의 적시성과 실행 가능성을 보장합니다. • 위험 관리: Tencent Cloud 는 ISO/IEC 27001:2022 표준에 따라 내부 위험 관리 프레임워크를 개발 및 유지하여 식별된 위험을 파악, 분석 및 관리합니다. Tencent Cloud 는 정기적으로 위험 평가를 수행하며, 업계 보안 사고 보고서, Tencent Cloud 실무 경험, 전문 기관 위험 데이터베이스 등의 위험 출처를 참고하여 Tencent Cloud 제품 및 서비스 프로세스 내의 위험을 식별합니다. Tencent Cloud 는 자산 가치, 위험 발생 가능성, 위험 영향 정도를 평가하고 위험 등급을 계산합니다. 위험 분석 결과에 따라 식별된 위험에 대한 대응 전략 및 상응하는 완화 조치를 제공하여 위험을 수용 가능한 수준으로
		2. 클라우드컴퓨팅서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등 중대한 변경사항이 발생한 경우	
		3. 클라우드컴퓨팅서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 아니한 경우	
		4. 제 1 항제 2 호 또는 제 3 호에 관한 중대한 변경사항이 발생한 경우	
		⑤ 제 4 항의 보고에 관한 양식, 첨부서류 등에 관해서는 금융감독원장이 정하는 바에 따른다.	
		⑥ 금융감독원장은 제 4 항에 따라 제출한 보고 서류가 누락되거나, 중요도 평가 또는 업무연속성계획·안전성 확보조치 등이 충분하지 않다고 판단하는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.	
		⑦ 제 1 항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		제 11 조제 1 호 및 제 2 호, 제 15 조제 1 항제 5 호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제 50 조의 2 에 따른 국외 사이버물을 위한 전자지급결제대행업자는 제외한다)가 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제 11 조제 2 호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.	낮춥니다.
		⑧ 그 밖에 금융회사 또는 전자금융업자의 클라우드컴퓨팅서비스 이용에 대해서는 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따른다.	• 감사 및 평가: Tencent Cloud 는 매년 독립된 제 3 기관의 전문 감사를 받으며, 검증보고서 성격의 시스템 및 조직 통제 보고서를 제공하여 클라우드 이용 기관, 독립 감사인, 규제 기관, 회사 주주 및 기타 이해관계자에게 Tencent Cloud 서비스 조직의 최신 내부 통제 현황을 투명하게 공개하고 있습니다. 한국의 경우, Tencent Cloud 는 한국 정보보호 관리체계(K-ISMS) 인증을 획득했으며, 매년 정기적으로 KISA 의 감사를 받습니다. 또한, Tencent Cloud 는 고객 측에서 시작하는 감사 또는 평가 활동에 적극적으로 대응 및 협조합니다. Tencent Cloud 의 보안성, 비즈니스 연속성 계획 및 보안 보장 조치 등과 관련된 자세한 정보는 제 6.4 장클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가기준, 제 6.5 장클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획, 그리고 제 6.6 장클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치를 참조하시기 바랍니다.

6.1.4 정보보호부문

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
15	해킹 등 방지대책	① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운영하여야 한다.	고객은 긴급 중요 패치의 신속한 처리, 내부 네트워크와 인터넷 격리 등 정보처리시스템 및 정보통신망이 해킹 등 전자적 침해를 받지 않도록 보호 조치를 취하고, 관련 조치에 대한 담당자를 지정하고 운영 결과를 보존하여야 합니다. 또한, 고객은 무선

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영 2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시 3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지. 다만, 다음 각 목의 경우에는 그러하지 아니하다. 가. 이용자의 고유식별정보 또는 개인신용정보(「신용정보의 이용 및 보호에 관한 법률」 제 40 조의 2 에 따른 가명처리에 관한 행위규칙을 준수한 가명정보는 제외)를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한한다) 나. 업무상 불가피한 경우로서 금융감독원장의 확인을 받은 경우 4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것 5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등	네트워크 설치 및 운영 시 무선 네트워크를 통한 불법 접근을 방지하기 위한 보안 조치를 취하여야 합니다. 네트워크 분할 또는 격리 요구사항에 대응하기 위해, 고객은 Tencent Cloud 가 제공하는 Virtual Private Cloud (VPC) 서비스를 이용하여 구매한 클라우드 플랫폼 자원에 대해 다수의 독립적인 네트워크 공간을 구축하고, 네트워크 세그먼트 분할 및 IP 주소 할당, 사용자 정의 라우팅 정책 등을 자유롭게 설정할 수 있습니다. VPC 서비스는 Tencent Cloud 를 기반으로 구축된 전용 클라우드 네트워크 공간으로, 사설 네트워크는 터널링 기술을 활용하여 물리적 네트워크 상에 가상 네트워크를 구성하고 가상화 기술을 적용함으로써 서로 다른 사설 네트워크 간의 내부 네트워크를 완전히 격리시켜 고객에게 독립적이고 격리된 안전한 클라우드 네트워크를 제공합니다. 사설 네트워크 내의 클라우드 서버에 대해서는 보안 그룹 및 네트워크 ACL 규칙 설정을 통해 인스턴스 수준 및 서브넷의 인바운드/아웃바운드 트래픽을 제어하여, 다양한 수준의 네트워크 접근 제어를 구현할 수 있습니다. 고객은 또한 클라우드 방화벽, 웹 애플리케이션 방화벽, DDoS 방어 등 네트워크 경계 보호 도구를 선택할 수 있습니다. 이 중 Cloud Firewall (CFW) 은 주로 고객에게 다양한 네트워크 경계의 보호를 제공하며, 방화벽 ACL 능동적 제어, IPS 실시간 차단, 가상 패치 및 악성 코드 탐지 등의 기능을 지원하여 기존 네트워크의 DMZ 영역 요구를 충족시키고 핵심 자산에 대한 집중 보호를 실현하며, VPC 간의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		외부통신망으로부터 물리적으로 분리할 것. 다만, 다음 각 목의 경우에는 그러하지 아니하다.	세분화된 격리 관제를 가능하게 합니다. Web Application Firewall (WAF) 은 Tencent Cloud 내부 및 외부 사용자가 웹 공격, 침입, 취약점 악용, 악성 코드 삽입, 변조, 백도어, 크롤링 등 웹사이트 및 웹 비즈니스 보안 문제에 대응할 수 있도록 지원합니다. Anti-DDoS 는 충분하고 우수한 DDoS 방어 자원과 지속적으로 발전하는 "자체 개발 + AI 지능형 인식" 정제 알고리즘을 결합하여 DDoS 공격 문제에 대응합니다.
		가. 이용자의 고유식별정보 또는 개인신용정보(「신용정보의 이용 및 보호에 관한 법률」 제 40 조의 2에 따른 가명처리에 관한 행위규칙을 준수한 가명정보는 제외)를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한한다)	네트워크 통신 보안 측면에서 , 고객의 Tencent Cloud 콘솔 상 통신은 HTTPS 보안 프로토콜의 암호화 보호를 받습니다. VPN Connection 은 또한 고객이 온프레미스 데이터센터와 Tencent Cloud 상의 자원 간 안전한 전송 연결을 구현하도록 지원합니다. VPN 터널은 IKE(키 교환 프로토콜) 및 IPsec을 사용하여 전송되는 데이터를 암호화하고, 인터넷 상에 안전하고 신뢰할 수 있는 데이터 터널을 구축하여 전송 과정 중 데이터의 안전을 보장합니다.
		나. 업무상 불가피한 경우로서 금융감독원장이 인정하는 경우	
		② 제 1 항제 1 호의 규정에 따른 정보보호시스템의 안전한 운영을 위하여 금융감독원장이 정하는 사항을 준수하여야 한다.	테넌트 격리 측면에서 , Tencent Cloud는 가상화 제어층 자원 접근 통제 정책, 클라우드 플랫폼 내부 사설 네트워크 간 격리 정책, 웹 콘솔 권한 할당 및 신원 인증, 인터페이스 세션 ID 및 접근 키 등의 보안 메커니즘을 제공하여, 각 고객이 자신이 구매한 클라우드 컴퓨팅 자원에만 접근할 수 있도록 보장하며, 다중 테넌트 간 접근 격리를 효과적으로 실현합니다. 효과적인 격리 수단을 통해, 동일 자원 풀 내 고객 데이터는 서로 보이지 않도록 하고, 테넌트가 다른 테넌트의 데이터에 접근, 획득 또는 변조할 수 없음을 보장합니다.
		③ 제 1 항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.	
		④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해의 예방, 피해 최소화 및 신속한 복구를 위한 대책을 수립·운영하여야 한다.	
		⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운영할 때에는 다음 각 호의 사항을 준수하여야 한다.	
		1. 무선통신망 이용 업무는	Tencent Cloud 내부의 네트워크 보안

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
	최소한으로 국한하고 법 제 21 조의 2 에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것	방어 및 관리에 대해, Tencent Cloud 는 네트워크 침층 방어 체계를 구축하고 업계 실무를 참고하여 네트워크 보안 아키텍처를 설계하며, 비즈니스 기능과 보안 위험에 따라 보안 영역을 구분하고, 서로 다른 보안 영역에 대해 물리적 또는 논리적 격리를 수행하며, 접근 통제 및 경계 방어 등의 조치를 통해 업무 네트워크와 생산 네트워크의 보안을 확보합니다. Tencent Cloud 는 방화벽, 침입 탐지/방지 시스템(IDS/IPS), DDoS 방어, 웹 보안 방어 등 다중 방어 메커니즘을 통해 악성 네트워크 트래픽을 신속히 탐지, 필터링 및 차단하여 Tencent Cloud 의 네트워크 보안을 보호합니다.	
	2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립·운용할 것	인터넷 탐색 보안 측면에서, Tencent Cloud 네트워크 팀은 인터넷 탐색 채널에 대한 통합 관리, 웹 페이지 보안 필터링 및 악성 URL 차단 활성화, 단말 보안 및 바이러스 백신 소프트웨어 배포, 직원에게 인터넷 안전 탐색 등 보안 의식 교육을 제공하는 다방면의 보호 조치를 취했습니다.	
	3. 무선통신망에 인가되지 않은 정보처리시스템 및 단말기의 접속을 차단하여야 하며, 비인가 무선접속장비(Access Point: AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것	무선 네트워크 관리 측면에서, Tencent Cloud 무선 네트워크는 보안 정책을 활성화하여 직원이 무선 네트워크에 로그인할 때 신원 인증이 필요합니다. 동시에 기업 IT 관리 백엔드는 무선 SSID 와 AP 를 검사하며, 불법 SSID 와 AP 가 발견되면 관련 IT 관리자에게 경보를 보내 처리하도록 합니다.	
⑦	금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 수립·운용하여야 한다.	패치 관리 측면에서 Tencent Cloud 는 최신 패치를 식별하고, 패치 설치 전 충분한 보안 테스트를 수행하여 패치 설치의 안전성을 보장합니다. Tencent Cloud 는 정기적으로 내부 각 비즈니스 팀에 패치 업그레이드 및 설치를 알리고, 엔드포인트 검사 도구를	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
16	악성코드 감염 방지대책	금융회사 또는 전자금융업자는 악성코드 감염·확산 방지, 피해 최소화 및 복구를 위한 대책을 수립·운영하여야 한다.	사용하여 패치 설치 상태를 정기적으로 스캔하며, 기한 내에 패치가 설치되지 않은 장치에 대해서는 자동으로 경보 작업 티켓을 생성합니다.
			고객은 악성 소프트웨어의 감염 및 전파를 방지하기 위한 조치를 수립·이행하여야 합니다. 고객은 Cloud Workload Protection Platform (CWPP)을 채택하여 클라우드 호스트에 보안 보호를 제공할 수 있습니다. CWPP 는 축적된 방대한 위협 데이터를 기반으로 머신러닝을 활용하여 고객에게 해킹 침입 탐지, 취약점 위험 경보 등 보안 보호 서비스를 제공하며, 비밀번호 해킹 차단, 비정상 로그인 알림, 트로이 목마 파일 탐지, 고위험 취약점 탐지 등 보안 기능을 포함하여 현재 서버가 직면한 주요 네트워크 보안 위협을 해결합니다.
			고객이 사고를 탐지하고 신속히 대응할 수 있도록 지원하기 위해, Tencent Cloud 는 일원화된 보안 관리 플랫폼인 Cloud Security Center (CSC)를 제공합니다. CSC 는 자산 센터, 위험 센터, 경보 센터, 고급 보안 관리 등의 기능을 통해 사전 위협 탐지, 사건 발생 시 대응 및 처리, 사후 추적 분석의 보안 운영 폐쇄 루프를 실현하도록 도와 보안 운영 효율성을 향상시킵니다. 고객의 규제 준수를 지원하기 위해 호스트 단말 보호 측면에서 Tencent Cloud 는 엔드포인트 탐지 및 대응(EDR) 도구를 배포하여 전체 네트워크 서버 단말 자산에 대한 포괄적인 모니터링 및 제어를 수행합니다. Tencent Cloud 가 사용하는 EDR 도구는 바이러스 백신 및 침입 탐지, 보안 기준선 및 취약점 스캔,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			그리고 명령 작업, 로그인 행위에 대한 보안 규정 준수 감사 등의 기능을 지원하며, 악성 프로그램이나 비정상적 행위를 식별할 때 경보를 발생시킵니다. Tencent Cloud 는 작업 티켓 시스템을 통해 경보 사건을 추적 및 처리합니다. 사무 단말 보호 측면에서 Tencent Cloud 는 내부적으로 소프트웨어 보안 규정을 수립하여 사무 단말(노트북 및 워크스테이션 포함)의 소프트웨어 사용 제한을 명확히 하고, 애플리케이션 허용 목록 기술을 활용하여 알려졌고 신뢰할 수 있는 프로그램만 실행하도록 허용하여 악성 소프트웨어 침입 위험을 줄입니다. Tencent Cloud 는 또한 제로 트러스트 보안 관리 시스템을 통해 사무 단말을 제어하며, 바이러스 제거, 취약점 수리, 사전 대응 방어 등의 보안 능력을 통해 랜섬웨어 방지, 피싱 공격 방지, 내부 횡적 이동 방지 등 포괄적인 보안 보호를 실현합니다.
17	홈페이지 등 공개용 웹서버 관리대책	금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운영하여야 한다. 1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ 구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것 2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 이중 인증수단을 적용할 것	고객은 공개 네트워크 서버와 내부 통신 네트워크 격리, 공개 네트워크 서버에 대한 접근 통제 및 이중 인증(2FA) 설정, 정보 유출 방지 조치 수립 및 적용 등 공개 네트워크 서버의 보안을 보장하기 위한 적절한 조치를 수립·이행하여야 합니다. 또한, 고객은 DMZ 구역에 이용자 정보 등 중요 정보를 저장·관리하지 않도록 제한하여야 합니다. 고객은 Tencent Cloud 가 제공하는 Virtual Private Cloud (VPC) 서비스를 이용하여 구매한 클라우드 플랫폼 자원에 대해 다수의 독립적인 네트워크 공간을 구축하고, 네트워크 세그먼트 분할 및 IP 주소 할당, 사용자 정의 라우팅 정책 등을 자유롭게 설정할 수 있습니다. VPC

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
3.	공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한하고, DMZ 구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 고유식별정보는 반드시 암호화하며 그 외 이용자 정보는 별도의 보안대책을 수립하여 저장·관리하여야 한다)	서비스는 Tencent Cloud 를 기반으로 구축된 전용 클라우드 네트워크 공간으로, 사설 네트워크는 터널링 기술을 활용하여 물리적 네트워크 상에 가상 네트워크를 구성하고 가상화 기술을 적용함으로써 서로 다른 사설 네트워크 간의 내부 네트워크를 완전히 격리시켜 고객에게 독립적이고 격리된 안전한 클라우드 네트워크를 제공합니다. 동시에, Tencent Cloud 는 Cloud Access Management (CAM) 를 통해 사설 네트워크 접근에 대한 권한 관리를 지원합니다. 예를 들어, 신원 관리 및 정책 관리를 통해 사용자의 사설 네트워크 접근 권한을 제어합니다.	또한, Cloud Firewall (CFW) 은 고객에게 서로 다른 네트워크 경계의 보호를 제공하여 클라우드 상의 접근 제어 통합 관리 및 로그 감사에 대한 보안 및 관리 요구사항을 해결합니다. 방화벽 ACL 능동적 제어, IPS 실시간 차단, 가상 패치 및 악성 코드 탐지를 지원하고, Tencent 위협 인텔리전스를 통합하여 호스트의 비정상적인 외부 연결을 실시간 차단함으로써 기존 네트워크의 DMZ 영역 요구를 충족시키고 핵심 자산에 대한 집중 보호를 실현하며, VPC 간의 세분화된 격리 관제를 가능하게 합니다.
4.	금융회사 또는 전자금융업자는 공개용 웹서버에 자료 게시 절차·내용에 관한 내부통제 방안과 개인정보 유출 및 위·변조를 방지하기 위한 보안조치 방안을 수립·운영하여야 한다.	또한, Cloud Firewall (CFW) 은 고객에게 서로 다른 네트워크 경계의 보호를 제공하여 클라우드 상의 접근 제어 통합 관리 및 로그 감사에 대한 보안 및 관리 요구사항을 해결합니다. 방화벽 ACL 능동적 제어, IPS 실시간 차단, 가상 패치 및 악성 코드 탐지를 지원하고, Tencent 위협 인텔리전스를 통합하여 호스트의 비정상적인 외부 연결을 실시간 차단함으로써 기존 네트워크의 DMZ 영역 요구를 충족시키고 핵심 자산에 대한 집중 보호를 실현하며, VPC 간의 세분화된 격리 관제를 가능하게 합니다.	Tencent Cloud 는 또한 엄격한 내부 네트워크 격리 규칙을 수립하여 물리적 및 논리적 격리 방식을 통해 Tencent Cloud 내부 업무 네트워크와 고객 데이터가 위치한 생산 환경을 완전히 격리시켰습니다.
			Tencent Cloud 는 또한 무단 접근을 방지하기 위해 생산 환경에 베스천 호스트(Bastion Host)를 전면 배포했습니다.
			더불어, Tencent Cloud 내부에는

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			네트워크 모니터링 시스템을 배포하여 라우터, 방화벽 및 네트워크 서버 등 네트워크 장비를 모니터링하고 경보를 발생시키며, 권한 통제, 승인 절차 등 다중 조치를 통해 비인가자의 내부 네트워크 자원 접근을 엄격히 금지하고 있습니다.
18	IP 주소 관리대책	금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP 주소"라 한다)의 안전한 사용을 위하여 주소 체계·할당·관리 등에 대한 내용을 포함한 적절한 대책을 수립·운영하고, 내부 IP 주소 및 외부 IP 주소의 인터넷 접속내용을 1 년 이상 별도로 기록·보관하여야 한다.	고객은 IP 주소의 안전한 사용을 보장하는 조치를 취하고, 내부 IP 주소와 외부 IP 주소의 인터넷 접속 현황을 각각 최소 1 년 이상 기록·저장하여야 합니다. 고객은 Tencent Cloud 가 제공하는 Virtual Private Cloud (VPC) 서비스를 이용하여 구매한 클라우드 플랫폼 자원에 대해 다수의 독립적인 네트워크 공간을 구축하고, 네트워크 세그먼트 분할 및 IP 주소 할당, 사용자 정의 라우팅 정책 등을 자유롭게 설정할 수 있습니다. VPC 서비스는 Tencent Cloud 를 기반으로 구축된 전용 클라우드 네트워크 공간으로, 사설 네트워크는 터널링 기술을 활용하여 물리적 네트워크 상에 가상 네트워크를 구성하고 가상화 기술을 적용함으로써 서로 다른 사설 네트워크 간의 내부 네트워크를 완전히 격리시켜 고객에게 독립적이고 격리된 안전한 클라우드 네트워크를 제공합니다. Tencent Cloud 는 IP 주소의 계획, 신청, 조회 및 변경 등을 위해 내부 IP 관리 시스템을 구축했습니다. 내부 및 외부망 IP 주소의 할당은 신청과 승인 절차를 거쳐야 하며, 네트워크 관리자가 통일하여 할당합니다. IP 관리 시스템을 통해 IP 주소 목록을 생성하고, 모든 내부 및 외부 IP 의 인터넷 접근 활동에 대해 접근 시간, 출발지 IP, 목적지 IP, 포트 등을 포함한 로그를 기록하여 보안 감사

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			요구사항을 충족시킵니다.
19	암호프로그램 및 키 관리 통제	① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다. ② 금융회사 또는 전자금융업자는 암호 및 인증시스템 등에 적용되는 키(Key)(프로그램 진위 및 무결성 확인에 사용되는 암호 또는 인증시스템 등에 적용되는 키를 포함한다)에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.	고객은 키 전체 생명주기 관리 관련 절차를 수립·이행하고, 암호화 프로그램의 원본 코드에 대한 접근을 제한하여야 합니다. Tencent Cloud 는 고객이 암호화 키의 전 생애 주기 관리를 구현할 수 있도록 돕기 위해 Key Management Service (KMS)을 제공합니다. 이를 통해 키가 안전한 방식으로 생성, 저장, 분배, 가져오기, 내보내기, 사용, 복구, 아카이빙 및 파기 등의 일련의 작업이 완료되어 키가 유출되지 않도록 보장합니다. 사용자 마스터 키(CMK)는 KMS 의 핵심 자원입니다. CMK 는 사용자의 1 급 키에 속하며, 주로 민감한 데이터의 암호화와 복호화에 사용됩니다. 사용자는 KMS 의 자동 생성 사용자 마스터 키 기능을 이용해 CMK 를 생성하거나, 자체 키를 가져와 CMK 를 구성할 수 있습니다. KMS 는 FIPS-140-2 인증을 받은 하드웨어 보안 모듈(HSM)을 사용하여 사용자 마스터 키를 보호합니다. 사용자 마스터 키 CMK 에는 사용자 키와 클라우드 제품 키 두 가지 유형이 있습니다. 사용자 키는 사용자가 콘솔 또는 API 를 통해 생성한 사용자 마스터 키입니다. 사용자는 사용자 키에 대해 생성, 활성화, 비활성화, 순환, 권한 제어 등의 작업을 수행할 수 있습니다. 클라우드 제품 키는 Tencent Cloud 제품/서비스가 키 관리 서비스를 호출할 때 자동으로 사용자를 위해 생성하는 CMK 입니다. 고객은 클라우드 제품 키에 대해 조회 및 키 순환 활성화 작업을 수행할 수 있습니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			CloudAudit 서비스는 키 관리 시스템 서비스의 관련 조작 이벤트를 기록할 수 있습니다. 고객은 클라우드 감사 콘솔에 로그인하여 관련 조작 기록을 확인할 수 있습니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 내부적으로 키 관리 메커니즘을 구축하고 관련 기준을 제정하여 키의 신청, 생성, 저장, 사용, 전달, 업데이트, 폐기 등 과정을 규범화합니다. 키 생명주기에 관련된 각 작업은 이중 통제, 엄밀한 인수인계, 적절한 보관, 적시 업데이트의 기본 요건을 준수하며, 권한 분리, 담당자 지정, 엄격한 승인, 상세한 기록, 실명 운영의 규정을 수립·이행하고, 사업 키 운영 로그를 보존하여 정기적으로 운영 감사를 실시합니다.
19-2	사용자 인증수단 관리	금융회사 또는 전자금융업자는 비밀번호, 생체정보 등 사용자 인증수단 유출을 방지하기 위하여 인증수단의 발급·보관·주기적 변경 및 인증오류 발생시 처리 절차 등을 포함한 관리방안을 수립·운용하여야 한다.	비밀번호 및 바이오인식 정보 등 사용자 인증 정보의 유출을 방지하기 위해, 고객은 인증 정보의 발급, 보관, 주기적 변경 및 인증 오류 시 처리 절차 등을 포함한 조치를 취하여야 합니다. 사용자 생체 인증 및 식별에 대해 Tencent Cloud 는 사용자에게 eKYC 을 제공합니다. eKYC 는 다양한 제품 우위를 갖추고 있어 고객에게 선도적이고 친절하며 포괄적이며 안전한 사용자 얼굴 정보 검증 서비스를 제공하여 고객의 다양한 얼굴 인증 요구를 충족시킵니다. eKYC 는 Tencent Cloud 의 다년간의 보안 경험과 선도적인 얼굴 공격 방지 알고리즘 역량을 결합하여, 정적 사진, 재촬영 동영상, 3D 마스크/머리 모델 등의 공격을 효과적으로 방어하여 고객이 신원 사기로 인한 손실을 줄일 수 있도록 합니다. 또한 Tencent Cloud 는 제품 테스트, 정기적인

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			취약성 스캔 및 전문 감사 등을 통해 eKYC 와 같은 클라우드 제품의 안전성을 보장합니다. 비밀번호 관리 측면에서 Tencent Cloud 고객은 사용자 계정 등록 시 등록 인터페이스를 통해 자체적으로 비밀번호를 설정합니다. Tencent Cloud 는 등록 인터페이스에서 비밀번호 길이, 복잡성 등의 요구사항을 포함한 비밀번호 정책을 제공하여 고객이 비밀번호 설정을 완료할 수 있도록 도와주며, 비밀번호가 고객이 입력한 이메일 주소와 동일하지 않도록 금지합니다. Tencent Cloud 계정 등록 인터페이스는 입력 오류 방지를 위해 고객이 설정한 비밀번호에 대한 재입력 확인을 요구합니다. 또한 Tencent Cloud 콘솔은 고객이 필요에 따라 로그인 보호 MFA 다중 요소 인증을 활성화할 수 있도록 지원하여 계정 보안 방어를 강화합니다. Tencent Cloud 는 또한 고객에게 Cloud Access Management (CAM)를 제공하여 고객이 Tencent Cloud 제품 및 자원에 대한 접근을 관리할 수 있도록 돕습니다. 여기서 사용자 마스터 계정은 서브 사용자를 생성하고 서브 사용자에게 신원 ID, 신원 증명 및 권한을 할당할 수 있습니다. 사용자는 접근 관리 콘솔을 통해 서브 사용자의 비밀번호 규칙(비밀번호 복잡성, 길이, 유효 기간 등 포함) 및 단일 로그인 세션 만료 시간을 수정할 수 있습니다. 비밀번호 유출을 방지하기 위해 Tencent Cloud 는 비밀번호에 SHA256 해시 암호화 및 소금 처리를 적용하여 평문 비밀번호 저장을 피합니다. 또한 Tencent Cloud 는 접근 통제 관리 규정을 수립하여 보안 기준에 따라

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			직원 계정 및 클라우드 고객 계정에 대한 비밀번호 정책(비밀번호 길이, 복잡성, 잠금 및 재설정 등 포함)을 설정합니다.

6.1.5 업무지속성 부문

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
23	비상대책 등의 수립·운영	① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립·준수하여야 한다. 1. 상황별 대응절차 2. 백업 또는 재해복구센터를 활용한 재해복구계획 3. 비상대응조직의 구성 및 운용 4. 입력대행, 수작업 등의 조건 및 절차 5. 모의훈련의 실시 6. 유관기관 및 관련업체와의 비상연락체제 구축 7. 보고 및 대외통보의 범위와 절차 등 8. 비상지원인력의 확보 및 운영 ③ 금융회사 또는 전자금융업자는 제 1 항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1 회 이상 점검하여 최신상태로 유지하고 관리하여야 한다. ④ 「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의	고객은 업무연속성 계획 및 비상 대응 관련 매뉴얼을 수립·준수하고, 매년 1 회 이상 업무연속성 확보 조치의 유효성을 점검하여야 합니다. 고객은 중앙처리장치, 데이터 저장 장치 등 주요 컴퓨터 장비에 이중화 또는 예비 장치를 설치하여야 합니다. 또한, 고객은 주 컴퓨팅 센터와 일정 거리 이상 떨어진 안전한 장소에 적정 규모와 인력을 갖춘 재해복구센터를 구축·운영하고, 매년 1 회 이상 전환 훈련을 실시하여야 합니다. Tencent Cloud 데이터 센터는 중국 본토, 아시아 태평양 지역, 북미 지역, 유럽 지역을 커버하며 지역(region)과 가용 영역(zone)으로 구성됩니다. Tencent Cloud의 서로 다른 지역 간은 완전히 격리되어 있으며, 각 지역은 다시 여러 개의 상호 격리된 가용 영역으로 구분됩니다. 현재 Tencent Cloud는 한국 내에 전력과 네트워크가 상호 독립된 두 개의 데이터 센터를 보유하고 있어, 고객이 한국 내에서 데이터를 저장, 처리 및 백업할 수 있도록 지원합니다. 고객은 비즈니스 발전 요구와 데이터 보안 요구에 따라 데이터와 시스템을 서로 다른 지역 또는 가용 영역에 자유롭게 배포 및 백업하여 비즈니스의 재해 복구 요구사항을 충족할 수 있습니다. 고객이 네트워크 보안 사건 발생 후

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립·준수하고 이를 금융위원회에 알려야 한다.	신속하게 대응하고 핵심 기능을 복구할 수 있도록 보장하기 위해, Tencent Cloud 가 제공하는 다양한 제품은 고가용성 특성을 갖추고 있어 고객이 시스템 또는 서비스의 고가용성을 실현하도록 돕습니다. 예를 들어:
⑤	금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운용하여야 한다.		• Cloud Load Balancer (CLB) 는 안전하고 빠른 4/7 계층 트래픽 분산 서비스를 제공하여, 트래픽 분산을 통해 애플리케이션 시스템의 외부 서비스 역량을 확장하고 단일 장애점을 제거합니다. CLB 는 클러스터 배포를 채택하며, 장애 인스턴스를 신속히 제거하여 고가용성을 실현합니다.
⑥	제 4 항에 따른 행동매뉴얼 또는 제 5 항에 따른 비상대책에는 제 1 항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.		• Cloud Virtual Machine (CVM) 은 서비스 고가용성과 데이터 고신뢰성의 특성을 갖추고 있습니다. CVM 에 탑재된 클라우드 디스크는 3 중 복사본 저장 전략을 제공하여 데이터가 어느 한 복사본에 장애가 발생할 경우 빠르게 데이터를 이전하고 복구할 수 있도록 보장합니다.
⑦	금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다.		• Cloud Object Storage (COS) 은 데이터의 다중 아키텍처, 다중 장치 간 중복 저장을 제공하여 사용자 데이터에 재해 복구 및 자원 격리 기능을 제공하여 데이터 지속성을 실현합니다.
⑧	다음 각 호의 금융회사 및 전자금융업자는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다.		• Cloud Native Database TDSQL-C: Tencent Cloud 의 자체 연구 개발 차세대 클라우드 네이티브 관계형 데이터베이스로서, 고가용성 클러스터 아키텍처를 채택하여 장애 노드를 자동 감지할 수 있으며, 초 단위 장애 전환 및 복구를 지원합니다.
⑨	제 8 항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3 시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24 시간 이내로 한다.		

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
	⑩	제 8 항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1 회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다.	• <u>TencentDB for MySQL</u> 은 데이터의 고신뢰성과 서비스의 고가용성을 실현하며, 완벽한 데이터 자동 백업 및 무손실 복구 메커니즘을 보유하고 있습니다. • <u>Tencent Kubernetes Engine (TKE)</u> 는 분산 서비스 아키텍처를 채택하여 서비스의 장애 자동 복구 및 빠른 이전을 보장합니다. 상태 유지 서비스 백엔드의 분산 저장과 결합하여 서비스와 데이터의 안전 및 고가용성을 실현합니다. 또한 Tencent Cloud 가 제공하는 다양한 저장 서비스 및 데이터베이스 서비스는 백업 기능을 갖추고 있으며, 다중 중복 백업, 이재 복구 등 요구사항을 지원합니다. Tencent Cloud 는 클라우드 제품 또는 서비스의 기능에 따라 고객에게 다중 저장 복사본 및 백업 서비스를 제공합니다. Tencent Cloud 는 자체 클라우드 컴퓨팅 환경에 적합한 비즈니스 연속성 관리 프레임워크를 설계 및 이행하여 포괄적인 비즈니스 연속성 관리 체계를 구축하고, 비즈니스 연속성 관리 규정을 수립하여 비즈니스 영향 분석, 비즈니스 연속성 계획, 비상 대응 및 재해 복구, 비상 훈련 및 테스트, 위기 관리 등을 포함하는 비즈니스 연속성 관리 관련 프로세스를 규정화했으며, 이미 ISO/IEC 22301 비즈니스 연속성 관리 체계의 국제 표준 인증을 획득했습니다. Tencent Cloud 는 클라우드 제품 및 서비스의 비즈니스 영향 분석 결과에 따라 서로 다른 대응 전략과 비즈니스 연속성 계획을 수립하고, 클라우드

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			제품 및 핵심 프로세스에 대해 상세한 재해 복구 계획을 수립했습니다. 관련 전략, 계획 및 계획은 장소, 인력, 장비, 시스템 및 정보 데이터 등 핵심 영역을 포괄하며, 비즈니스 우선순위에 따라 대응하는 재해 복구 프로세스를 수립하여 재해 복구 체계가 완전하고 질서 있으며 실행 가능하도록 보장합니다. Tencent Cloud는 요구사항에 따라 엄격히 정기 훈련을 수행하여 계획 등의 실행 가능성을 보장합니다. 고객 비즈니스의 지속적 가용성을 보장하기 위해 Tencent Cloud는 서버, 네트워크 장비, 보안 장비 등의 하드웨어 장비에 대해 중복 또는 핫 스탠바이 메커니즘을 설정하여 하드웨어 장애 발생 시 데이터가 손실되지 않고 비즈니스가 복구될 수 있도록 보장합니다. Tencent Cloud는 매년 자사의 비즈니스 연속성 관리 체계를 검토 및 업데이트하며, 비즈니스 영향 분석 결과에 따라 관련 제품 및 서비스의 비즈니스 연속성 계획과 재해 복구 계획을 검토하고 필요에 따라 업데이트합니다. 내부 비즈니스 연속성 관리 규정 요구에 기반하여 Tencent Cloud는 또한 비상 계획 연락처 목록을 유지 관리하고, 전담 인력을 지정하여 비상 계획 연락처 목록에 포함된 관련 당사자의 연락처 정보가 실제적이고 유효하도록 유지하는 책임을 집니다.
24	비상대응 훈련 실시	① 금융회사 또는 전자금융업자는 제 23 조제 4 항에 따른 행동매뉴얼 또는 같은 조 제 5 항에 따른 비상대책에 따라 연 1 회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제 23 조제 10 항에 따른	고객은 매년 비상 대응 계획 또는 매뉴얼에 따라 비상 대응 훈련을 1 회 실시하고, 그 결과를 금융서비스위원회에 보고하여야 합니다. 고객은 Tencent Cloud Smart Advisor 서비스를 활용하여 비즈니스 연속성

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		재해복구전환훈련을 포함하여 실시할 수 있다.	테스트의 계획 및 실행을 지원받을 수 있습니다. 이 서비스는 여러 ITOM 분야의 세부 애플리케이션을 위한 클라우드 통제 플랫폼으로, Tencent Cloud의 방대한 운영 전문가 경험을 기반으로 위험 점검, 장애 모의훈련 등 다양한 통제 최적화를 통해 클라우드 인프라를 개선합니다. 클라우드 어드바이저는 IaaS부터 PaaS까지 다양한 장애 유발 시나리오와 여러 업종별 훈련 경험 템플릿을 제공하여, 가용 영역 간 재해 복구 등 여러 전형적 애플리케이션 시나리오를 포괄함으로써 고객이 자체 비즈니스 요구에 따라 성숙된 솔루션을 신속하고 효율적으로 재사용하여 시스템 가용성을 높일 수 있도록 지원합니다.
②	금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다.		고객의 규제 지침 준수를 지원하기 위해 Tencent Cloud는 내부적으로 정기적으로 비상 대응 및 재해 복구 훈련과 테스트를 수행합니다. Tencent Cloud는 훈련 계획에 대한 위험 평가를 실시하여 훈련으로 인한 서비스 부정적 영향을 방지합니다. Tencent Cloud의 재해 복구 훈련은 일반적으로 실제와 유사한 전형적 재해 복구 시나리오(공격-방어 대응 및 대규모 장애 등 포함)를 모의하여 시스템의 재해 복구 능력, 대응 속도 및 복구 능력을 종합적으로 점검합니다. 훈련 종료 후 관련 부서는 훈련 보고서를 작성하고 개선 조치에 따라 시정을 진행하며, 보고서를 기록 보관합니다.
③	금융위원회는 제 2 항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다. 1. 「정부조직법」 제 17 조에 따른 "국가정보원(국가사이버안전센터)" 2. 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」 제 12 조에 따른 "경찰청(사이버수사국)" 3. 침해사고대응기관 4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관		적절한 경우 Tencent Cloud는 고객의 보안 훈련에 관련 기술 지원을 제공할
④	금융회사 또는 전자금융업자 ⁵ 는 제 1 항 및 제 2 항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.		

⁵ "전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」 제 3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			수도 있습니다.
25	정보처리 시스템의 성능관리	금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.	고객은 장애 예방 및 시스템 성능 최적화를 위해 정보처리시스템의 사용 현황 및 추이를 정기적으로 분석하여야 합니다. Tencent Cloud 가 고객에게 제공하는 클라우드 서비스는 각 서비스별로 약정된 서비스 수준 계약에 기반하여 제공되며, 각 서비스의 성능 지표, 측정 기준 및 보고 요구사항은 각 제품의 서비스 수준 계약에 명확히 기재되어 Tencent Cloud 공식 웹사이트에 게시됩니다. 각 클라우드 서비스의 성능과 가용성은 지속적으로 추적되며, 관련 지표는 관리 콘솔을 통해 고객이 실시간으로 모니터링할 수 있습니다. Tencent Cloud 는 또한 고객에게 Tencent Cloud Observability Platform (TCOP) 을 제공하여 클라우드 제품/서비스 모니터링을 지원합니다. TCOP 는 클라우드 서버, 클라우드 데이터베이스 등 클라우드 제품이 자체 보고하는 다양한 모니터링 지표와 고객이 사용자 정의 구성하여 보고하는 모니터링 지표를 수집 및 시각화 차트로 표시하여, 고객이 클라우드 제품 자원 사용률, 애플리케이션 성능 및 클라우드 제품 운영 상태를 실시간으로 파악할 수 있도록 돕습니다. Tencent Cloud 는 또한 고객을 위해 일원화된 보안 관리 플랫폼인 Cloud Security Center (CSC)를 제공하여, 클라우드 방화벽, 웹 애플리케이션 방화벽의 위협 경보 및 로그를 수집하고 Tencent Cloud 의 위협 인텔리전스, 자체 보안 지식 기반을 활용하여 데이터를 자동 분석 및 조사함으로써 고객에게 집중화된

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			위협 탐지, 조사, 대응 능력을 제공합니다.
34	전자금융 거래 시 준수사항	금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제 36 조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)	고객은 전화 등 거래 수단의 특수한 성질상 암호화가 불가능한 경우, 또는 조례상 면제가 인정되는 기타 경우를 제외하고, 전자금융거래에 대해 통신 암호화를 실시하여야 합니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스는 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 고객의 비즈니스에 포트 수준의 통신 보안을 보장합니다. Tencent Cloud는 데이터 보안 관리 기준선을 수립하여, 민감한 데이터 전송 시 사용해야 할 안전한 데이터 전송 프로토콜을 명확히 하고, 동시에 안전하지 않은 데이터 전송 프로토콜 사용을 금지하여 고객의 민감한 비즈니스 데이터가 전송 과정에서 안전성과 무결성을 유지하도록 보장합니다. 또한, 고객은 다음과 같은 Tencent Cloud 서비스를 사용하여 다양한 시나리오에서의 데이터 안전한 전송을 실현할 수 있습니다: • Direct Connect (DC): 전용성과 높은 보안성을 갖춘 대역폭 네트워크 연결을 제공합니다. 사용자가 네트워크 링크를 독점하여 데이터 유출 위험이 없습니다. • VPN Connection: 네트워크 터널링 기술을 기반으로, 온프레미스 데이터센터와 Tencent Cloud 상의 자원 간의 안전한 전송 연결을 실현합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			VPN 터널은 IKE(키 교환 프로토콜) 및 IPsec 을 사용하여 전송되는 데이터를 암호화하고, 인터넷 상에 안전하고 신뢰할 수 있는 데이터 터널을 구축하여 전송 과정 중 데이터의 안전을 보장합니다.

6.1.6 취약점 분석 및 사고 대응 등

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
37-2	전자금융기반시설의 취약점 분석·평가 주기, 내용 등	① 전자금융기반시설의 취약점 분석·평가는 총자산이 2 조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300 명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1 회 이상(홈페이지에 대해서는 6 개월에 1 회 이상) 실시하여야 한다. ② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5 인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100 분의 30 이상은 「정보보호산업의 진흥에 관한	고객은 금융거래 전자 네트워크에 대한 취약점 분석·평가를 최소 연 1 회(주요 사이트의 경우 최소 반기 1 회) 실시하여야 하며, 평가는 내부 전담 팀 또는 외부 평가 기관 등이 수행할 수 있습니다. 고객은 또한 평가 결과를 토대로 취약점을 제거하거나 시정/핵심 조치를 실시하기 위한 개선 계획을 수립·이행하여야 합니다. Tencent Cloud 는 고객에게 Vulnerability Scanning Service (VSS)를 제공하여 기업 네트워크 자산을 탐지하고 그 위험을 식별할 수 있도록 지원합니다. Tencent 의 다년간 축적된 보안 경험과 위협 인텔리전스를 기반으로, VSS 는 풍부하고 포괄적인 취약성 규칙 데이터베이스를 구축하였으며, 전문적이고 효율적인 0Day/1Day/NDay 취약성 탐지 능력을 보유하고 있습니다. 이를 통해 고객 자산의 가용성, 안전성 및 규정 준수 여부에 대해 정기적인 보안 스캔, 지속적인 위험 경고 및 취약성 탐지를 수행하여 고객에게 전문적인 수정 권고를 제공함으로써 보안 위험을 줄일 수 있습니다. VSS 는 또한

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		법률 시행규칙」 제 8 조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제 37 조의 3 제 1 항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다. ③ 제 1 항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1 회 이상(홈페이지에 대해서는 6 개월에 1 회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석·평가의 내용은 금융감독원장이 정한다. ④ 금융회사 및 전자금융업자는 해당 주기 내에 평가 대상 시설과 평가기간을 나누어 평가할 수 있다. ⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다. - 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행 - 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것 - 이행계획의 시행 결과는 최고경영자에게 보고할 것 ⑥ 금융회사 또는 전자금융업자는 제 1 항 또는	호스트 보안, 웹 애플리케이션 방화벽 등의 클라우드 제품과 연동을 지원하여 위험 모니터링부터 위험 처리까지의 폐쇄형 루프를 실현합니다. Tencent Cloud 는 또한 내부적으로 위험 및 취약성 관리 관련 절차를 구축하여, 정보 시스템에 직면한 위험과 취약점을 적시에 식별하고 개선 또는 패치하기 위한 조치를 취할 수 있도록 합니다. Tencent Cloud 는 취약점 스캔 시스템을 통해 정기적으로 스캔 작업을 생성하여 클라우드 환경 내 자산에 대한 취약점 스캔을 수행하고, 발견된 취약점을 분석, 분류 및 수정 처리합니다. 평가 결과 취약점이 고객의 비즈니스에 영향을 미칠 가능성이 있는 경우, 공식 웹사이트 공지 및 사이트 내 메시지를 통해 취약점 관련 정보를 고객에게 적시에 통지합니다. 통지 내용에는 취약점 설명, 영향 범위 및 정도, Tencent Cloud 가 취한 통제 조치, 고객을 위한 수정 권고 및 구체적인 조작 지침 등이 포함됩니다. Tencent Cloud 는 또한 외부 취약점 보고 플랫폼을 구축하고 "취약점 보상 프로그램"을 운영하여 업계 보안 전문가들을 초청하여 해커의 관점에서 Tencent Cloud 시스템의 보안 취약점과 위험을 발견하도록 돕고, 보안 문제를 적시에 수정하여 Tencent Cloud 의 생태계 보안을 유지합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		제 3 항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.	
37-4	침해사고 통지의 방법	금융회사 및 전자금융업자는 법 제 21 조의 5 에 따른 침해사고가 발생한 사실을 안 때에는 지체 없이 사고 내용, 사고에 따른 영향 등을 <별지 7 호 서식>에 기재하여 금융위원회에 보고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24 시간을 경과하여서는 아니된다.	고객은 전자 침해 행위로 인한 사고(전자금융기반시설의 교란 및 마비 등)가 발생하였음을 인지한 때에는 24 시간 이내에 규정된 서식에 따라 금융서비스위원회에 사고 내용 및 사고 영향을 보고하여야 합니다. 고객이 커뮤니케이션 및 고지 의무를 효과적으로 이행할 수 있도록 지원하기 위해 Tencent Cloud 는 정보 보안 사건 대응, 사건 에스컬레이션, 사건 통지 등의 관련 절차를 구축하여 사고의 영향을 받을 수 있거나 이미 받은 회사 내부 인원 및 고객 등 이해관계자들에게 적시에 경보 또는 통지를 제공하고, 모든 당사자가 질서 있고 적시에 효율적으로 소통과 협업을 할 수 있도록 합니다. 고객에게 영향을 미칠 수 있는 보안 사건의 경우 Tencent Cloud 는 정보 보안 사건의 영향 범위와 정도에 따라 내부 검토를 거친 후, 적절한 방법으로 고객에게 정보 보안 사건 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.
37-5	정보기술부문 및 전자금융 사고보고	① 금융회사 및 전자금융업자는 정보기술부문 및 전자금융과 관련된 사고에 관하여 다음 각 호를 준수하여야 한다. 1. 사고의 유형 분류, 처리단계, 조치방법, 영향도 및 심각도 평가 방법 등이 포함된 절차를 마련·운영. 2. 금융감독원장이 정하는	고객은 사고 대응, 분류, 평가 및 처리 관련 절차를 수립·이행하고, 금융감독원이 정의한 사고가 발생한 경우 즉시 금융감독원에 보고하여야 합니다. Tencent Cloud 는 정보 보안 사건 관리 규정을 수립하고, 정보 보안 보고, 대응 및 처리 메커니즘과 관련 절차를 마련하였으며, 사건 처리 절차에서 각 팀의 역할과 구체적인

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		사고가 발생한 경우에는 지체없이 금융감독원장에게 보고 ② 금융회사 및 전자금융업자는 제 1 항제 2 호에 따른 사고보고를 고의로 지연하거나 숨긴 자에 대하여 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다. ③ 금융감독원장은 제 1 항제 2 호에 따라 보고 받은 내용을 지체 없이 금융위원장에게 보고하여야 한다. ④ 제 1 항제 2 호의 사고보고와 관련하여 사고보고 대상, 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.	책임을 명확히 하였습니다. Tencent Cloud 는 내부 보안 운영 시스템을 사용하여 보안 사건을 기록합니다. 탐지 및 식별된 보안 사건에 대해 Tencent Cloud 는 사건의 성격, 데이터 민감도, 영향 범위 등의 요소를 고려하여 보안 사건을 분석 및 등급 분류하고, 적시에 해당 책임자에게 알려 사건을 추적 처리하도록 합니다. Tencent Cloud 보안팀은 7*24 시간 운영되는 보안 운영 체계를 기반으로 취약점 모니터링, 침입 추적, 공격 차단 등의 핵심 시나리오에 집중하여, 보안 경보에 실시간으로 대응하고 공격 추적 및 비상 대응 계획을 신속히 수립함으로써 보안 사건의 확산을 효과적으로 억제합니다. 고객에게 영향을 미칠 수 있는 보안 사건의 경우 Tencent Cloud 는 정보 보안 사건의 영향 범위와 정도에 따라 내부 검토를 거친 후, 적절한 방법으로 고객에게 정보 보안 사건 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.
37-6	침해사고대응기관 지정 및 업무범위 등	① 침해사고에 대응하기 위한 침해사고대응기관은 다음 각 호의 자로 한다. 1. 금융보안원 2. 삭제 3. 금융위원장이 지정한 자 ⑤ 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 연 1 회 이상 침해사고 대응 및 복구훈련 계획을 수립·시행하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게	고객은 매년 1 회 이상 침해사고 대응 및 복구 훈련 계획을 수립·이행하고, 계획 및 결과를 침해사고 대응 기관(금융감독원 등)에 제출하여야 합니다. 또한, 고객은 침해사고 대응 기관의 사고 대응 복구 및 교육 결과 점검에 협조하고, 지침에 따라 개선을 실시하여야 합니다. 고객은 Tencent Cloud Smart Advisor 서비스를 활용하여 비즈니스 연속성 테스트의 계획 및 실행을 지원받을 수 있습니다. 이 서비스는 여러 ITOM 분야의 세부 애플리케이션을 위한 클라우드 통제 플랫폼으로, Tencent Cloud 의 방대한 운영 전문가 경험을

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		제출하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다.	기반으로 위험 점검, 장애 모의훈련 등 다양한 통제 최적화를 통해 클라우드 인프라를 개선합니다.
		1. 법 제 2 조제 3 호가목의 금융회사 중 신용협동조합	클라우드 어드바이저는 IaaS 부터 PaaS 까지 다양한 장애 유발 시나리오와 여러 업종별 훈련 경험 템플릿을 제공하여, 가용 영역 간 재해 복구 등 여러 전형적 애플리케이션 시나리오를 포괄함으로써 고객이 자체 비즈니스 요구에 따라 성숙된 솔루션을 신속하고 효율적으로 재사용하여 시스템 가용성을 높일 수 있도록 지원합니다.
		2. 법 제 2 조제 3 호다목·라목의 금융회사	
		3. 시행령 제 2 조제 4 호부터 제 6 호까지의 조합	
		4. 시행령 제 5 조제 2 항의 요건을 충족한 금융회사	
			고객의 규제 준수를 지원하기 위해 고객의 규제 지침 준수를 지원하기 위해 Tencent Cloud는 내부적으로 정기적으로 비상 대응 및 재해 복구 훈련과 테스트를 수행합니다. Tencent Cloud는 훈련 계획에 대한 위험 평가를 실시하여 훈련으로 인한 서비스 부정적 영향을 방지합니다. Tencent Cloud의 재해 복구 훈련은 일반적으로 실제와 유사한 전형적 재해 복구 시나리오(공격-방어 대응 및 대규모 장애 등 포함)를 모의하여 시스템의 재해 복구 능력, 대응 속도 및 복구 능력을 종합적으로 점검합니다. 훈련 종료 후 관련 부서는 훈련 보고서를 작성하고 개선 조치에 따라 시정을 진행하며, 보고서를 기록 보관합니다.
			적절한 경우 Tencent Cloud는 고객의 보안 훈련에 관련 기술 지원을 제공할 수도 있습니다.

6.2 허가 및 등록의 세부요건

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
50	인력 및 물적 시설 세부요건	① 법 제 28 조 및 제 29 조에 따라 허가를 받거나 등록을 하고자 하는 자는 인력과 물적 시설에 대한 다음 각 호의 요건을 모두 갖추어야 한다. 1. 신청 당시 전산업무 종사 경력이 2 년 이상인 임직원을 5 명 이상 확보하고 있거나 허가·등록 시점에 확보 가능할 것 2. 전자금융업을 원활히 영위하는데 필요한 전산기기를 갖출 것 3. 전산장애 발생 시 전산자료 손실에 대비한 백업(backup)장치를 구비할 것 4. 전자금융업의 원활한 영위를 위한 각종 프로그램을 갖출 것 5. 전산자료 보호 등을 위한 적절한 정보처리시스템⁶ 관리방안을 확보하고 정보보호시스템 등 감시운영체제를 구축할 것 6. 전산실 등의 구조 및 내장, 설비 등의 안전성을 확보하고 적절한 보안대책을 수립할 것	허가 취득을 위해, 고객은 인력 배치, 컴퓨터 장비, 백업 메커니즘, 정보보안 및 모니터링 관련 시스템, 기계실 보안성 등 측면이 감독 요건을 충족하도록 보장하여야 합니다. 정보 자산의 모니터링과 분석을 위해, Tencent Cloud 는 또한 고객에게 Tencent Cloud Observability Platform (TCOP) 을 제공하여 클라우드 제품/서비스 모니터링을 지원합니다. TCOP 는 클라우드 서버, 클라우드 데이터베이스 등 클라우드 제품이 자체 보고하는 다양한 모니터링 지표와 고객이 사용자 정의 구성하여 보고하는 모니터링 지표를 수집 및 시각화 차트로 표시하여, 고객이 클라우드 제품 자원 사용률, 애플리케이션 성능 및 클라우드 제품 운영 상태를 실시간으로 파악할 수 있도록 돕습니다. Tencent Cloud 는 또한 고객을 위해 일원화된 보안 관리 플랫폼인 Cloud Security Center (CSC)를 제공하여, 클라우드 방화벽, 웹 애플리케이션 방화벽의 위험 경보 및 로그를 수집하고 Tencent Cloud 의 위협 인텔리전스, 자체 보안 지식 기반을 활용하여 데이터를 자동 분석 및 조사함으로써 고객에게 집중화된 위협 탐지, 조사, 대응 능력을 제공합니다. 해 복구 및 백업 측면에서 Tencent Cloud 는 자체 클라우드 컴퓨팅 환경에 적합한 비즈니스 연속성 관리 프레임워크를 설계 및 시행하고, 포괄적인 비즈니스 연속성 관리 체계를 구축하여 ISO/IEC 22301 비즈니스 연속성 관리 체계의 국제 표준 인증을 획득하였습니다. Tencent Cloud 데이터 센터는 중국 본토, 아시아 태평양 지역, 북미 지역, 유럽

⁶ "정보보호시스템"이라 함은 정보처리시스템내 정보를 유출·위변조·훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램을 말한다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			지역을 커버하며 지역(region)과 가용 영역(zone)으로 구성됩니다. Tencent Cloud의 서로 다른 지역 간은 완전히 격리되어 있으며, 각 지역은 다시 여러 개의 상호 격리된 가용 영역으로 구분됩니다. 고객은 비즈니스 발전 요구와 데이터 보안 요구에 따라 데이터와 시스템을 서로 다른 지역 또는 가용 영역에 자유롭게 배포 및 백업하여 비즈니스의 재해 복구 요구사항을 충족할 수 있습니다. 고객 비즈니스의 지속적인 가용성을 보장하기 위해 Tencent Cloud는 클라우드 제품이 단일 지역 내에서 여러 데이터 센터를 활용한 다중화 메커니즘을 적용하도록 요구합니다. 고객 비즈니스의 지속적 가용성을 보장하기 위해 Tencent Cloud는 서버, 네트워크 장비, 보안 장비 등의 하드웨어 장비에 대해 중복 또는 핫 스탠바이 메커니즘을 설정하여 하드웨어 장애 발생 시 데이터가 손실되지 않고 비즈니스가 복구될 수 있도록 보장합니다. Tencent Cloud에서 제공하는 다양한 저장 서비스와 데이터베이스 서비스는 모두 백업 기능을 갖추고 있어 고객의 다양한 백업 요구를 충족시킵니다. 예를 들어: • 고객이 Cloud Object Storage (COS)에 저장한 데이터는 교차 리전 복제 기능을 통해 여러 지정된 리전에 동시에 저장될 수 있어, 예기치 않게 일부 데이터가 손실된 경우에도 중복 데이터를 통해 완전한 데이터를 찾아 복구할 수 있으며, 하나의 가용 구역 저장소가 불가항력적인 재해로 손상을 입을 경우 발생할 수 있는 손실을 방지하여 다중 중복 백업과 재해 복구 효과를 달성할 수 있습니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			• <u>Cloud Block Storage (CBS)</u>의 스냅샷 백업 기능은 CBS의 특정 시점 스냅샷을 생성하여 데이터를 백업함으로써 변조 및 실수로 인한 삭제로 인한 데이터 손실을 방지하고, 비즈니스 장애 시 신속한 롤백이 가능하도록 보장합니다. • <u>Cloud File Storage (CFS)</u>은 정기적인 스냅샷 기능을 제공하여 고객이 유연하게 백업 작업 전략을 설정할 수 있도록 하며, 서로 다른 비즈니스에 대해 서로 다른 정기 스냅샷 전략을 채택할 것을 권장합니다. • <u>Cloud Native Database TDSQL-C</u>는 논리적 백업과 스냅샷 백업 두 가지 백업 유형을 지원하며, 완전한 데이터 백업과 이후 일정 기간 동안의 binlog 백업을 통해 전체 TDSQL-C MySQL 클러스터나 특정 데이터베이스/테이블을 임의의 시점으로 복구할 수 있습니다. • <u>TencentDB for MySQL</u>은 데이터베이스를 백업하기 위한 자동 백업과 수동 백업 두 가지 방식을 지원하며, 교차 리전 백업 기능을 제공하여 고객의 재해 복구 능력을 향상시키고 동시에 데이터의 신뢰성을 높입니다. • <u>TencentDB for MongoDB</u>는 데이터의 자동 백업과 무손실 복구 메커니즘을 제공하며, 다중 노드 백업 데이터를 지원합니다. 고객은 백업 메커니즘을 통해 여러 날 동안의 백업 데이터를 저장하여 재해 상황 시 데이터 복구를 용이하게 할 수 있습니다. 물리적 환경 보안 측면에서, Tencent Cloud는 물리적 보안 관리 제도를 수립하여 운영 안전을 규제하고, 위험을

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			적시에 식별하며, 물리적 보안 관리를 강화하고 있습니다. Tencent Cloud는 전 세계의 각 데이터센터를 관련 국제 표준 및 현지 안전 요구사항에 따라 입지 선정, 건설 또는 임대하여 환경적 위험을 충분히 고려하고 높은 확률의 환경 위험 지역을 피합니다. 현재 Tencent Cloud는 한국에 두 개의 임대형 데이터센터를 구축했습니다. 데이터센터의 탄력성과 안전성을 보장하기 위해 Tencent Cloud는 데이터 공급업체 선정, 계약상의 제약부터 지속적인 감독에 이르기까지 전 과정에 걸쳐 엄격한 관리 체계를 구축했습니다. Tencent Cloud는 매년 정기적으로 실시하는 내부 및 외부 감사를 통해 운영사 데이터센터에 대한 현장 점검을 수행하여 운영사 데이터센터가 Tencent Cloud가 규정한 정보 보안 요구사항을 준수하는지 확인합니다. Tencent Cloud는 운영사에 데이터센터에 연기 감지기, 피뢰 및 접지 장치, 화재 경보기 및 스프링클러 시스템, 전력 공급 시스템, 분기 회로 시스템, 신선 공기 시스템, 공조 시스템, 온도 감지 장치 등을 설치하도록 요구하며, 인력을 배치하여 24시간 유지보수를 수행하고 장비 장애의 신속한 해결을 지원하도록 합니다. 또한 Tencent Cloud는 데이터센터 운영사에 물리적 보안 비상 계획을 수립하고, 정기적으로 데이터센터 직원에 대한 안전 훈련을 조직하도록 요구합니다. 보안 및 모니터링 측면에서 Tencent Cloud는 운영사에 보안 요원을 배치하여 엄격히 점검 목록과 점검 계획에 따라 각 기기실 및 장비 상황을 순찰하며, 각 검사 지점에서 서명 및 점검 시간을 기록하도록 요구하고, 기반 시설 장애나 보안 사건이 발견될 경우 즉시

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			데이터센터 비상 사건 대응 절차를 가동하도록 합니다. Tencent Cloud는 또한 운영사에 데이터센터에 7*24 시간 사각지대 없는 비디오 모니터링 경보 시스템을 설치하고, 보안실에서 이를 감시하며, 모니터링 기록을 안전하게 저장하고 충분한 시간 동안 보관하도록 요구합니다.

6.3 전자금융업무의 감독

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
60	외부주문등에 대한 기준	① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. - 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영 - 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지 - 계좌번호, 비밀번호 등 이용자 금융정보 무단보관 및 유출 금지 - 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립 - 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용	고객은 전자금융거래를 외주·위탁할 때, 외주 정보처리시스템 개발 관련 사업장 및 컴퓨터 장비를 내부 사업과 분리, 위변조 방지 및 정보 유출 방지 등 보안 조치 수립, 전자금융 보조 사업자와의 전용 회선 연결, 백업 및 비상 대책 수립, 전자금융 보조 사업자에 대한 지속적 평가, 외주 업체의 무단 재위탁 금지 등 일련의 규범을 준수하여야 합니다. 클라우드 서비스 제공업체로서 Tencent Cloud는 국제 사이트 공식 웹사이트에 온라인 본서비스 General Service Level Agreement 데이터 개인정보 보호 및 보안 계약 등 법적 문서를 제공하여, Tencent Cloud가 제공하는 서비스 내용 및 서비스 수준, 사용자 데이터 및 지식 재산권 보호, 고객과 Tencent Cloud 양측의 보안 책임과 의무, 서비스 기간 및 계약 종료 시나리오, 분쟁 해결 메커니즘, 통지 메커니즘 등을 명확히 합니다. 고객은 또한 오프라인 계약을 Tencent Cloud와 체결하여 계약 내 조항 및 세부사항을 협의할 수 있습니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
6.	정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립	정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립	하도급 처리에 대해 , 계약에는 하도급 사전 동의, 하도급업체 추가 또는 변경 전 통지, 데이터 보호 의무 등 조항이 명시되어 있습니다. 고객의 사전 동의 없이 Tencent Cloud 는 계약/합의에 따라 고객을 대행하여 수행하는 어떠한 처리 작업도 하도급하지 않습니다. 하도급 처리 업체 추가 또는 변경과 관련된 예정된 변경사항은 Tencent Cloud 가 이메일 등의 채널을 통해 고객에게 통지합니다.
7.	외부주문등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것	외부주문등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것	하도급업체 관리 측면에서 Tencent Cloud 는 완비된 공급망 보안 관리 체계를 구축하여, 엄격한 공급업체 보안 평가 및 자격 심사, 정기적인 감독 및 평가, 명확한 아웃소싱 서비스 계약 등의 조치를 통해 공급업체를 효과적으로 통제하고, 하도급이 Tencent Cloud 의 고객에 대한 관련 서비스 제공 능력 및 고객 정보 처리 과정의 기밀성과 무결성에 영향을 미치지 않도록 보장합니다.
8.	업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립	업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립	고객 데이터 보호 측면에서 고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. 서비스 제공 또는 문제 해결의 필요성이 있고, 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 부처의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 상황이 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 직접 접촉하지 않습니다.
9.	정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립·운용하고, 통제는 제 8 조제 1 항제 2 호의 조직에서 수행	정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립·운용하고, 통제는 제 8 조제 1 항제 2 호의 조직에서 수행	Tencent Cloud 는 접근 통제 및 권한 관리, 직원과의 기밀 유지 계약 체결, 데이터 유출 방지 도구 배포 등의 조치를 통해 고객 데이터를 보호합니다.
10.	전자금융보조업자에 대한 재무건전성을 연 1 회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시	전자금융보조업자에 대한 재무건전성을 연 1 회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시	고객의 데이터 저장 보호를 지원하기
11.	전자금융보조업자가 제공하는 서비스의 품질수준을 연 1 회 이상 평가할 것	전자금융보조업자가 제공하는 서비스의 품질수준을 연 1 회 이상 평가할 것	
12.	전자금융보조업자가 사전 동의 없이 다시 외부주문등 계약을 체결하거나 계약업체를 변경하지 못하도록 하고, 사전 동의시 해당 계약서에 제 7 호의 사항을 기재하도록 통제	전자금융보조업자가 사전 동의 없이 다시 외부주문등 계약을 체결하거나 계약업체를 변경하지 못하도록 하고, 사전 동의시 해당 계약서에 제 7 호의 사항을 기재하도록 통제	
13.	업무수행인력에 대하여 사전 신원조회 실시(이 경우 신원보증보험 증권 징구로 갈음할 수 있다) 또는 대표자의 신원보증서 징구, 인력변경시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안	업무수행인력에 대하여 사전 신원조회 실시(이 경우 신원보증보험 증권 징구로 갈음할 수 있다) 또는 대표자의 신원보증서 징구, 인력변경시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
	수립		위해 Tencent Cloud 의 여러 저장 및 데이터베이스 제품은 데이터 암호화 기능을 지원하고, 안전한 고강도 암호화 알고리즘을 사용하며, Key Management Service (KMS) 통합을 통해 키 전 생애 주기 관리를 구현하여 데이터의 기밀성을 보장합니다.
14.	외부주문등은 자체 보안성검토 및 정기(금융감독원장이 정하는 중요 점검사항에 대해서는 매일) 보안점검 실시		데이터 전송 보호 측면에서, 고객의 Tencent Cloud 콘솔 상의 모든 통신은 HTTPS 보안 프로토콜의 암호화 보호를 받습니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스는 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 고객의 비즈니스에 포트 수준의 통신 보안을 제공합니다. 또한, 고객은 다음과 같은 Tencent Cloud 서비스를 사용하여 다양한 시나리오에서의 데이터 안전한 전송을 실현할 수 있습니다:
②	금융회사 또는 전자금융업자는 제 1 항제 10 호 및 제 11 호의 평가결과를 금융감독원장에게 보고하여야 한다.		• Direct Connect (DC): 전용성과 높은 보안성을 갖춘 대역폭 네트워크 연결을 제공합니다. 사용자가 네트워크 링크를 독점하여 데이터 유출 위험이 없습니다. • VPN Connection: 네트워크 터널링 기술을 기반으로, 온프레미스 데이터센터와 Tencent Cloud 상의 자원 간의 안전한 전송 연결을 실현합니다. VPN 터널은 IKE(키 교환 프로토콜) 및 IPsec 을 사용하여 전송되는 데이터를 암호화하고, 인터넷 상에 안전하고 신뢰할 수 있는 데이터 터널을 구축하여 전송 과정 중 데이터의 안전을 보장합니다.
			고객의 비즈니스가 지속적이고 안정적으로 이용 가능하도록 보장하기

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			위해, Tencent Cloud 는 전 세계 여러 지역에서 관련 국제 표준과 현지 안전 요구사항에 따라 데이터 센터를 건설하거나 임대하여 고객에게 다중 지역(Region) 및 다중 가용 구역(Availability Zone) 선택권을 제공함으로써, 비즈니스의 재해 복구 요구사항과 서비스 수준을 충족시킵니다. Tencent Cloud 가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 스토리지 서비스, 데이터베이스 서비스, 컨테이너 및 미들웨어 서비스, 보안 서비스 등 다양한 클라우드 제품/서비스는 모두 고가용성 특성을 갖추고 있으며, 이에 상응하는 재해 복구 및 복원 계획을 마련하고 있습니다. 고객의 백업 전략 구현을 지원하기 위해 Tencent Cloud 는 클라우드 제품 또는 서비스의 기능에 따라 고객에게 다중 스토리지 복사본 및 백업 서비스를 제공하며, 제품 서비스 수준 계약(Service Level Agreement, SLA)에 따른 책임을 다합니다. Tencent Cloud 가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 스토리지 서비스, 데이터베이스 서비스, 컨테이너 및 미들웨어 서비스 등 다양한 클라우드 제품/서비스는 고객이 자체 시스템 및 데이터의 백업 전략을 구성할 수 있도록 지원하여 고객의 다양한 백업 요구를 충족시킵니다. 고객의 아웃소싱 평가 및 검사 요구사항에 부합하기 위해, Tencent Cloud 는 전담 인력을 배치하여 고객이 시작한 감사 또는 검토 활동에 적극적으로 대응할 수 있습니다. Tencent Cloud 는 매년 독립된 제 3 기관의 전문 감사를 받으며, 검증보고서 성격의 시스템 및 조직 통제 보고서를 제공하여 클라우드

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			이용 기관, 독립 감사인, 규제 기관, 회사 주주 및 기타 이해관계자에게 Tencent Cloud 서비스 조직의 최신 내부 통제 현황을 투명하게 공개하고 있습니다. 비즈니스 수행 인력 관리에 대해, Tencent Cloud 는 내부적으로 완비된 인적 자원 관리 기준과 절차를 수립하여 직무 요구사항에 맞춰 인력을 채용 및 배치합니다. 채용 과정에서 Tencent Cloud 는 후보 직원에 대한 심사를 실시하여, 그들의 성실성 상태, 직업 자격, 이력 및 규정 준수 위험을 평가하여 직무 요구사항과 회사의 보안 관리 기준에 부합하는지 확인합니다.

6.4 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가기준

"<별표 2 의 2> 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가기준"에는 금융회사 또는 전자금융업자가 제 14 조의 2 제 1 항 제 2 호에 따라 클라우드 서비스 제공자의 안전성을 평가하는 기준이 포함되어 있으며, 이는 "필수" 기준과 "대체" 기준으로 구분됩니다. 본 규정에 따르면, 관련 업무가 제 14 조의 2 제 1 항 제 1 호에 따라 비중요 업무로 분류되거나, 클라우드 서비스 제공자가 한국 내외 클라우드 서비스 관련 보안 인증 등을 지속적으로 유지하고 있음을 확인한 경우에는 "대체" 항목에 대한 평가를 생략할 수 있습니다.

한국의 경우, Tencent Cloud 는 한국 정보보호 관리체계(K-ISMS) 인증을 획득했으며, 매년 정기적으로 KISA 의 감사를 받습니다. Tencent Cloud 의 인증 자격 획득에 대한 자세한 내용은 본 가이드 [제 2 장 Tencent Cloud 보안 및 프라이버시 컴플라이언스](#)를 참조하시기 바랍니다.

본 장에서는 Tencent Cloud 가 클라우드 서비스 제공자로서 관련 기준 요구사항을 어떻게 준수하는지 설명합니다.

6.4.1 정보보호 정책 및 법규 준수

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
1.1	정보보호 정책	1.1.1. 【대 체】 조직 전반에 적용하고 있는 정보보호 정책 및 지침 또는 규정을 수립·시행하고 있는가? 1.1.2. 【대 체】 정기적으로 정보보호정책의 타당성을 검토, 평가하여 수정, 보완하기 위한 절차를 마련하고 이행하고 있는가?	Tencent Cloud는 정보 보안 관리 정책을 수립하였으며, 이는 정보 보안 종합 전략, 보안 조직 구조 및 보안 관리 체계로 구성되어 클라우드 플랫폼의 안전한 운영과 위험 관리를 효과적으로 지원합니다. Tencent Cloud의 정보 보안 정책은 매년 정기적으로 검토되어 클라우드 보안 관리 체계의 통제 목표, 통제 절차 및 통제 조치가 관련 보안 전략, 표준, 절차 및 법적 요구사항에 부합하는지 확인하며, 정보 보안 정책의 적절성과 유효성을 보장합니다. Tencent Cloud는 또한 수용 가능한 사용 정책을 수립하여 직원 및 제 3자가 Tencent Cloud 회사 자원(IT 시스템, 네트워크, 장비, 데이터 등을 포함하되 이에 국한되지 않음)을 사용할 때의 책임과 의무를 명확히 하고, 합리적인 사용 행위를 규정하며 잠재적 위험을 방지합니다. Tencent Cloud는 ISO/IEC 27001 정보 보안 관리 체계, ISO/IEC 27017 클라우드 서비스 정보 보안 관리 체계, ISO/IEC 22301 업무 연속성 관리 체계, ISO/IEC 20000 정보 기술 서비스 관리 체계 등의 국제 보안 관련 표준 인증을 획득하였습니다. 정기적인 검토 및 평가 측면에서, Tencent Cloud 보안팀은 매년 최소 한 차례 이상 내부 보안 감사를 실시하며, 클라우드 플랫폼 및 내부 시스템의 상황을 지속적으로 모니터링하여 양호한 보안 태세를 유지하고 관련 법률 규정 및 보안 관리 표준의 규정과 요구사항을 준수하도록 합니다. Tencent Cloud는 매년 독립된 제 3기관의 전문 감사를 받으며, 검증보고서 성격의 시스템 및 조직 통제 보고서를 제공하여 클라우드 이용 기관, 독립 감사인, 규제 기관, 회사 주주 및 기타 이해관계자에게 Tencent Cloud 서비스 조직의 최신 내부 통제 현황을 투명하게 공개하고 있습니다. 한국의 경우, Tencent Cloud는 한국

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			정보보호 관리체계(K-ISMS) 인증을 획득했으며, 매년 정기적으로 KISA의 감사를 받습니다.
1.2	정보보호 조직	1.2.1 【대체】조직의 정보보호를 위한 전담조직을 구성하여 안전성 확보 및 이용자 보호 등 정보보호 활동을 효과적으로 수행하고 있는가? 1.2.2 【대체】정보 보안 및 정보자산과 관련된 모든 인력의 역할과 책임을 정의하고, 이용자의 정보보호 역할과 책임을 명확하게 정의하고 있는가?	정보 보안 관리 조직 구조 측면에서 Tencent Cloud는 클라우드 보안 및 정보 보안 관련 조직 구조를 구축하여 각 계층의 보안 기능 역할과 관련 책임을 명확히 하고, 정보 보안 감사 및 정보 보안 위험 평가 등 작업 메커니즘을 정의했습니다. Tencent는 보안 기술 위원회와 다양한 기능 및 분야별 전문 보안 팀을 설립했으며, 내부적으로 완비된 인적 자원 관리 기준과 절차를 구축하여 직무 요구사항에 따라 인력을 채용 및 배치하도록 하고 있습니다. Tencent Cloud는 업계의 베테랑 전문가 서비스 팀을 결집하여 고객에게 안전하고 신뢰할 수 있으며 전문적이고 규정을 준수하는 제품과 서비스를 제공하기 위해 노력하고 있습니다.
1.3	법 및 정책 준수	1.3.1 【필수】이용자가 법령 등 의무준수를 위해 필요한 사항을 지원 및 협조하도록 체계가 마련되어 있는가?	Tencent Cloud는 사업을 운영하는 관할 구역의 법률 및 규정을 엄격히 준수하며, 진보된 국제 및 업계 보안 표준을 식별 및 채택하고, 보안 및 규정 준수 관련 절차를 수립하여 Tencent Cloud의 보안 및 규정 준수 수준을 향상시키고 고객이 신뢰할 수 있는 클라우드 서비스를 구축했습니다. 현재까지 Tencent Cloud는 제3자 독립 감사 또는 평가 방식을 통해 다수의 보안 및 개인정보 보호 규정 준수 인증 또는 자격을 취득하여, Tencent Cloud의 보안 관리 및 개인정보 보호 구축이 관련 인증 기준 또는 업계 모범 사례를 충족함을 입증했습니다. Tencent Cloud의 규정 준수 정보에 대해 더 자세히 알아보려면 Tencent Cloud Compliance 페이지를 참조하십시오. 관련 규정 준수 인증서나 보고서가 필요한 경우,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			Compliance Document Center 를 통해 신청하여 다운로드하십시오.
1.4	보안감사	1.4.1【필수】접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할수 있는 보안감사 증적(로그)은 식별할 수있는 형태로 기록 및 모니터링 되고, 비인가 된 접근 및 변조로부터 보호되고있는가?	Tencent Cloud는 CloudAudit를 제공하여 Tencent Cloud 계정 활동에 대한 감독, 규정 준수 점검, 작업 검토 및 위험 검토를 수행합니다. CloudAudit을 통해 고객은 특정 기간 내 Tencent Cloud 계정에서 발생한 변경 사항의 포괄적인 이력 기록을 수집하여 보안 및 운영 문제를 발견하고 해결할 수 있습니다. Cloud Log Service (CLS)는 일원화된 로그 서비스 플랫폼으로, 고객이 비즈니스 운영, 보안 모니터링, 로그 감사, 로그 분석 등의 문제를 해결하도록 돕습니다. 또한, 고객은 Elasticsearch Service (ES) 서비스를 사용하여 클라우드 서버, 컨테이너 등의 다른 클라우드 제품 실시간 로그, 또는 비즈니스의 기존 및 증분 비즈니스 데이터를 Tencent Cloud ES 클러스터로 수집 전송하여 데이터의 분산 저장, 쿼리 분석을 수행할 수 있습니다. Tencent Cloud는 내부적으로 로그 수집 및 관리 규정과 메커니즘을 구축하여 로그인 로그, 작업 로그, 이벤트 로그 등 로그 데이터의 기록, 추출, 분석, 감사 등을 관리 통제하여 시스템 활동 이상 및 위험을 탐지하고 방지합니다. 동시에, Tencent Cloud는 상세한운영 보안 기준선을 설정하고, 이상 행위 모니터링 측면에서 다년간 축적된 경험을 바탕으로 완비된 규칙 데이터베이스를 구축하여 신뢰할 수 있는 운영 보안 자동화 감사 도구를 만들어 이상 행위를 적시에 식별하고 실시간 경보를 자동으로 트리거할 수 있도록 했습니다.

6.4.2 인적보안

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
2.1	내부인력 보안	2.1.1 【대체】클라우드서비스의 시스템 운영, 개발, 보안등에 관련된 모든 임직원을 주요 직무자로지정하여 관리하고 있는가?	Tencent Cloud는 클라우드 보안 및 정보 보안 관련 조직 구조를 구축하고, 직무 분리 등의 원칙에 기초하여 다양한 계층의 보안 기능 역할 및 관련 책임을 명확히 정의했으며, 정보 보안 감사와 정보 보안 위험 평가 등의 업무 메커니즘을 수립했습니다. Tencent는 보안 기술 위원회와 다양한 기능 및 분야별 전문 보안 팀을 설립했으며, 내부적으로 입사 절차, 재직 기간 절차, 퇴사 절차 등을 포함한 완비된 인적 자원 관리 기준과 절차를 마련하여 직무 요구사항에 따라 인력을 채용하고 배치하도록 보장합니다.
		2.1.2 【대체】권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위험을 줄이기 위하여 직무 분리 기준을 수립·적용하고 있는가?	입사 전, 지원자는 면접을 받게 되며 Tencent Cloud는 해당 직무 요구사항에 맞는 역량을 갖추었는지 평가합니다. 적용 가능한 법률과 직무 등급에 따라 인사 부서는 채용 전 후보자에 대한 신원 조사를 실시합니다. 신원 조사에는 과거 근무 경력, 범죄 이력 조사, 학력 조사가 포함됩니다. 신원 조사 결과는 Tencent Cloud의 인적 자원 관리 시스템에 기록됩니다.
		2.1.3 【대체】조직 내 인력의 인사 변경 발생시 지체없이해당 사용자의 정보자산 반납, 접근 권한변경 및 회수가 이루어 지고 있는가?	채용 후, 내부 직원은 반드시 채용 계약서와 비밀 유지 계약서에 서명해야 합니다. 채용 계약서에는 Tencent Cloud의 기존 보안 정책, 직원 또는 제 3자가 준수해야 하는 정보 보안 및 개인정보 보호 의무가 명시되어 있으며, 비밀 유지 계약서에는 계약 체결자의 기밀 유지 의무와 책임, 그리고 비밀 유지 조항 위반 시 받을 수 있는 제재가 포함되어 있습니다. 직원 재직 기간 동안 Tencent Cloud는 정보 보안 정책, 절차 및 지침에 대해 직원을 교육하기 위한 일련의 정보 보안 교육 및 학습 메커니즘을 구축했습니다. 직원은 정기적으로 정보 보안 인식 교육에 참여합니다.
			Tencent Cloud의 퇴사 절차에는 사용자

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			계정과 권한의 적시 종료, 회사 자산 회수 등의 프로세스가 포함됩니다. Tencent Cloud의 물리적 자산은 지정된 담당자에게 배정되며 Tencent Cloud 내부 전용 자산 추적 시스템을 통해 등록됩니다. Tencent Cloud는 자산의 실제 존재 여부를 확인하고 결과를 기록하기 위해 정기적으로 자산 실사를 수행합니다.
2.2	외부인력 보안	2.2.1 【대체】외부인력에 대한 보안요구사항 준수 여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하고 있는가?	아웃소싱 직원 관리 측면에서, Tencent Cloud는 완벽한 공급망 보안 관리 시스템을 구축하여 공급업체 직원의 활동을 감독하고 관리하며, 정기적으로 평가를 실시하여 공급업체 및 관련 직원의 활동이 Tencent Cloud의 해당 규정 제도에 부합하도록 보장합니다. Tencent Cloud는 완비된 징계 메커니즘을 구축하여 회사 규정을 위반하거나 어떠한 방식으로든 무단 공개를 시도한 직원에 대해서는 징계 절차에 따라 처리하며, 위반 행위의 경우 상황에 따라 노동 계약 해지, 법적 소송 제기, 형사 책임 추적을 포함한 적절한 제재 조치를 취합니다.

6.4.3 위험평가 및 관리

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
3.1	자산 식별 및 분류	3.1.1 【대체】클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하고 있는가?	Tencent Cloud는 내부적으로도 정보 자산 관리 규정 및 전 생애 주기 관리 프로세스를 수립하여, 전자 데이터, 하드웨어 및 그 가상 장비, 인프라, 애플리케이션 시스템 및 소프트웨어 등 자산에 대해 분류 및 등급별 관리 및 보호를 수행합니다. Tencent Cloud는 자산 관리 시스템을 통해 하드웨어 장비 및 소프트웨어 구성 요소를 관리하며, 자산 등록 및 바인딩, 자산 재고 파악 및 정보 업데이트, 자산 폐기 및 교체 등을 포함하여, 클라우드 플랫폼의 기반 시스템이 안정적으로 운영되도록

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			보장하고 비즈니스 시스템에 신뢰할 수 있는 지원을 제공합니다.
3.2	자산 변경관리	3.2.1 【대체】시스템 통합, 전환 및 재개발 시 클라우드컴퓨팅서비스 운영에 지장을 초래하지 않도록 통제절차를 마련하여 적용하고 있는가?	Tencent Cloud는 제품 및 설정 변경 관리 기준을 수립하여 변경 프로세스의 각 단계와 관련 책임자를 명확히 했으며, 변경이 시행되기 전에 적절한 승인과 테스트를 거치도록 합니다. 동시에 Tencent Cloud는 긴급 변경 관리 프로세스를 정의하여 긴급 변경은 적절한 승인을 받은 후에만 진행될 수 있습니다. 응용 프로그램 및 설정 파일, 운영 체제, 데이터베이스 변경 등 모든 유형의 프로그램 변경은 배포 전에 비즈니스 영향 분석을 수행하고 변경 롤백 계획을 수립하며 관련 책임자의 승인을 받아야 합니다. Tencent Cloud 변경 릴리스 시스템은 변경 작업이 권한이 있는 담당자만 수행할 수 있도록 강제하며, 변경 관련 로그를 보존하고 정기적으로 로그를 검토합니다. 변경 릴리스 후 Tencent Cloud 운영 팀은 생산 환경에서 변경 상황을 검증, 모니터링하고 결과를 기록합니다. 또한 Tencent Cloud는 운영 요청의 중요성/긴급성, 변경 범위 등의 속성에 따라 영향 등급을 분류합니다. 외부 환경, 제품, 인프라 및 네트워크 설정에 영향을 미칠 수 있는 변경 요청에 대해서는 Tencent Cloud가 공지, 이메일, Tencent Cloud 콘솔 및/또는 기타 적절한 채널을 통해 고객에게 통지합니다.
3.3	위험관리	3.3.1 【대체】클라우드서비스를 제공하기 위한 핵심자산 및 서비스를 대상으로 주기적으로 취약점 점검을 수행하고, 발견된 위험에 대한	Tencent Cloud는 내부 취약점 스캔 메커니즘과 외부 취약점 수집 플랫폼을 구축했습니다. Tencent Cloud는 취약점 스캔 시스템을 사용하여 클라우드 환경의 보안 취약점을 정기적으로 스캔하며, 스캔 범위는 가상화 계층,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		보완조치를 수행하고 있는가?	시스템 계층 및 애플리케이션 계층을 포괄합니다. 스캔 완료 후 Tencent Cloud 보안팀은 발견된 취약점을 분석, 분류 및 처리합니다. 발견된 보안 취약점은 작업 티켓 시스템에 입력되어 취약점이 정해진 시간 내에 적절히 처리되도록 보장됩니다.

6.4.4 서비스 공급망 관리

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
4.1	공급망 관리정책	4.1.1 【대체】공급망과 관련한 보안 요구사항을 정의하는 관리정책을 수립하고 이행하는가?	Tencent Cloud는 완비된 공급망 보안 관리 체계를 구축하여, 엄격한 공급업체 보안 평가 및 자격 심사, 정기적인 감독 및 평가, 명확한 아웃소싱 서비스 계약 등의 조치를 통해 공급업체를 효과적으로 통제하고, 하도급이 Tencent Cloud의 고객에 대한 관련 서비스 제공 능력 및 고객 정보 처리 과정의 기밀성과 무결성에 영향을 미치지 않도록 보장합니다.
4.2	공급망 변경관리	4.2.1 【대체】공급망 상에서 발생하는 모든 기록 및 보고서에 대해 정기적으로 모니터링 및 검토를 수행하는가?	Tencent Cloud는 정례적 감시 및 평가 메커니즘을 구축하여 정기적으로 공급업체의 기술 역량, 서비스 응답 효율성 및 위험 관리 효과 등을 종합적으로 평가하여, 공급업체의 위험이나 결함으로 인해 Tencent Cloud의 고객에게 제공하는 핵심 서비스 역량이 영향을 받지 않도록 합니다. Tencent Cloud는 양측 간에 체결된 서비스 수준 계약(SLA)을 엄격히 준거하여 공급업체에 정해진 주기로 SLA 이행 보고서를 제출할 것을 요구하며, 보고서에는 서비스 기간 내 중대 사건 처리 기록, 주요 성능 지표 달성 현황 및 유지보수 작업 요약 등의 핵심 내용이 포함되어야 합니다. Tencent Cloud는 정기적으로 공급업체에 대한 성과 평가를 실시하며, 성과 평가 결과는 향후

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			공급업체 협력의 중요한 근거로 활용됩니다.

6.4.5 업무연속성 계획 및 재해복구

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			Tencent Cloud는 자체 클라우드 컴퓨팅 환경에 적합한 비즈니스 연속성 관리 프레임워크를 설계 및 이행하여 포괄적인 비즈니스 연속성 관리 체계를 구축하고, 비즈니스 연속성 관리 규정을 수립하여 비즈니스 영향 분석, 비즈니스 연속성 계획, 비상 대응 및 재해 복구, 비상 훈련 및 테스트, 위기 관리 등을 포함하는 비즈니스 연속성 관리 관련 프로세스를 규정화했으며, 이미 ISO/IEC 22301 비즈니스 연속성 관리 체계의 국제 표준 인증을 획득했습니다.
5.1	장애대응	5.1.1 【대체】클라우드서비스가 중단되지 않도록 업무 지속성 확보방안을 수립하고 이행하는가?	Tencent Cloud 데이터센터는 중국 본토, 아시아 태평양 지역, 북미 지역, 유럽 지역을 포괄하며, 지역(Region)과 가용 구역(Zone)으로 구성되어 전 세계 여러 지역에 걸쳐 분포되어 있습니다. 현재 Tencent Cloud는 한국에 두 개의 임대형 데이터센터를 배치했습니다. 고객은 비즈니스 발전 요구와 데이터 보안 요구사항에 따라 데이터와 시스템을 서로 다른 지역 또는 다른 가용 영역에 자유롭게 유연하게 배포하고, 서로 다른 비즈니스 연속성 모드를 채택하여 비즈니스 재해 복구 요구사항을 충족할 수 있습니다. 또한 Tencent Cloud가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 스토리지 서비스, 데이터베이스 서비스, 컨테이너 및 미들웨어 서비스 등 다양한 클라우드

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			제품/서비스는 모두 고가용성의 특징을 갖추고 있습니다. 예를 들어: Cloud Load Balancer (CLB) 는 안전하고 빠른 4/7 계층 트래픽 분산 서비스를 제공하여, 트래픽 분산을 통해 애플리케이션 시스템의 외부 서비스 역량을 확장하고 단일 장애점을 제거합니다. CLB 는 클러스터 배포를 채택하며, 장애 인스턴스를 신속히 제거하여 고가용성을 실현합니다. Cloud Virtual Machine (CVM) 은 서비스 고가용성과 데이터 고신뢰성의 특징을 갖추고 있습니다. CVM 에 탑재된 클라우드 디스크는 3 중 복사본 저장 전략을 제공하여 데이터가 어느 한 복사본에 장애가 발생할 경우 빠르게 데이터를 이전하고 복구할 수 있도록 보장합니다. Cloud Object Storage (COS) 은 데이터의 다중 아키텍처, 다중 장치 간 중복 저장을 제공하여 사용자 데이터에 재해 복구 및 자원 격리 기능을 제공하여 데이터 지속성을 실현합니다. Cloud Native Database TDSQL-C: Tencent Cloud 의 자체 연구 개발 차세대 클라우드 네이티브 관계형 데이터베이스로서, 고가용성 클러스터 아키텍처를 채택하여 장애 노드를 자동 감지할 수 있으며, 초 단위 장애 전환 및 복구를 지원합니다. TencentDB for MySQL 은 데이터의 고신뢰성과 서비스의 고가용성을 실현하며, 완벽한 데이터 자동 백업 및 무손실 복구 메커니즘을 보유하고 있습니다. Tencent Kubernetes Engine (TKE)

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			는 분산 서비스 아키텍처를 채택하여 서비스의 장애 자동 복구 및 빠른 이전을 보장합니다. 상태 유지 서비스 백엔드의 분산 저장과 결합하여 서비스와 데이터의 안전 및 고가용성을 실현합니다.
			Tencent Cloud는 정보 보안 사건 관리 규정을 수립하고, 정보 보안 보고, 대응 및 처리 메커니즘과 관련 절차를 마련하였으며, 사건 처리 절차에서 각 팀의 역할과 구체적인 책임을 명확히 하였습니다.
			Tencent Cloud는 내부 보안 운영 시스템을 사용하여 보안 사건을 기록합니다. 탐지 및 식별된 보안 사건에 대해 Tencent Cloud는 사건의 성격, 데이터 민감도, 영향 범위 등의 요소를 고려하여 보안 사건을 분석 및 등급 분류하고, 적시에 해당 책임자에게 알려 사건을 추적 처리하도록 합니다.
5.1.2	【필수】클라우드서비스 중단이나 피해가 발생한 경우 장애보고 절차에 따라 장애상황을 기록하고 이용자에게 현황을 파악할 수 있도록 관련 정보를 제공하는가?		고객에게 영향을 미칠 수 있는 보안 사건의 경우 Tencent Cloud는 정보 보안 사건의 영향 범위와 정도에 따라 내부 검토를 거친 후, 적절한 방법으로 고객에게 정보 보안 사건 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.
			사건 증거/사건 정보의 수집 및 관리 측면에서, Tencent Cloud는 내부적으로 보안 사건 증거 수집에 관한 관련 기준을 명확히 했습니다. 정보 보안 사건 접수, 조사 평가, 처리, 추적 과정에서, 관련 책임 부서는 접수한 정보 보안 사건에 관한 기록을 유지 관리하며 기록의 완전성과 기밀성을 보장합니다. Tencent Cloud는 고객의 요구에 따라, 합리성과 실행 가능성 평가를 기반으로 고객의 디지털 포렌식과 사후 보안 사건 조사 및 분석에 효과적인 지원을

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			제공합니다.
		5.1.3 【대 체】클라우드서비스 중단이나 피해가 발생하는 경우, 재해복구목표시간 내 서비스의 장애를 처리하고 복구할 수 있는가?	클라우드 비즈니스의 지속적 가용성을 보장하기 위해, Tencent Cloud는 클라우드 제품 및 서비스에 대해 비즈니스 영향 분석을 수행하여 각 비즈니스의 복구 시간 목표(RTO)와 복구 지점 목표(RPO)를 명확히 했으며, 비즈니스 영향 분석 결과에 따라 서로 다른 대응 전략과 비즈니스 연속성 계획을 수립하고, 클라우드 제품 및 핵심 프로세스에 대해 상세한 재해 복구 계획을 마련했습니다. 관련 전략, 계획 및 계획은 장소, 인력, 장비, 시스템 및 정보 데이터 등 핵심 영역을 포괄하며, 비즈니스 우선순위에 따라 대응하는 재해 복구 프로세스를 수립하여 재해 복구 체계가 완전하고 질서 있으며 실행 가능하도록 보장합니다. Tencent Cloud는 정기적으로 비즈니스 연속성 계획에 따라 클라우드 제품에 대한 비즈니스 연속성 훈련 테스트를 진행하여 계획, 예방책 등의 실행 가능성을 보장합니다. Tencent Cloud는 또한 돌발사건의 감시와 보고, 비상 대응, 재해 복구, 위기 처리 등의 프로세스를 명확히 했으며, 최단 시간 내에 돌발사건의 부정적 영향을 최소화하는 데 주력합니다. Tencent Cloud는 돌발사건 경보 시스템을 통해 사건 보고, 분석 및 사건 등급 분류를 수행하며, 사건 등급에 해당하는 복구 시간 요구사항과 대응 전략에 따라 대응 또는 복구 작업을 진행하여 최대한 운영 중단 사건이 자산 보안, 비즈니스 운영 등에 미치는 손실을 피하고 줄이도록 합니다.
5.2	서비스 가용성	5.2.1 【필 수】가상화 서버, 설비 등 정보처리설비의 장애로 인해 서비스가 중단되지 않도록 관련 설비를	Tencent Cloud 데이터센터는 중국 본토, 아시아 태평양 지역, 북미 지역, 유럽 지역을 포괄하며, 지역(Region)과 가용 구역(Zone)으로 구성되어 전 세계 여러

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		이중화하고, 백업 체계를 마련하고 이행하는가?	지역에 걸쳐 분포되어 있습니다. 현재 Tencent Cloud는 한국에 두 개의 임대형 데이터센터를 배치했습니다. 고객은 비즈니스 발전 요구와 데이터 보안 요구사항에 따라 데이터와 시스템을 서로 다른 지역 또는 다른 가용 영역에 자유롭게 유연하게 배포하고, 서로 다른 비즈니스 연속성 모드를 채택하여 비즈니스 재해 복구 요구사항을 충족할 수 있습니다. 고객 비즈니스의 지속적 가용성을 보장하기 위해 Tencent Cloud는 서버, 네트워크 장비, 보안 장비 등의 하드웨어 장비에 대해 중복 또는 핫 스탠바이 메커니즘을 설정하여 하드웨어 장애 발생 시 데이터가 손실되지 않고 비즈니스가 복구될 수 있도록 보장합니다. 데이터 백업 측면에서 Tencent Cloud는 백업 관리 절차를 수립하여 관련 법률 및 규범 요구사항에 따라 수집 및 처리된 중요한 데이터를 백업합니다. 내부 중요 정보의 경우 Tencent Cloud는 데이터 등급에 따라 서로 다른 데이터의 백업 전략을 수립하고 정기적으로 복구 테스트를 수행합니다. 클라우드 고객 데이터의 경우 Tencent Cloud는 클라우드 제품 또는 서비스의 기능에 따라 고객에게 다중 저장 복사본 및 백업 서비스를 제공하며, 제품 서비스 수준 계약에 명시된 바에 따라 제공하는 데이터 백업 서비스에 대한 책임을 집니다. Tencent Cloud가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 저장 서비스, 데이터베이스 서비스, 컨테이너 및 미들웨어 서비스 등 다양한 클라우드 제품/서비스는 모두 고가용성 특성을 갖추고 있어 고객이 시스템 또는 서비스의 고가용성을 실현하는 데 도움을 줍니다. 예를 들면:

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			• 고객이 Cloud Object Storage (COS)에 저장한 데이터는 교차 리전 복제 기능을 통해 여러 지정된 리전에 동시에 저장될 수 있어, 예기치 않게 일부 데이터가 손실된 경우에도 중복 데이터를 통해 완전한 데이터를 찾아 복구할 수 있으며, 하나의 가용 구역 저장소가 불가항력적인 재해로 손상을 입을 경우 발생할 수 있는 손실을 방지하여 다중 중복 백업과 재해 복구 효과를 달성할 수 있습니다. • Cloud Block Storage (CBS)의 스냅샷 백업 기능은 CBS의 특정 시점 스냅샷을 생성하여 데이터를 백업함으로써 변조 및 실수로 인한 삭제로 인한 데이터 손실을 방지하고, 비즈니스 장애 시 신속한 롤백이 가능하도록 보장합니다. • Cloud File Storage (CFS)은 정기적인 스냅샷 기능을 제공하여 고객이 유연하게 백업 작업 전략을 설정할 수 있도록 하며, 서로 다른 비즈니스에 대해 서로 다른 정기 스냅샷 전략을 채택할 것을 권장합니다. • Cloud Native Database TDSQL-C는 논리적 백업과 스냅샷 백업 두 가지 백업 유형을 지원하며, 완전한 데이터 백업과 이후 일정 기간 동안의 binlog 백업을 통해 전체 TDSQL-C MySQL 클러스터나 특정 데이터베이스/테이블 임의의 시점으로 복구할 수 있습니다. • TencentDB for MySQL은 데이터베이스를 백업하기 위한 자동 백업과 수동 백업 두 가지 방식을 지원하며, 교차 리전 백업 기능을 제공하여 고객의 재해 복구 능력을 향상시키고 동시에

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			데이터의 신뢰성을 높입니다. TencentDB for MongoDB는 데이터의 자동 백업과 무손실 복구 메커니즘을 제공하며, 다중 노드 백업 데이터를 지원합니다. 고객은 백업 메커니즘을 통해 여러 날 동안의 백업 데이터를 저장하여 재해 상황 시 데이터 복구를 용이하게 할 수 있습니다.
5.2.2	【대체】	주기적으로 서비스 연속성(가용성) 확보를 위한 점검을 수행하고 있는가?	Tencent Cloud는 일반적으로 정기적으로 비상 대응 및 재해 복구 훈련을 통해 서비스 연속성(가용성)을 검증합니다. Tencent Cloud는 비즈니스 연속성 계획을 기반으로 훈련 계획을 수립하고, 훈련 위험 평가를 수행하며, 이에 상응하는 보장 조치를 수립하여 훈련으로 인한 서비스 부정적 영향을 피합니다. Tencent Cloud의 재해 복구 훈련은 일반적으로 실제와 유사한 전형적 재해 복구 시나리오(공격-방어 대응 및 대규모 장애 등 포함)를 모의하여 시스템의 재해 복구 능력, 대응 속도 및 복구 능력을 종합적으로 점검합니다. 훈련 종료 후 관련 부서는 훈련 보고서를 작성하고 개선 조치에 따라 시정을 진행하며, 보고서를 기록 보관합니다. Tencent Cloud는 매년 자사의 비즈니스 연속성 관리 체계를 검토 및 업데이트하며, 비즈니스 영향 분석 결과에 따라 관련 제품 및 서비스의 비즈니스 연속성 계획과 재해 복구 계획을 검토하고 필요에 따라 업데이트합니다.

6.4.6 침해사고 대응 및 관리

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
6.1	침해사고 대응 절차 및 체계	6.1.1 【대체】해킹 등 전자적 침해행위로 인한 피해 발생 시 대응을 위한 침해사고 대응절차를 수립하고 이행하는가?	사건 대응 및 처리 측면에서 Tencent Cloud는 정보 보안 사건 관리 규정을 수립하고, 정보 보안 보고, 대응 및 처리 메커니즘과 관련 절차를 마련하였으며, 사건 처리 절차에서 각 팀의 역할과 구체적인 책임을 명확히 하였습니다. Tencent Cloud는 내부 보안 운영 시스템을 사용하여 보안 사건을 기록합니다. 탐지 및 식별된 보안 사건에 대해 Tencent Cloud는 사건의 성격, 데이터 민감도, 영향 범위 등의 요소를 고려하여 보안 사건을 분석 및 등급 분류하고, 적시에 해당 책임자에게 알려 사건을 추적 처리하도록 합니다. Tencent Cloud는 또한 네트워크 보안 비상 계획을 구축하여 네트워크 공격, 악성 프로그램, 데이터 보안, 장비 시설 장애, 재해성 사건 등 다양한 유형의 네트워크 보안 비상 상황을 포괄하고 있습니다. 이를 통해 완비된 비상 계획 체계 구축을 기초로, 비상 대응팀 구축을 지원으로, 비상 대응 프로세스 규격화를 중점으로 하여, 모니터링 경보, 보고 및 처리 등의 업무 능력을 더욱 강화하고 네트워크 보안 사건이 Tencent Cloud에 미치는 부정적 영향을 예방하고 줄이고자 합니다.
		6.1.2 【대체】침해사고 발생 시 신속한 대응이 가능하도록 주기적으로 침해사고 대응절차에 기반한 훈련을 실시하고 있는가?	사건 대응 절차의 효과성과 신속성을 보장하기 위해 Tencent Cloud 내부 비즈니스 부서는 정기적으로 보안 사건 비상 대응 훈련을 진행하며, 보안 기술 발전과 상황 변화에 따라 보안 팀 직원들에게 기술 교육을 제공하여 최신 보안 규정과 운영 절차를 이해하고 준수하며, 최신 정보 보안 기준과 모범 사례를 숙지하도록 합니다.
		6.1.3 【필수】금융권 통합 보안관제수행을 위한 지원 체계가 마련되어 있는가?	Tencent Cloud 보안팀은 7*24 시간 운영되는 보안 운영 체계를 기반으로 취약점 모니터링, 침입 추적, 공격 차단 등의 핵심 시나리오에 집중하여, 보안

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			경보에 실시간으로 대응하고 공격 추적 및 비상 대응 계획을 신속히 수립함으로써 보안 사건의 확산을 효과적으로 억제합니다. Tencent Cloud는 또한 고객의 보안 운영을 지원하기 위해 일련의 관련 제품 및 서비스를 제공합니다. 이는 다음과 같습니다: Cloud Security Center (CSC): 통합 보안 관리 플랫폼으로서, 자산 센터, 리스크 센터, 경보 센터, 고급 보안 관리를 통해 고객이 사전 위협 탐지, 사중 대응·처리, 사후 추적 분석의 보안 운영 클로즈드 루프를 실현할 수 있도록 지원합니다. CSC는 클라우드 자산에 대한 통합 보안 관리를 지원하며, 자산 자동화 실사, 보안 리스크 탐지·식별, 보안 리스크 자동화 대응·처리 기능을 포함합니다. CSC는 클라우드 방화벽, 웹 애플리케이션 방화벽의 위협 경보 및 로그를 수집하고, Tencent Cloud 위협 인텔리전스 및 자체 보안 지식 데이터베이스를 활용하여 데이터에 대한 자동화된 분석·조사를 수행하여 고객에게 집중화된 위협 탐지, 조사, 처리 역량을 제공합니다. Threat Intelligence Center (TIX): 통합 인텔리전스 서비스 플랫폼으로서, 기초 인텔리전스, 공격면 인텔리전스, 비즈니스 인텔리전스 등 세 가지 핵심 인텔리전스 역량을 제공하며, 인텔리전스 조회, IOC 분석·판단, 공격면 관리 등의 기능을 지원합니다. 이를 통해 고객이 보안 사고를 보다 효율적으로 분석·판단하고 기업 자산의 노출 리스크를 보다 전면적으로 평가할 수 있도록 지원하여, 기업의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			효율적인 입체적 보안 방어 체계 구축을 돕습니다. 또한, Tencent Cloud의 Cloud Log Service (CLS), CloudAudit 및 Flow Logs 등 여러 로그 제품과 서비스는 "로그 다운로드", "로그 내보내기", "로그 전달" 등의 기능을 통해 고객이 자신의 클라우드 로그를 로컬에 다운로드하여 확인하거나, 지정된 제3자 시스템(고객의 온프레미스 SIEM/SOC 플랫폼 포함)으로 전달할 수 있도록 지원합니다.
6.2	침해사고 대응	6.2.1 【필수】침해사고 발생 시 침해사고 대응절차에 따라 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황등을 신속하게 알리고 있는가?	Tencent Cloud는 정보 보안 사건 대응, 사건 에스컬레이션, 사건 통지 등의 관련 절차를 구축하여 사고의 영향을 받을 수 있거나 이미 받은 회사 내부 인원 및 고객 등 이해관계자들에게 적시에 경보 또는 통지를 제공하고, 모든 당사자가 질서 있고 적시에 효율적으로 소통과 협업을 할 수 있도록 합니다. 고객에게 영향을 미칠 수 있는 보안 사건의 경우 Tencent Cloud는 정보 보안 사건의 영향 범위와 정도에 따라 내부 검토를 거친 후, 적절한 방법으로 고객에게 정보 보안 사건 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.

6.4.7 사용자 인증 및 접근통제

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
7.1	접근통제 정책	7.1.1 【대체】비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하고 이행하는가?	Tencent Cloud는 접근 통제 관리 관련 기준을 수립하여 클라우드 플랫폼 제품, 단말 시스템, 호스트 운영 체제, 응용 시스템, 네트워크 장비 등에 대한 접근 통제 활동을 규정화했습니다. Tencent Cloud는 사용자 계정이 고유 식별자를

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			사용하도록 요구하며, 보안 기준에 따라 직원 계정에 대한 비밀번호 정책(비밀번호 길이, 복잡성, 잠금 및 재설정 등 포함)을 설정합니다. 내부 단말, 운영 체제, 응용 프로그램 및 네트워크 장비에 대해서는 Tencent Cloud가 로그인 실패 횟수 제한 및 세션 타임아웃 정책을 구성했습니다. Tencent Cloud는 제로 트러스트 보안 관리 시스템을 통해 직원의 접근 인증을 수행하며, 사용자는 내부 자원에 접근하기 전에 이중 요소 인증을 완료해야 합니다. Tencent Cloud는 직원 계정의 로그인 상태에 대해 실시간 보안 모니터링을 시행하여, 어떠한 비정상적인 로그인 행위라도 탐지되면 IT 보안 시스템이 즉시 해당 계정 소유자에게 연락하여 확인 및 처리하도록 하고, 관련 사건을 상세히 기록합니다. Tencent Cloud는 또한 권한 부여 정책 및 권한 분리 매트릭스 메커니즘을 수립하여 최소 권한 원칙을 준수하며, 직무 책임에 따라 필요한 운영 권한을 할당하고, 권한에 유효 기한을 설정하여 권한의 정교한 통제를 실현합니다. Tencent Cloud는 직위 역할에 대응하는 인원 신상 정보와 각 비즈니스 시스템 권한 수준의 기록을 유지 관리하며, 정기적으로 내부 권한 심사 작업을 조직하여 권한이 남용되거나 오용되지 않도록 보장합니다.
7.2	접근권한 관리	7.2.1 【대체】클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 검토하고 있는가? 7.2.2 【필수】이용자의 정보처리시스템과 관련된 단말기 및 전산자료에	Tencent Cloud는 접근 통제 관리 규정을 수립하여 권한 부여 정책 및 권한 분리 매트릭스 메커니즘을 명확히 하고, 직위 역할에 대응하는 인원 신상 정보와 각 비즈니스 시스템의 권한 수준 기록을 유지 관리합니다. Tencent Cloud는 최소 권한 원칙을 엄격히 준수하며, 기본적으로 최소 권한 통제를 시행합니다. Tencent Cloud는 정기적으로 내부 권한 심사 작업을 조직하여 권한이

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		접근 권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련하고 적용하고 있는가?	남용되거나 오용되지 않도록 보장합니다. 더 이상 필요하지 않은 접근 권한에 대해서는 적절한 후속 조치를 취하여 불필요한 접근 권한을 적시에 철회합니다. Tencent Cloud 생산 환경에는 베스천 호스트(Bastion Host)가 전면 배포되어 있으며, 이를 통해 백엔드 시스템 구성 요소의 관리자 계정 권한을 중앙 집중식으로 통제합니다. 내부 운영 인원이 베스천 호스트에 접근하려면 권한 부여 승인이 필요하며, 특정 Tencent Cloud 내부 운영 인원만 접근할 수 있고, 베스천 호스트 로그인 시 이중 요소 인증이 필요합니다. 운영 작업 기록은 로깅 플랫폼에 집중 저장되며, Tencent Cloud 내부 감사팀이 정기적으로 로그를 검토합니다. 로그 관리 플랫폼에는 비정상적인 사용자 작업 및 활동을 탐지하기 위한 규칙이 정의되어 있으며, 식별된 비정상적인 사항은 자동으로 보안팀에 전달되어 조사됩니다. 고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. 서비스 제공 또는 문제 해결의 필요성이 있고, 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 부처의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 상황이 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 직접 접촉하지 않습니다. Tencent Cloud는 데이터 접근 권한에 대해 전 노드 실명제 심사 및 유지 관리를 시행하여 데이터 자산의 무결성과 비즈니스 서비스의 신뢰성을 보호하며, 실시간 모니터링 및 차단 메커니즘을 구축하여 비정상적인 데이터 접근 행위를 탐지하고 차단합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
7.3	사용자 식별 및 인증	7.3.1 【대 체】 이용자가 클라우드서비스 이용 시 추가 인증수단을 요청하는 경우 이를 제공하고 있는가?	클라우드 사용자 접근 통제 관리 측면에서, Tencent Cloud 는 접근 통제 관리 관련 절차를 수립하여 클라우드 고객 계정의 등록, 관리 및 지원과 관련된 기준을 포함합니다. Tencent Cloud 는 클라우드 고객에게 접근 통제 관리 기능을 제공하여 고객이 자체적으로 접근 통제 정책을 수립하고 해당 정책을 통해 구매한 클라우드 제품에 대한 접근을 관리할 수 있도록 합니다.
		7.3.2 【대 체】이용자의 안전한 클라우드서비스 이용을 위해 계정 및 패스워드 등의 관리절차 마련하고 안내하고 있는가?	Tencent Cloud 는 고객에게 관리 콘솔을 제공하여 고객이 클라우드 자원을 중앙 집중식으로 관리 및 통제할 수 있도록 지원합니다. 고객이 클라우드 계정을 등록할 때, 각 클라우드 고객에게 고유하게 식별 가능한 계정이 할당되며 비밀번호 설정 규칙/정책이 구성되고, 관리 콘솔은 사용자 계정 이름의 고유성을 자동으로 확인합니다. 고객이 관리 콘솔에 로그인할 때, 신원 및 인증 정보 그리고 운영 명령은 HTTPS 프로토콜을 통해 전송됩니다. 고객은 공개 API 를 통해 클라우드 서비스와 데이터를 중앙 집중식으로 관리할 수 있습니다. 고객이 Open API 기능을 등록할 때, 각 고객에게 할당된 접근 키를 적용하여 인증해야 합니다. Tencent Cloud 는 고객이 다중 요소 인증을 활용하여 계정 로그인 및 비밀번호 변경과 같은 민감한 작업의 보안성을 강화하도록 지원합니다. Tencent Cloud 는 또한 계정 비밀번호 재설정 및 수정 기능을 제공합니다.
			Tencent Cloud 는 또한 고객에게 Cloud Access Management (CAM) 를 제공하여 고객이 Tencent Cloud 제품 및 자원에 대한 접근을 관리할 수 있도록 돕습니다. 여기서 사용자 마스터 계정은 서브 사용자를 생성하고 서브 사용자에게 신원 ID, 신원 증명 및 권한을 할당할 수

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			있습니다. 사용자는 접근 관리 콘솔을 통해 서버 사용자의 비밀번호 규칙(비밀번호 복잡성, 길이, 유효 기간 등 포함) 및 단일 로그인 세션 만료 시간을 수정할 수 있습니다. 비밀번호 유출을 방지하기 위해 Tencent Cloud는 비밀번호에 SHA256 해시 암호화 및 소금 처리를 적용하여 평문 비밀번호 저장을 피합니다. CAM은 또한 다양한 방식의 이차 인증 기능을 지원하며, CloudAudit를 통해 Tencent Cloud 계정 활동에 대한 감독, 규정 준수 점검, 작업 검토 및 위험 검토를 지원합니다. Tencent Cloud 관련 제품의 조작 가이드, 사용자 매뉴얼 등은 문서화되어 공식 웹사이트를 통해 고객에게 제공됩니다. Tencent Cloud는 또한 고객에게 Tencent Cloud 제품 상식 및 관련 전문 능력에 기반한 Tencent Cloud Training and Certification을 제공하여 고객의 기술 역량과 클라우드 숙련도를 향상시킵니다. 또한, Tencent Cloud는 고객에게 7*24 시간 작업 티켓, 7*24 시간 핫라인, 지능형 고객 서비스, 셀프 서비스 등 다중 채널을 제공하여 고객의 문제와 피드백을 끊임없이 처리합니다. Tencent Cloud의 고객 서비스 팀과 기술 전문가는 고객에게 신속하고 효과적인 지원을 제공합니다.

6.4.8 가상화 및 인프라 보안

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
8.1	가상화 보안	8.1.1 【대체】 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하고 있는가?	Tencent Cloud는 고객에게 관리 콘솔을 제공하여 고객이 클라우드 리소스를 중앙 집중식으로 관리 및 제어할 수 있도록 지원합니다. 고객은 콘솔을 통해 Tencent Cloud 제품과 서비스를 구매, 조회, 사용할 수 있으며, 최근 액세스 및

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			현재 사용 중인 클라우드 제품, 모니터링 경보, 보류 중인 작업 티켓, 미결제 청구서 등의 내용을 확인할 수 있습니다.
8.1.2	【필수】	이용자가 클라우드서비스 이용 중 가상자원*을 삭제할 경우 삭제대상과 관련된 모든 자원이 복구되지 않는 방법으로 삭제되는가? *가상머신(이미지, 백업, 스냅샷 등), 가상스토리지, 가상소프트웨어, 가상환경 설정정보 등	고객이 특정 인스턴스를 더 이상 필요로 하지 않을 경우, 인스턴스를 폐기할 수 있습니다. 수동으로 폐기된 인스턴스는 휴지통으로 이동되며, 최대 2 시간 동안 휴지통에 보관됩니다. 휴지통에 있는 인스턴스에 대해 고객은 다양한 시나리오와 요구사항에 따라 연장, 복구 또는 완전 삭제를 선택할 수 있습니다. Tencent Cloud는 리소스를 재활당하기 전에 표준 정책 및 계약 요구사항에 따라 엄격한 논리적 삭제 또는 물리적 삭제를 적시에 수행하여, 고객의 인증 정보, 파일, 디렉토리, 데이터베이스 레코드 등 민감한 정보가 저장된 공간이 재활당되거나 다른 사용자에게 할당되기 전 완전히 삭제되도록 보장합니다.
8.1.3	【필수】	가상자원에 대한 무결성을 보장하고 가상자원 손상 시 이용자에게 안내하고있는가?	Tencent Cloud가 고객에게 제공하는 Cloud Virtual Machine (CVM) 은 확장 가능한 가상화 컴퓨팅 서비스로, 고객이 CPU, 메모리, 하드 디스크, 네트워크, 보안 등의 리소스를 사용자 정의할 수 있도록 지원합니다. Tencent Cloud는 고객에게 공식 정품 기반 운영 체제와 Tencent Cloud가 제공하는 초기화 구성 요소를 포함한 안전한 공식 공용 이미지를 제공합니다. CVM은 또한 고객이 사용자 정의 이미지를 생성하거나 이미지 가져오기 기능을 통해 가져오고, 사용자 정의 이미지를 공유 및 삭제하는 것을 지원합니다. Tencent Cloud는 CVM에 대해 클라우드 모니터링을 제공하여 다양한 실시간 경보를 지원하며, DDoS 방어, DNS 하이재킹 탐지, 침입 탐지, 취약점 스캔, 웹사이트 악성코드 탐지, 로그인 보호 등의 보안 서비스를 제공합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			컨테이너 이미지 관리 측면에서, Tencent Cloud Container Registry (TCR) 는 고객에게 안전하고 전용적이며 고성능의 컨테이너 이미지 호스팅 및 배포 서비스를 제공합니다. 고객은 Tencent Cloud Container Security Service (TCSS)를 활용하여 컨테이너 및 이미지 보안을 보호할 수 있습니다. TCSS 는 컨테이너 자산 관리, 이미지 보안 스캔, 런타임 침입 탐지, 보안 기준선 설정 관리 등의 기능을 지원하여, 이미지 생성·저장부터 실행까지 컨테이너 전체 생명주기 보호를 제공하고 고객이 컨테이너 보안 방어 체계를 구축할 수 있도록 지원합니다. Tencent Cloud 전문 팀이 7*24 시간 운영 유지 보수 서비스를 제공하며, 선진 서버 모니터링 및 진단 기술을 활용하여 서버의 각종 장애를 자동으로 감지하고 즉시 자동으로 복구 프로세스를 실행합니다. 선진 원격 관리 도구를 통합하여 데이터센터 현장 및 공급업체 자원을 자동으로 조율하고 서버 장애를 적시에 복구합니다. 고객에게 영향을 미칠 수 있는 장애나 사건의 경우, Tencent Cloud 는 장애나 사건의 영향 범위와 정도에 따라 내부 심사를 거친 후, 적절한 방식으로 고객에게 장애나 사건의 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.
8.1.4	【대체】하이퍼바이저 등 물리적/논리적 가상화 서버(기능) 및 인터페이스에 대한 보안관리 및 접근통제를 수행하고 있는가?		물리적 접근 통제 측면에서, Tencent Cloud 는 데이터센터 운영사에 출입 통제 승인 시스템 내 완전한 인력 접근 통제 보안 매트릭스를 구축하고, 다양한 인력의 접근 및 운영 행위에 대한 효과적 통제를 요구합니다. 또한 Tencent Cloud 는 데이터센터 운영사의 보안 담당자가 엄격히 점검 목록과 점검

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			계획에 따라 각 기계실 및 장비 상황을 순찰하며, 데이터센터에 7*24 시간 사각지대 없는 비디오 모니터링 경보 시스템을 설치하고 보안실에서 이를 감시하도록 요구합니다. 물리적 접근 통제 측면에서, Tencent Cloud는 생산 환경에 베스천 호스트(Bastion Host)를 전면 배포하여, 이를 통해 Tencent Cloud 백엔드 시스템 구성 요소의 관리자 계정 권한과 계정 활동을 중앙 집중식으로 관리합니다. 베스천 호스트(Bastion Host) 접근은 권한 부여 승인이 필요하며, 특정 Tencent Cloud 내부 운영 인원만 접근할 수 있고, 베스천 호스트 로그인에는 적절한 신원 인증이 필요합니다. 백엔드 운영 작업 기록은 모두 로깅 플랫폼에 집중 저장되며, Tencent Cloud 내부 감사팀이 정기적으로 기록을 검토합니다.
		8.1.5 【필수】가상자원 관리 시스템*과 가상 소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 관리적, 물리적, 기술적 보호대책을 수립하고 이행하는가? * 가상자원을 제공하기 위한 웹사이트(클라우드 포털, 클라우드 콘솔, API 등)	Tencent Cloud 가상 머신 및 가상 서비스 사용 과정 중 보안 통제를 강화하기 위해, Tencent Cloud는 내부적으로 가상화 보안 관리 관련 규정을 수립하여 가상 머신 리소스의 관리 책임, 권한 관리, 구성 관리 등 관련 기준을 명확히 했습니다. Tencent Cloud는 가상 머신 격리 및 리소스 제어, 패치 관리 및 취약점 방어, 하이퍼바이저 보안 강화 등의 기술적 수단을 통해 다양한 측면에서 가상화 보안 방어 체계를 구축합니다.
8.2	가상환경 보호	8.2.1 【대체】이용자의 가상환경 보호를 위한 악성코드 방지대책을 수립하고 이행하는가?	보안 구성 측면에서, Tencent Cloud는 내부적으로 네트워크 보안 구성 기준과 보안 기준선 기준을 구축하여, 네트워크 장비, 방화벽, 호스트 서버 운영 체제, 데이터베이스 및 응용 시스템의 보안 구성을 표준화 관리하도록 했습니다. 라우터, 방화벽 및 네트워크 서버 등 네트워크 장비의 보안 정책 및 매개변수 설정은 정기적으로 검토되어 정책과

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			매개변수의 유효성을 보장합니다. 보안 모니터링 측면에서, Tencent Cloud 내부에는 네트워크 모니터링 시스템을 배포하여 라우터, 방화벽 및 네트워크 서버 등 네트워크 장비를 모니터링하고 경보를 발생시키며, 권한 통제, 승인 절차 등 다중 조치를 통해 비인가자의 내부 네트워크 자원 접근을 엄격히 금지하고 있습니다. Tencent Cloud는 엔드포인트 탐지 및 대응(EDR) 도구를 배포하여 전체 네트워크 서버 단말 자산에 대한 포괄적인 모니터링 및 제어를 수행합니다. Tencent Cloud가 사용하는 EDR 도구는 바이러스 백신 및 침입 탐지, 보안 기준선 및 취약점 스캔, 그리고 명령 작업, 로그인 행위에 대한 보안 규정 준수 감사 등의 기능을 지원하며, 악성 프로그램이나 비정상적 행위를 식별할 때 경보를 발생시킵니다. 취약점 스캔 및 침투 테스트에 대해, Tencent Cloud는 취약점 스캔 시스템을 통해 정기적으로 스캔 작업을 생성하여 클라우드 환경 내 자산에 대한 취약점 스캔을 수행하고, 발견된 취약점을 분석, 분류 및 수정 처리합니다. Tencent Cloud는 정기적으로 전체 링크 대규모 침투 테스트를 수행하여 시스템의 잠재적 보안 위험을 사전에 식별하고 조기에 수리하며, 신제품 출시 전이나 중대 변경 등 상황에서 유연하게 대상 지향적인 침투 테스트를 진행합니다. Tencent Cloud는 컨테이너 클라우드 환경의 안전을 보장하기 위해, 전방위적이고 계층화된 컨테이너 보안 체계를 구축했습니다. 컨테이너 클라우드 내부와 외부 간(즉, 남북 방향)의 네트워크 보안에 대해서는, 웹 애플리케이션 방화벽, 분산 서비스 거부(DDoS) 공격 방어 시스템, 웹 애플리케이션 취약점 스캔, 침입 탐지 및 방어 시스템(IDPS) 등과 같은 기존의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			보안 제품 및 역량을 직접 재사용하여, 상응하는 보안 탐지 및 보호를 실현합니다. 컨테이너 클라우드 내부(즉, 동서 방향)의 보안에 대해서는, Tencent Cloud는 상응하는 컨테이너 보안 메커니즘을 채택하여 구현하며, 보안 역량의 원생화, 보안 좌측 이동 및 제로 트러스트와 같은 보안 설계 원칙에 기반하고, 계층화된 보안 체계를 도입하여, 컨테이너 클라우드 플랫폼을 수용하는 인프라 계층, 컨테이너와 컨테이너 클라우드 플랫폼 기반 구조 계층, 그리고 컨테이너가 수용하는 애플리케이션 계층에서 각각 보안 보호를 실현합니다.
8.3	인프라 보안	8.3.1 【대체】클라우드서비스와 관련된 내외부 네트워크를 보호하기 위한 정보보호시스템을 설치하고 운영하고 있는가? 8.3.2 【대 체】업무, 서비스 등을 고려한 영역 간 네트워크를 분리하여 운영하고 있는가? 8.3.3 【필 수】이용자의 가상환경 보호 및 네트워크 분리를 위해 필요한 기능을 제공하는가?	네트워크 보안 보호 및 관리를 시행하기 위해 Tencent Cloud는 네트워크 보안 관리 규정과 네트워크 침범 방어 체계를 구축했습니다. Tencent Cloud는 관리 제도와 프로세스를 통해 네트워크 보안 통제와 보호 기준, 그리고 이에 상응하는 역할과 책임을 명확히 하여 Tencent Cloud 네트워크가 수반하는 비즈니스가 안전하게 운영되도록 보장합니다. Tencent Cloud는 네트워크 침범 방어 체계를 구축하고 업계 실무를 참고하여 네트워크 보안 아키텍처를 설계하며, 비즈니스 기능과 보안 위험에 따라 보안 영역을 구분하고, 서로 다른 보안 영역에 대해 물리적 또는 논리적 격리를 수행하며, 접근 통제 및 경계 방어 등의 조치를 통해 업무 네트워크와 생산 네트워크의 보안을 확보합니다. Tencent Cloud는 방화벽, 침입 탐지/방지 시스템(IDS/IPS), DDoS 방어, 웹 보안 방어 등 다중 방어 메커니즘을 통해 악성 네트워크 트래픽을 신속히 탐지, 필터링 및 차단하여 Tencent Cloud의 네트워크 보안을 보호합니다. 데이터 전송 보호 측면에서, 고객의 Tencent Cloud 콘솔 상의 모든 통신은

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			HTTPS 보안 프로토콜의 암호화 보호를 받습니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스는 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 고객의 비즈니스에 포트 수준의 통신 보안을 제공합니다. 테넌트 격리 측면에서, Tencent Cloud는 가상화 제어층 자원 접근 통제 정책, 클라우드 플랫폼 내부 사설 네트워크 간 격리 정책, 웹 콘솔 권한 할당 및 신원 인증, 인터페이스 세션 ID 및 접근 키 등의 보안 메커니즘을 제공하여, 각 고객이 자신이 구매한 클라우드 컴퓨팅 자원에만 접근할 수 있도록 보장하며, 다중 테넌트 간 접근 격리를 효과적으로 실현합니다. 효과적인 격리 수단을 통해, 동일 자원 풀 내 고객 데이터는 서로 보이지 않도록 하고, 테넌트가 다른 테넌트의 데이터에 접근, 획득 또는 변조할 수 없음을 보장합니다. 고객은 Tencent Cloud가 제공하는 <u>Virtual Private Cloud (VPC)</u> 서비스를 이용하여 구매한 클라우드 플랫폼 자원에 대해 다수의 독립적인 네트워크 공간을 구축하고, 네트워크 세그먼트 분할 및 IP 주소 할당, 사용자 정의 라우팅 정책 등을 자유롭게 설정할 수 있습니다. VPC 서비스는 Tencent Cloud를 기반으로 구축된 전용 클라우드 네트워크 공간으로, 사설 네트워크는 터널링 기술을 활용하여 물리적 네트워크 상에 가상 네트워크를 구성하고 가상화 기술을 적용함으로써 서로 다른 사설 네트워크 간의 내부 네트워크를 완전히 격리시켜 고객에게 독립적이고 격리된 안전한 클라우드 네트워크를 제공합니다. 사설 네트워크 내의 클라우드 서버에 대해서는 보안 그룹 및 네트워크 ACL 규칙 설정을 통해 인스턴스 수준 및 서브넷의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			인바운드/아웃바운드 트래픽을 제어하여, 다양한 수준의 네트워크 접근 제어를 구현할 수 있습니다. 또한, Tencent Cloud는 또한 고객이 네트워크 보안을 효과적으로 관리할 수 있도록 다수의 서비스를 제공합니다. 예를 들어: • <u>Tencent Cloud EdgeOne</u>은 Tencent의 글로벌 에지 노드를 기반으로 고객에게 보안 보호 및 가속 서비스를 제공하며, DDoS 방어, 지능형 웹 보호, BOT/크롤러 유형 공격 방어, DNS 해석 등의 기능을 갖추고, 고객이 비즈니스 요구에 따라 사용자 정의 접근 통제 규칙을 구성할 수 있도록 지원합니다. • <u>Cloud Firewall (CFW)</u>은 주로 고객에게 다양한 네트워크 경계의 보호를 제공하며, 방화벽 ACL 능동적 제어, IPS 실시간 차단, 가상 패치 및 악성 코드 탐지 등의 기능을 지원하여 기존 네트워크의 DMZ 영역 요구를 충족시키고 핵심 자산에 대한 집중 보호를 실현하며, VPC 간의 세분화된 격리 관제를 가능하게 합니다. • <u>Web Application Firewall (WAF)</u>은 Tencent Cloud 내부 및 외부 사용자가 웹 공격, 침입, 취약점 악용, 악성 코드 삽입, 변조, 백도어, 크롤링 등 웹사이트 및 웹 비즈니스 보안 문제에 대응할 수 있도록 지원합니다. • <u>Anti-DDoS</u>는 충분하고 우수한 DDoS 방어 자원과 지속적으로 발전하는 "자체 개발 + AI 지능형 인식" 정제 알고리즘을 결합하여 DDoS 공격 문제에 대응합니다.

6.4.9 개발 및 운영 보안

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
9.1	시스템 분석 및 설계	9.1.1 【대체】 보안감사증적(로그)의 정확성을 보장하기 위해 표준시각으로 동기화하고 있는가?	Tencent Cloud는 네트워크 시간 프로토콜(Network Time Protocol, NTP)을 통해 현재 정확한 세계 표준시(UTC)를 표시합니다. Tencent Cloud는 내부망 NTP 서버를 제공하여 Tencent Cloud 클라우드 상의 인스턴스가 사용할 수 있도록 하며, 비-Tencent Cloud 장비의 경우 고객은 Tencent Cloud가 제공하는 공용망 NTP 서버를 사용할 수 있습니다. 또한 Tencent Cloud는 정기적으로 NTP 서버의 시간 동기화 상태를 점검하여 전 네트워크 시간이 통일되고 정확하며 신뢰할 수 있도록 보장합니다.
9.2	구현 및 시	9.2.1 【대체】테스트 시 이용자 정보 사용을 금지(부하테스트 등의 불가피한 경우 이용자 정보 변환 사용 및 테스트 종료 즉시 삭제)하고 있는가?	Tencent Cloud는 업계 모범 사례를 참고하여 네트워크 보안 아키텍처를 설계하며, 비즈니스 기능과 보안 위험에 따라 보안 영역을 구분하고, 서로 다른 보안 영역에 대해 물리적 또는 논리적 격리를 수행합니다. 접근 제어 및 경계 보호 등의 조치를 통해 업무 네트워크, 생산 네트워크 등의 안전을 보장하며, 개발 테스트 환경에서 비탈취되지 않은 생산 환경 데이터의 사용을 금지합니다. 고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. 서비스 제공 또는 문제 해결의 필요성이 있고, 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 부처의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 상황이 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 직접 접촉하지 않습니다.

6.4.10 암호화 및 데이터 보호

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
10.1	데이터 보호	10.1.1 【대체】 데이터 분류기준에 따라 데이터를 분류하고 관리하고 있는가?	Tencent Cloud는 데이터 보안 관련 관리 절차를 수립하여 데이터 분류 및 등급화와 데이터 보호 원칙을 명확히 했으며, 데이터 소유자가 데이터 분류 및 등급화 요구에 따라 데이터 수집, 전송, 접근 통제, 백업, 거래 보호, 그리고 제3자와의 정보 전송 관리 전 생애 주기 동안 상응하는 보안 보호 조치를 시행하여 데이터의 기밀성, 무결성 및 가용성을 보호하도록 요구합니다. Tencent Cloud 전자 데이터의 분류에는 고객 클라우드 비즈니스 데이터, Tencent Cloud 데이터 및 개인정보 데이터가 포함됩니다. 이 중 고객 클라우드 비즈니스 데이터는 고객(클라우드 테넌트)의 클라우드 상 비즈니스 데이터 정보를 의미하며, Tencent Cloud 데이터는 Tencent Cloud 서비스의 운영 및 유지보수 과정에서 생성된 데이터를 의미하고, 개인정보 데이터는 고객이 클라우드 서비스 사용 과정에서 제공하는 개인 데이터를 의미합니다. 고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. 서비스 제공 또는 문제 해결의 필요성이 있고, 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 부처의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 상황이 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 직접 접촉하지 않습니다.
		10.1.2 【대체】 이용자의 데이터 소유권을 명확하게 확립하고 있는가?	고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. 클라우드 서비스 제공업체로서 Tencent Cloud는 국제 사이트 공식 웹사이트에

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			온라인 <u>본서비스</u> <u>General Service Level Agreement</u> 데이터 개인 정보 보호 및 보안 계약 등 법적 문서를 제공하여 Tencent Cloud가 제공하는 서비스 내용과 서비스 수준, 사용자 데이터 및 지식 재산권 보호, 고객과 Tencent Cloud 양측의 보안 책임과 의무 등을 명확히 합니다. 고객은 또한 Tencent Cloud와 오프라인 계약을 체결하여 계약 내 조항 및 세부사항을 협의할 수 있습니다.
			클라우드 서비스 제공자로서, 기술적 조치, 관리 제도 및 보안 아키텍처 설계를 통해 사용자 데이터가 입력, 출력, 전송, 교환 및 저장 전 생애 주기 과정에서의 무결성을 보장합니다.
			데이터 저장 무결성 보장에 대해, Tencent Cloud는 데이터 저장 시 다중 복사본 중복 저장 및 삭제 코드 기술을 사용하고 무결성 오류가 감지될 경우 필요한 복구 조치를 취하여 데이터의 내결함성을 크게 향상시킵니다. Tencent Cloud 전문 팀이 7*24 시간 운영 유지 보수 서비스를 제공하며, 선진 서버 모니터링 및 진단 기술을 활용하여 서버의 각종 장애를 자동으로 감지하고 즉시 자동으로 복구 프로세스를 실행합니다. 선진 원격 관리 도구를 통합하여 데이터센터 현장 및 공급업체 자원을 자동으로 조율하고 서버 장애를 적시에 복구합니다.
10.1.3	【대체】입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 보장하고 있는가?		데이터 전송 무결성 보장에 대해, 고객의 Tencent Cloud 콘솔 통신은 모두 HTTPS 보안 프로토콜의 암호화 보호를 받습니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스 또한 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 데이터가 전송 및 교환 과정에서 변조, 손실되거나 불법 콘텐츠가 삽입되는 것을 방지하고, 데이터 전송 링크의 무결성과 신뢰성을 보장합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
10.1.4	【대체】데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호기능을 이용자에게 제공하고 있는가?	10.1.4 【대체】데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호기능을 이용자에게 제공하고 있는가?	Tencent Cloud 콘솔은 Cloud Access Management (CAM)를 통해 고객에게 안전한 권한 배분과 서브 계정 관리 기능을 제공하여, 고객이 사용자 및 역할이 수행할 수 있는 작업과 접근 가능한 자원을 편리하게 제어할 수 있도록 지원합니다. 고객은 CAM을 통해 마스터 계정과 소속 서브 계정에 2차 신원 인증을 활성화하여 계정 보안을 강화할 수 있으며, CloudAudit를 활용하여 Tencent Cloud 전체 인프라에서 발생하는 사용자 활동 및 API 사용 현황과 관련된 로그를 기록하고 지속적으로 모니터링·보존할 수 있습니다. Tencent Cloud는 또한 Bastion Host (BH)를 제공하여 사용자, 자산, 계정, 운영 권한 등의 차원에 기반한 세분화된 권한 부여를 지원하여, 사용자가 보유한 권한이 자산 접근 및 업무 수행에 필요한 최소한의 권한임을 보장합니다. 베스천 호스트(Bastion Host)도 작업 감사 기능을 지원하여, 사용자의 작업 로그를 기록 및 분석하여 보안 사건의 효과적인 추적을 보장합니다. 고객은 Data Security Audit (DSA) 서비스도 이용할 수 있습니다. CDS는 인공지능 기반의 데이터베이스 보안 감사 시스템으로, 기업 네트워크 내 데이터베이스의 각종 세션 정보, 접근 작업, SQL 구문에 대한 전수 감사 및 데이터베이스 저장을 지원하고, 다양한 규칙 라이브러리와 위협 탐지 엔진을 통해 작업 중의 악의적 행위를 식별하며 관리자에게 즉시 통보하여 상응하는 보안 방어 조치를 취할 수 있도록 합니다. 위변조 방지 측면에서, Tencent Cloud는 고객에게 SSL Certificates 서비스를 제공합니다. 최고 수준의 디지털 인증서 기관(CA) 및 대리점과 협력하여 고객의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			웹사이트와 모바일 애플리케이션에 HTTPS 솔루션을 제공합니다. SSL Certificates는 인증서 신청, 관리 및 배포 기능을 포함한 SSL 인증서 원스톱 서비스를 제공합니다. SSL Certificates는 또한 사용자가 임의 기관에서 발급한 SSL 인증서를 업로드하여 모든 인증서를 통합 관리하고 각 인증서의 유효 기간을 모니터링할 수 있도록 지원합니다. 또한, Tencent Cloud의 여러 저장 및 데이터베이스 제품은 데이터 암호화 기능을 지원하고, 안전한 고강도 암호화 알고리즘을 사용하며, Key Management Service (KMS) 통합을 통해 키 전 생애 주기 관리를 구현하여 데이터의 기밀성을 보장합니다. KMS는 FIPS-140-2 인증을 받은 하드웨어 보안 모듈(HSM)을 사용하여 키를 생성하고 보호하며, 고객의 암호화 키 전 생애 주기 관리를 지원할 수 있습니다. Tencent Cloud는 내부적으로 접근 통제 관리 규정을 수립하고 권한 관리 및 인가 메커니즘을 구축했습니다. Tencent Cloud는 최소 권한 원칙을 엄격히 준수하며, 기본적으로 최소 권한 통제를 시행합니다. Tencent Cloud는 데이터 접근 권한에 대해 전 노드 실명제 심사 및 유지 관리를 시행하여 데이터 자산의 무결성과 비즈니스 서비스의 신뢰성을 보호하며, 실시간 모니터링 및 차단 메커니즘을 구축하여 비정상적인 데이터 접근 행위를 탐지하고 차단합니다. Tencent Cloud는 또한 정기적으로 내부 권한 심사 작업을 조직하여 권한이 남용되거나 오용되지 않도록 보장합니다. Tencent Cloud는 생산 환경에 베스천 호스트(Bastion Host)를 전면 배포하여, 이를 통해 Tencent Cloud 백엔드 시스템 구성 요소의 관리자 계정 권한과 계정 활동을 중앙 집중식으로 관리합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			베스천 호스트(Bastion Host) 접근은 권한 부여 승인이 필요하며, 특정 Tencent Cloud 내부 운영 인원만 접근할 수 있고, 베스천 호스트 로그인에는 적절한 신원 인증이 필요합니다. 백엔드 운영 작업 기록은 모두 로깅 플랫폼에 집중 저장되며, Tencent Cloud 내부 감사팀이 정기적으로 기록을 검토합니다. 다중 테넌트의 데이터 격리에 대해, Tencent Cloud는 "데이터 기밀성" 원칙을 엄격히 준수하며, 가상화 제어층 자원 접근 통제 정책, 클라우드 플랫폼 내부 사설 네트워크 간 격리 정책, 웹 콘솔 권한 할당 및 신원 인증, 인터페이스 세션 ID와 접근 키 등의 보안 메커니즘을 통해 테넌트가 다른 테넌트의 데이터에 접근, 획득 또는 변조할 수 없도록 보장합니다.
10.1.5	【대체】	이용자의 데이터가 처리되는 위치를 추적하기 위한 방안을 제공하고 있는가?	Tencent Cloud의 인프라는 전 세계 여러 지역에 분포되어 있으며, 지역(region)과 가용 영역(zone)으로 구성됩니다. 각 지역은 독립적인 지리적 영역이며, 각 가용 영역은 독립적인 장애 유지보수 도메인으로 각 가용 영역은 물리적으로 격리되어 있습니다. 고객은 비즈니스 발전 요구와 데이터 보안 요구에 따라 데이터와 시스템을 서로 다른 지역 또는 다른 가용 영역에 자유롭게 유연하게 배치할 수 있습니다. Tencent Cloud는 공개적이고 투명한 원칙을 견지하며, 고객이 데이터 저장 위치 등의 정보, 즉 데이터가 저장된 데이터센터 위치, 데이터 콜드 백업 상황 및 콜드 백업 데이터의 저장 위치 등을 알아야 할 경우, Tencent Cloud는 적절한 채널을 통해 고객에게 정보를 적시에 제공합니다.
10.1.6	【필수】	이용자의 클라우드서비스 이용계약 종료 시 이용자의 모든	고객이 비즈니스 변경 또는 향후 IT 계획 수립으로 인해 계약 합의를 종료해야 할 경우, 언제든지 클라우드 데이터와 생산

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		가상자원은 불가능하도록 하는가?	복구가 삭제하고 환경에 대해 백업 및 마이그레이션을 선택할 수 있습니다. 고객의 서비스가 종료된 후 Tencent Cloud는 엄격한 데이터 삭제 방식을 따릅니다. 보존 기간 만료 후 복제본 및 백업을 포함한 고객 데이터를 완전히 삭제하며, 삭제된 데이터는 복원할 수 없습니다.
			Tencent Cloud의 여러 저장 및 데이터베이스 제품은 데이터 암호화 기능을 지원하고, 안전한 고강도 암호화 알고리즘을 사용하며, Key Management Service (KMS) 통합을 통해 키 전 생애 주기 관리를 구현하여 데이터의 기밀성을 보장합니다. KMS는 FIPS-140-2 인증을 받은 하드웨어 보안 모듈(HSM)을 사용하여 키를 생성하고 보호하며, 고객의 암호화 키 전 생애 주기 관리를 지원할 수 있습니다. 키가 해독되거나 악용될 위험을 줄이기 위해 KMS는 키 순환을 지원하고, 효력을 잃은, 폐기된, 또는 유출된 키를 안전하고 신뢰할 수 있는 방법으로 삭제합니다. 삭제된 키는 복구할 수 없으며, 해당 키로 암호화된 데이터도 더 이상 복호화할 수 없습니다.
10.2	암호화	10.2.1 【대체】이용자 데이터 처리 시 암호화를 적용하여 보호하고 있는가?	
		10.2.2 【대체】암호키의 안전한 관리 절차를 수립하고 안전하게 보관하고 있는가?	Tencent Cloud는 내부적으로도 암호화 및 키 관리 기준을 수립하여 키의 신청, 생성, 저장, 사용, 전달, 갱신, 파기 등 과정의 보안 요구사항을 명확히 했습니다. 키 수명 주기와 관련된 모든 작업은 이중 통제, 엄격한 인수인계, 적절한 보관, 적시 갱신의 기본 요구사항을 이행합니다. 키 사용 과정에서 책임과 권한 분리, 엄격한 승인, 실명 확인 후 작업 수행 등 요구사항을 준수하고, 비즈니스 키 조작 로그를 보존하며 정기적으로 조작 감사를 수행합니다. 또한, Tencent Cloud는 키 용도, 키가 보호하는 데이터의 민감도, 키 유출 가능성 및 영향성 등의 요소를 종합적으로 고려하여 키의 전 생애 주기를

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
관리합니다.			

6.4.11 물리적 보안

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
11.1	물리적 보호구역	11.1.1 【필수】 전산실 내 주요시설에 출입통제, 감시제어를 위한 설비가 마련되어 있는가?	물리적 접근 통제 측면에서 Tencent Cloud는 데이터센터 운영사에 인원 범주와 접근 권한에 따라 출입 통제 승인 시스템 내 완전한 인력 접근 통제 보안 매트릭스를 구축하여, 각종 인원의 접근 및 운영 행위를 효과적으로 관리 및 통제하도록 요구합니다. Tencent Cloud는 운영사에 데이터센터에 출입하는 각종 방문객이나 직원에 대한 신원 확인과 휴대품 검사를 실시하고, 그들이 휴대한 물품을 등록하도록 요구합니다. 보안 및 모니터링 측면에서 Tencent Cloud는 운영사에 보안 요원을 배치하여 엄격히 점검 목록과 점검 계획에 따라 각 기기실 및 장비 상황을 순찰하며, 각 검사 지점에서 서명 및 점검 시간을 기록하도록 요구하고, 기반 시설 장애나 보안 사건이 발견될 경우 즉시 데이터센터 비상 사건 대응 절차를 가동하도록 합니다. Tencent Cloud는 또한 운영사에 데이터센터에 7*24 시간 사각지대 없는 비디오 모니터링 경보 시스템을 설치하고, 보안실에서 이를 감시하며, 모니터링 기록을 안전하게 저장하고 충분한 시간 동안 보관하도록 요구합니다.
		11.1.2 【필수】 고유식별정보 또는 개인신용정보를 처리하는 경우 전산실 내 무선통신망 사용을 제한(통제) 하고 있는가?	Tencent Cloud 무선 네트워크는 보안 정책을 활성화하여 직원이 무선 네트워크에 로그인할 때 신원 인증이 필요합니다. 동시에 기업 IT 관리 백엔드는 무선 SSID와 AP를 검사하며, 불법 SSID와 AP가 발견되면 관련 IT 관리자에게 경보를 보내 처리하도록

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			합니다.
		11.1.3 【대체】사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하고 있는가?	물리적 환경 보안 측면에서, Tencent Cloud는 물리적 보안 관리 제도를 수립하여 운영 안전을 규제하고, 위험을 적시에 식별하며, 물리적 보안 관리를 강화하고 있습니다. Tencent Cloud는 회사 보안 구역을 중요 보안 구역과 일반 보안 구역으로 구분하고, 보안 경계, 출입 통제 및 검사, 그리고 비디오 감시 장치를 설치합니다. Tencent Cloud는 직원에게 민감한 정보가 포함된 종이 문서 등을 포함한 업무 환경 내 정보 자산의 안전을 유지하도록 요구합니다. Tencent Cloud 직원 단말에는 잠금 정책이 설정되어 직원이 단말 장치를 떠날 때 장치가 잠기도록 합니다. 복사기, 팩스, 문서 파쇄기, 프린터 등의 무인 장비는 승인되지 않은 사용과 침입을 피하기 위해 업무 구역 내 감시가 가능한 적절한 위치에 배치됩니다.
11.2	정보처리 시설 및	11.2.1 【필수】고유식별정보 및 개인신용정보를 처리하는 모든 정보처리시스템을 국내에 설치하고 있는가?	현재 Tencent Cloud는 한국에 두 개의 데이터센터를 보유하고 있으며, 클라우드 서버, 클라우드 데이터베이스, 클라우드 스토리지 등을 포함한 다양한 클라우드 컴퓨팅 서비스를 제공합니다. 한국 고객은 한국 현지에서 자신의 데이터를 저장, 처리 및 백업할 수 있습니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud는 사업장 소재 관할권의 법률 및 규정을 엄격히 준수하며, 정보 보안 운영이 관련 법률, 규정, 표준 및 절차 요건에 부합하도록 보안 및 규정 준수 관련 절차를 마련하였습니다. Tencent Cloud는 공개적이고 투명한 원칙을 견지하며, 고객이 데이터 저장

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			위치 등의 정보, 즉 데이터가 저장된 데이터센터 위치, 데이터 콜드 백업 상황 및 콜드 백업 데이터의 저장 위치 등을 알아야 할 경우, Tencent Cloud는 적절한 채널을 통해 고객에게 정보를 적시에 제공합니다. 또한 Tencent Cloud의 개인정보 수집, 처리 및 공유에 관한 자세한 정보는 개인 정보 처리 방침을 참조하시기 바랍니다.
		11.2.2 【필수】각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재 감지기, 소화 설비, 누수 감지기, 항온 항습기, 무정전 전원장치(UPS), 이중 전원선 등의 설비를 갖추고 있는가?	Tencent Cloud는 고객에게 안전하고 안정적이며 지속적이고 신뢰할 수 있는 물리적 시설 기반을 제공하기 위해 노력하. Tencent Cloud는 전 세계의 각 데이터센터를 관련 국제 표준 및 현지 안전 요구사항에 따라 입지 선정, 건설 또는 임대하여 환경적 위험을 충분히 고려하고 높은 확률의 환경 위험 지역을 피합니다. 현재 Tencent Cloud는 한국에 두 개의 임대형 데이터센터를 구축했습니다. Tencent Cloud는 운영사에 데이터센터에 완전한 소방 시스템(지정 구역 화재 감지 시스템, 자동 소화 시스템, 비상 사용용 수동 소화 장치 등)을 설치하도록 요구합니다. Tencent Cloud는 또한 운영사에 데이터센터에 피뢰 시스템, 방사선 차단 시스템, 전력 공급 시스템, UPS 시스템, 조명 시스템 등 컴퓨터실 정상 작동에 필요한 시설을 설치하도록 요구하며, 데이터센터 유지보수 인력이 교대로 근무하여 24 시간 유지보수 및 장비 장애 신속 해결을 보장하도록 합니다.
		11.2.3 【대체】정보처리시설 내 이용자 정보(자료)가 저장된 장비를 폐기하는 경우 복구가 불가능하도록 처리하고 있는가?	Tencent Cloud 서비스 제공에 사용되는 매체에 장애가 발생하여 교체가 필요하거나 사용 기한이 도래하여 폐기해야 할 경우, Tencent Cloud는 엄격한 절차에 따라 안전한 물리적 파기 방식을 통해 하드 디스크가 완전히

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			파기되도록 하고, 파기 기록에 등록합니다.

6.5 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획

"<별표 2의 3> 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획"은 금융회사 또는 전자금융서비스 제공자가 클라우드 서비스 이용 과정에서 비즈니스 연속성 측면에서 계획하고 시행해야 할 대책을 포함하고 있으며, "필수 사항"과 "추가 사항"으로 구분됩니다. 본 규정 제 14 조의 2 제 1 항 제 1 호에 따르면, 사용되는 클라우드 컴퓨팅 서비스가 중요 업무로 분류되는 경우, 금융회사 또는 전자금융서비스 제공자는 "필수 사항"과 "추가 사항"을 모두 준수해야 합니다. 사용되는 클라우드 컴퓨팅 서비스가 비중요 업무로 분류되는 경우, "필수 사항"만 준수하면 됩니다.

<별표 2의 3> "필수 사항"은 본 규정 조항 원문에 대한 인용이므로, 이에 대응하는 준수성 답변은 본 가이드 [제 6.1 장 "전자금융거래의 안전성 확보 및 이용자 보호"](#), [제 6.2 장 "허가 및 등록의 세부요건"](#), 그리고 [제 6.3 장 "전자금융업무의 감독"](#)의 관련 내용을 참조하시기 바랍니다. 본 장에서는 주로 <별표 2의 3> "추가 사항"을 중심으로, Tencent Cloud가 클라우드 서비스 제공자로서 금융회사 등이 관련 요구사항을 준수하도록 어떻게 지원하는지 설명합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
1	데이터 백업 등 장애 대비	【필수 사항】: 제 13 조 ④ 4 : 비상시에 대비하여 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것. 제 13 조 ④ 6-7: 6. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것 7. 주요 백업 전산자료에 대하여 정기적으로 검증할 것 제 14 조 1-3: 1. 다음 각 목을	고객은 백업 시, 클라우드 서비스 관련 중요 구성 파일, 가상 시스템 이미지 등을 데이터 백업 대상에 포함하여야 합니다. Tencent Cloud가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 컨테이너 및 미들웨어 서비스 등 다양한 클라우드 제품/서비스는 모두고가용성 특징을 갖추고 있어, 고객이 네트워크 보안 사건 발생 후 신속히 대응하고 핵심 기능을 복구할 수 있도록 보장합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		작성 · 보관 할 것	예를 들면 다음과 같습니다:
		가. 주요 정보처리시스템에 대한 운영매뉴얼	• Cloud Virtual Machine (CVM) 은 서비스 고가용성과 데이터 고신뢰성의 특성을 갖추고 있습니다. CVM 에 탑재된 클라우드 디스크는 3 중 복사본 저장 전략을 제공하여 데이터가 어느 한 복사본에 장애가 발생할 경우 빠르게 데이터를 이전하고 복구할 수 있도록 보장합니다.
		나. 주요 정보처리시스템에 대한 정기적인 유지보수 실시 내용을 기록한 유지보수관리대장	• Tencent Kubernetes Engine (TKE) 는 분산 서비스 아키텍처를 채택하여 서비스의 장애 자동 복구 및 빠른 이전을 보장합니다. 상태 유지 서비스 백엔드의 분산 저장과 결합하여 서비스와 데이터의 안전 및 고가용성을 실현합니다.
		다. 정보처리시스템에 대한 책임자명부 및 장애상황기록부	
		2. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능하도록 모니터링시스템을 갖출 것	
		3. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것.	
		제 14 조 5: 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1 년 이상 기록 · 관리할 것.	Tencent Cloud 에서 제공하는 다양한 저장 서비스와 데이터베이스 서비스는 모두 백업 기능을 갖추고 있어 고객의 다양한 백업 요구를 충족시킵니다. 예를 들어:
		제 50 조 ① 3: 전산장애 발생 시 전산자료 손실에 대비한 백업(backup)장치를 구비할 것	• 고객이 Cloud Object Storage (COS) 에 저장한 데이터는 교차 리전 복제 기능을 통해 여러 지정된 리전에 동시에 저장될 수 있어, 예기치 않게 일부 데이터가 손실된 경우에도 중복 데이터를 통해 완전한 데이터를 찾아 복구할 수 있으며, 하나의 가용 구역 저장소가 불가항력적인 재해로 손상을 입을 경우 발생할 수 있는 손실을 방지하여 다중 중복 백업과 재해 복구 효과를 달성할 수 있습니다.
		【 추가 사항 】 : 클라우드서비스와 관련된 중요 설정파일, 가 상 시스템 이미지 등을 데이터 백업 대상에 포함	• Cloud Block Storage (CBS) 의 스냅샷 백업 기능은 CBS 의 특정 시점 스냅샷을 생성하여

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			데이터를 백업함으로써 변조 및 실수로 인한 삭제로 인한 데이터 손실을 방지하고, 비즈니스 장애 시 신속한 롤백이 가능하도록 보장합니다. Cloud File Storage (CFS) 은 정기적인 스냅샷 기능을 제공하여 고객이 유연하게 백업 작업 전략을 설정할 수 있도록 하며, 서로 다른 비즈니스에 대해 서로 다른 정기 스냅샷 전략을 채택할 것을 권장합니다. Cloud Native Database TDSQL-C 는 논리적 백업과 스냅샷 백업 두 가지 백업 유형을 지원하며, 완전한 데이터 백업과 이후 일정 기간 동안의 binlog 백업을 통해 전체 TDSQL-C MySQL 클러스터나 특정 데이터베이스/테이블을 임의의 시점으로 복구할 수 있습니다. TencentDB for MySQL 은 데이터베이스를 백업하기 위한 자동 백업과 수동 백업 두 가지 방식을 지원하며, 교차 리전 백업 기능을 제공하여 고객의 재해 복구 능력을 향상시키고 동시에 데이터의 신뢰성을 높입니다. TencentDB for MongoDB 는 데이터의 자동 백업과 무손실 복구 메커니즘을 제공하며, 다중 노드 백업 데이터를 지원합니다. 고객은 백업 메커니즘을 통해 여러 날 동안의 백업 데이터를 저장하여 재해 상황 시 데이터 복구를 용이하게 할 수 있습니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 내부적으로 백업

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
2	이중화 또는 예비장치 확보 등	【필수 사항】: 제 23 조③: 금융회사 또는 전자금융업자는 제 1 항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1 회 이상 점검하여 최신상태로 유지하고 관리하여야 한다. 제 23 조⑦: 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다. 【추가 사항】: 클라우드 서비스 제공과 관련된 지리적 특성, 동시 장애 발생 가능성 등을 고려하여 중복 설계 및 구성	관리 절차를 수립하여, 관련 법규 요구사항에 따라 수집 및 처리된 중요한 데이터를 백업합니다. 내부 중요 정보에 대해서는, Tencent Cloud 가 데이터 등급에 기반하여 서로 다른 데이터의 백업 전략을 수립하고 정기적으로 복구 테스트를 수행합니다. Tencent Cloud 는 백업 전략에 따라 서버, 네트워크 장비, 응용 시스템의 구성 파일, 로그 등의 정보를 백업하여, 파일 손상 시 신속히 복구될 수 있도록 합니다. 고객은 클라우드 서비스의 지리적 특성 및 동시 장애 발생 가능성 등을 고려하여 이중화 메커니즘을 설계·구현하여야 합니다. Tencent Cloud 데이터 센터는 중국 본토, 아시아 태평양 지역, 북미 지역, 유럽 지역을 커버하며 지역(region)과 가용 영역(zone)으로 구성됩니다. Tencent Cloud 의 서로 다른 지역 간은 완전히 격리되어 있으며, 각 지역은 다시 여러 개의 상호 격리된 가용 영역으로 구분됩니다. 현재 Tencent Cloud 는 한국 내에 전력과 네트워크가 상호 독립된 두 개의 데이터 센터를 보유하고 있어, 고객이 한국 내에서 데이터를 저장, 처리 및 백업할 수 있도록 지원합니다. 고객은 비즈니스 발전 요구와 데이터 보안 요구에 따라 데이터와 시스템을 서로 다른 지역 또는 가용 영역에 자유롭게 배포 및 백업하여 비즈니스의 재해 복구 요구사항을 충족할 수 있습니다. Tencent Cloud 가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 저장 서비스, 데이터베이스 서비스, 컨테이너 및 미들웨어 서비스 등 다양한 클라우드 제품/서비스는 모두 고가용성 특성을 갖추고 있어 고객이

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			시스템 또는 서비스의 고가용성을 실현하는 데 도움을 줍니다. 예를 들면: Cloud Load Balancer (CLB) 는 안전하고 빠른 4/7 계층 트래픽 분산 서비스를 제공하여, 트래픽 분산을 통해 애플리케이션 시스템의 외부 서비스 역량을 확장하고 단일 장애점을 제거합니다. CLB 는 클러스터 배포를 채택하며, 장애 인스턴스를 신속히 제거하여 고가용성을 실현합니다. Cloud Virtual Machine (CVM) 은 서비스 고가용성과 데이터 고신뢰성의 특성을 갖추고 있습니다. CVM 에 탑재된 클라우드 디스크는 3 중 복사본 저장 전략을 제공하여 데이터가 어느 한 복사본에 장애가 발생할 경우 빠르게 데이터를 이전하고 복구할 수 있도록 보장합니다. Cloud Object Storage (COS) 은 데이터의 다중 아키텍처, 다중 장치 간 중복 저장을 제공하여 사용자 데이터에 재해 복구 및 자원 격리 기능을 제공하여 데이터 지속성을 실현합니다. Cloud Native Database TDSQL-C: Tencent Cloud 의 자체 연구 개발 차세대 클라우드 네이티브 관계형 데이터베이스로서, 고가용성 클러스터 아키텍처를 채택하여 장애 노드를 자동 감지할 수 있으며, 초 단위 장애 전환 및 복구를 지원합니다. TencentDB for MySQL 은 데이터의 고신뢰성과 서비스의 고가용성을 실현하며, 완벽한 데이터 자동 백업 및 무손실

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			복구 메커니즘을 보유하고 있습니다. Tencent Kubernetes Engine (TKE) 는 분산 서비스 아키텍처를 채택하여 서비스의 장애 자동 복구 및 빠른 이전을 보장합니다. 상태 유지 서비스 백엔드의 분산 저장과 결합하여 서비스와 데이터의 안전 및 고가용성을 실현합니다. 고객 비즈니스의 지속적인 가용성을 보장하기 위해 Tencent Cloud 는 클라우드 제품이 단일 지역 내에서 여러 데이터 센터를 활용한 다중화 메커니즘을 적용하도록 요구합니다. 고객 비즈니스의 지속적 가용성을 보장하기 위해 Tencent Cloud 는 서버, 네트워크 장비, 보안 장비 등의 하드웨어 장비에 대해 중복 또는 핫 스탠바이 메커니즘을 설정하여 하드웨어 장애 발생 시 데이터가 손실되지 않고 비즈니스가 복구될 수 있도록 보장합니다.
3	훈련 및 사고 관리	【필수 사항】: 제 15 조④: 금융회사 또는 전자금융업자는 해킹 등 전자적 침해의 예방, 피해 최소화 및 신속한 복구를 위한 대책을 수립·운용하여야 한다. 제 16 조: 금융회사 또는 전자금융업자는 악성코드 감염·확산 방지, 피해 최소화 및 복구를 위한 대책을 수립·운용하여야 한다. 제 23 조④: 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립·준수하여야	고객은 사고 관리 및 관련 훈련 계획에 클라우드 서비스 제공자의 역할, 책임, 비상 연락망 등의 내용을 포함하여야 합니다. 고객이 규제 요구사항을 충족하도록 지원하기 위해, Tencent Cloud 의 비즈니스 연속성 관련 절차는 재해 사고 기간의 내부/외부 커뮤니케이션 전략을 명확히 하고, 다중 채널 커뮤니케이션 방식을 구축했으며, 이는 콘솔 공지, 공식 웹사이트, 사이트 내 메시지, SMS 및 이메일 등을 포함하여 고객에게 영향을 미칠 수 있는 사건을 적시에 발표할 수 있도록 합니다. Tencent Cloud 는 클라우드 콘솔을 통해 작업 티켓 서비스를 제공하여,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		한다.	고객이 보안, 가용성 및 기밀성과 관련된 장애, 사건, 문제 및 불만을 보고할 수 있도록 지원합니다. Tencent Cloud 작업 티켓 시스템은 계층별 응답 메커니즘을 통해 고객 작업 티켓에 우선순위를 할당하며, 일선 기술 팀이 효과적으로 해결할 수 없는 경우 시스템이 자동으로 서비스 에스컬레이션 절차를 트리거하여 제품 또는 기술 팀이 개입해 협력 처리함으로써 고객의 요구나 피드백이 적시에 응답 및 처리되도록 보장합니다. Tencent Cloud 는 또한 공식 웹사이트에 온라인 및 전화 채널을 제공하여, 고객이 Tencent Cloud 서비스 사용 시 발생하는 문제를 피드백할 수 있도록 지원합니다. Tencent Cloud 는 다중 지역 상호 백업 고객 서비스 센터를 보유하고 있어, 고객의 문의 또는 요구를 7*24 시간 중단 없이 처리하며, 고품질, 24 시간 기술 지원을 제공할 수 있습니다. 또한 고객은 적용 가능한 서비스 플랜을 선택하여, 전용 지원 그룹, 전용 기술 서비스 매니저, 부가가치 서비스 등으로 구성된 전용 지원을 받을 수 있습니다.
		1. 상황별 대응절차	현지 지원 측면에서, Tencent Cloud 는 정보 보안 연락 담당자를 지정했으며, 각 지역의 정보 보안 연락 담당자는 규정 준수 및 업무 요구사항에 따라 현지 규제 기관 및 고객과 원활한 소통을 유지하여 Tencent Cloud 가 법률, 규제 및 계약 합의를 준수하도록 합니다.
		2. 백업 또는 재해복구센터를 활용한 재해복구계획	적절한 경우 Tencent Cloud 는 고객의 보안 훈련에 관련 기술 지원을 제공할 수도 있습니다.
		3. 비상대응조직의 구성 및 운용	
		4. 입력대행, 수작업 등의 조건 및 절차	
		5. 모의훈련의 실시	
		6. 유관기관 및 관련업체와의 비상연락체제 구축	
		7. 보고 및 대외통보의 범위와 절차 등	
		8. 비상지원인력의 확보 및 운영	
		제 23 조③-⑥: ③ 금융회사 또는 전자금융업자는 제 1 항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1 회 이상 점검하여 최신상태로 유지하고 관리하여야 한다.	
		④ 「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의 「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립·준수하고 이를 금융위원회에 알려야 한다.	
		⑤ 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운용하여야 한다.	
		⑥ 제 4 항에 따른 행동매뉴얼 또는 제 5 항에 따른 비상대책에는	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		제 1 항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.	
		제 23 조⑧-⑩: ⑧ 다음 각 호의 금융회사 및 전자금융업자는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정거리 이상 떨어진 안전한 장소에 구축·운영하여야 한다.	
		⑨ 제 8 항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3 시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24 시간 이내로 한다.	
		⑩ 제 8 항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1 회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다.	
		제 24 조①-④: ① 금융회사 또는 전자금융업자는 제 23 조제 4 항에 따른 행동매뉴얼 또는 같은 조 제 5 항에 따른 비상대책에 따라 연 1 회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제 23 조제 10 항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다.	
		② 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		합동비상대응훈련을 실시할 수 있다. ③ 금융위원회는 제 2 항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다. 1. 「정부조직법」 제 17 조에 따른 "국가정보원(국가사이버안전센터)" 2. 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」 제 12 조에 따른 "경찰청(사이버수사국)" 3. 침해사고대응기관 4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관 ④ 금융회사 또는 전자금융업자는 제 1 항 및 제 2 항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다. 제 37 조의 6 ⑤ : 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 연 1 회 이상 침해사고 대응 및 복구훈련 계획을 수립·시행하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게 제출하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다. 1. 법 제 2 조제 3 호가목의 금융회사 중 신용협동조합 2. 법 제 2 조제 3 호다목·라목의 금융회사 3. 시행령 제 2 조제 4 호부터 제 6 호까지의 조합 4. 시행령 제 5 조제 2 항의 요건을	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		충족한 금융회사.	
		【 추가 사항 】 : 훈련 및 사고관리 계획에 클라우드서비스 제공자 의 역할, 책임, 비상연락망 등을 포함	
4	비상대책 수립	【 필수 사항 】 : 제 23 조⑤: 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운영하여야 한다. 【 추가 사항 】 : 계약 변경, 파산 등과 같은 중대한 상황 발생에 대비한 공급 대체 방안, 업무 복구 가능성 식별 등 출구전략 수립	고객은 계약 변경, 파산 등 중대한 사건에 대비한 공급 대체 방안, 퇴출 전략 등을 수립하여 사업의 복구 가능성을 보장하여야 합니다. 클라우드 서비스 제공업체로서 Tencent Cloud 는 국제 사이트 공식 웹사이트에 온라인 본서비스 General Service Level Agreement 데이터 개인 정보 보호 및 보안 계약 등 법적 문서를 제공하여 Tencent Cloud 가 제공하는 서비스 내용과 서비스 수준, 사용자 데이터 및 지식 재산권 보호, 고객과 Tencent Cloud 양측의 보안 책임과 의무 등을 명확히 합니다. 고객은 또한 Tencent Cloud 와 오프라인 계약을 체결하여 계약 내 조항 및 세부사항을 협의할 수 있습니다. 고객이 비즈니스 변경 또는 향후 IT 계획 수립으로 인해 계약 합의를 종료해야 할 경우, 언제든지 클라우드 데이터와 생산 환경에 대해 백업 및 마이그레이션을 선택할 수 있습니다. Tencent Cloud 는 고객이 일반적인 표준 형식을 사용하여 데이터를 백업하거나 마이그레이션할 수 있도록 지원합니다. 따라서 고객은 클라우드 도입 단계와 동일한 전송 방식 및 프로토콜을 사용하거나, Direct Connect (DC), VPN Connection 등의 네트워크 서비스 제품을 활용하여 데이터의 클라우드 이탈 시에도 안전성과 신뢰성을 보장할 수 있습니다. Tencent Cloud 와 고객 간의 서비스 계약에 따라, 클라우드 서비스 만료 또는 종료 시 고객이 Tencent Cloud 서비스를

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			사용하며 클라우드 서버에 저장한 데이터는, 보존 기간 만료 전에 반드시 데이터 마이그레이션을 완료해야 합니다. 고객의 서비스가 종료된 후 Tencent Cloud 는 엄격한 데이터 삭제 방식을 따릅니다. 보존 기간 만료 후 복제본 및 백업을 포함한 고객 데이터를 완전히 삭제하며, 삭제된 데이터는 복원할 수 없습니다. 제품/서비스 변경 또는 종료 통지와 관련하여, Tencent Cloud 는 공지사항, 이메일, Tencent Cloud 콘솔 내 메시지 또는 기타 적절한 채널을 통해 고객에게 통보하며, 제품 또는 서비스의 기능, 버전, 변경사항 등의 정보를 공개적으로 발표합니다.

6.6 클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치

"<별표 2 의 4>클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치"에는 금융회사 또는 전자금융서비스 제공자가 클라우드 서비스 이용 과정에서 클라우드 서비스 관련 안전사고를 예방하기 위해 취해야 할 안전 대책이 포함되어 있으며, "필수 사항"과 "추가 사항"으로 구분됩니다. 본 규정 제 14 조의 2 제 1 항 제 1 호에 따르면, 사용되는 클라우드컴퓨팅서비스가 중요 업무로 분류되는 경우, 금융회사 또는 전자금융서비스 제공자는 "필수 사항"과 "추가 사항"을 모두 준수하여야 합니다. 사용되는 클라우드컴퓨팅서비스가 비중요 업무로 분류되는 경우, "필수 사항"만 준수하면 됩니다.

<별표 2 의 4>의 "필수 사항"은 본 규정 조항 원문에 대한 인용이므로, 이에 대응하는 준수성 답변은 본 가이드 [제 6.1 장 "전자금융거래의 안전성 확보 및 이용자 보호"](#) 및 [제 6.2 장 "허가 및 등록의 세부요건"](#), 그리고 [제 6.3 장 "전자금융업무의 감독"](#)의 관련 내용을 참조하시기 바랍니다. 본 장에서는 주로 <별표 2 의 4>의 "추가 사항"을 중심으로, Tencent Cloud 가 클라우드 서비스

제공자로서 금융회사 등이 관련 요구사항을 준수하도록 어떻게 지원하는지 설명합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
1	계정관리	【필수 사항】: 제 13 조①1: 사용자 인증 수단을 개인별로 부여하고 접근권한은 최소한으로 부여하는 등 적절한 접근권한 관리 및 통제 절차를 수립·운용할 것 제 13 조①11: 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것 제 13 조②: 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다. 제 14 조 6: 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 이중인증 절차를 시행하고, 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하며, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것 제 17 조 2: 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 이중 인증수단을 적용할 것 【추가 사항】: 클라우드 관리 콘솔에 접근하는 관리자 계정에 대한 이중인증 등 강화된 보안조치 적용	고객은 클라우드 관리 콘솔에 접근하는 관리자 계정에 이중 인증(2FA) 등 보안 조치를 실시하여야 합니다. 클라우드 사용자 접근 제어 관리 측면에서, Tencent Cloud 는 클라우드 고객에게 접근 제어 관리 기능을 제공하여 고객이 자체적으로 접근 제어 정책을 수립하고, 해당 정책을 통해 구매한 클라우드 제품에 대한 접근을 관리할 수 있도록 합니다. Tencent Cloud 는 고객에게 관리 콘솔을 제공하여 고객이 클라우드 자원을 중앙 집중식으로 관리 및 통제할 수 있도록 지원합니다. 고객이 클라우드 계정을 등록할 때, 각 클라우드 고객에게 고유하게 식별 가능한 계정이 할당되며 비밀번호 설정 규칙/정책이 구성되고, 관리 콘솔은 사용자 계정 이름의 고유성을 자동으로 확인합니다. 고객이 관리 콘솔에 로그인할 때, 신원 및 인증 정보 그리고 운영 명령은 HTTPS 프로토콜을 통해 전송됩니다. 고객은 공개 API 를 통해 클라우드 서비스와 데이터를 중앙 집중식으로 관리할 수 있습니다. 고객이 Open API 기능을 등록할 때, 각 고객에게 할당된 접근 키를 적용하여 인증해야 합니다. Tencent Cloud 는 고객이 다중 요소 인증을 활용하여 계정 로그인 및 비밀번호 변경과 같은 민감한 작업의 보안성을 강화하도록 지원합니다. Tencent Cloud 는 또한 계정 비밀번호 재설정 및 수정 기능을 제공합니다. Tencent Cloud 는 또한 고객에게 Cloud Access Management (CAM)를 제공하여 고객이 Tencent Cloud 제품 및 자원에 대한 접근을 관리할 수 있도록 돕습니다. 여기서 사용자

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			마스터 계정은 서버 사용자를 생성하고 서버 사용자에게 신원 ID, 신원 증명 및 권한을 할당할 수 있습니다. 사용자는 접근 관리 콘솔을 통해 서버 사용자의 비밀번호 규칙(비밀번호 복잡성, 길이, 유효 기간 등 포함) 및 단일 로그인 세션 만료 시간을 수정할 수 있습니다. 비밀번호 유출을 방지하기 위해 Tencent Cloud 는 비밀번호에 SHA256 해시 암호화 및 소금 처리를 적용하여 평문 비밀번호 저장을 피합니다. CAM 은 또한 다양한 방식의 이차 인증 기능을 지원하며, CloudAudit 를 통해 Tencent Cloud 계정 활동에 대한 감독, 규정 준수 점검, 작업 검토 및 위험 검토를 지원합니다. Tencent Cloud 는 또한 Bastion Host (BH)를 제공하여 고객이 사용자 관리, 권한 부여 관리, 인증 관리 및 종합 감사를 수행할 수 있도록 지원합니다. 베스천 호스트는 사용자 시나리오의 실제 필요에 따라 정적 비밀번호, LDAP 등 다양한 유형의 인증 방식을 다른 사용자에게 제공할 수 있습니다. 보안성을 강화하기 위해 Tencent Cloud 베스천 호스트는 사용자가 이중 요소 인증을 사용할 수 있도록 지원합니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 내부적으로 접근 제어 관리 기준을 수립하여, 사용자 계정이 고유 식별자를 사용하도록 요구하며, 보안 기준에 따라 직원 계정에 대한 비밀번호 정책을 설정합니다. Tencent Cloud 는 제로 트러스트 보안 관리 시스템을 통해 직원의 접근 인증을 수행하며, 사용자가 내부 자원에 접근하기 위해서는 먼저 이중 요소 신원 인증을 완료해야 합니다. Tencent Cloud 는 내부적으로 권한 부여 정책 및 권한 분리 매트릭스 메커니즘을 수립하고, 직위 역할에 해당하는 인원

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			신원 정보와 각 비즈니스 시스템의 권한 수준 기록을 유지 관리합니다. Tencent Cloud 생산 환경에는 베스천 호스트(Bastion Host)가 전면 배포되어 있으며, 이를 통해 백엔드 시스템 구성 요소의 관리자 계정 권한을 중앙 집중식으로 통제합니다. 내부 운영 인원이 베스천 호스트에 접근하려면 권한 부여 승인이 필요하며, 특정 Tencent Cloud 내부 운영 인원만 접근할 수 있고, 베스천 호스트 로그인 시 이중 요소 인증이 필요합니다. 운영 작업 기록은 로깅 플랫폼에 집중 저장되며, Tencent Cloud 내부 감사팀이 정기적으로 로그를 검토합니다.
2	접근통제	【필수 사항】: 제 13 조①2-3: 2. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것 3. 전산자료 및 전산장비의 반출·반입을 통제할 것 제 13 조 ③ :금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운영하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제 28 조제 2 항에 따라 이중확인 및 모니터링을 하여야 한다. 제 19 조의 2: 금융회사 또는 전자금융업자는 비밀번호, 생체정보 등 사용자 인증수단 유출을 방지하기 위하여 인증수단의 발급·보관·주기적 변경 및 인증오류 발생시 처리 절차 등을 포함한 관리방안을 수립·운영하여야 한다.	고객은 클라우드 자원의 접근 절차를 문서화하고, 콘솔 관리자 계정은 별도로 격리된 단말에서만 접근하도록 제한하여야 합니다. Tencent Cloud 관련 제품의 조작 가이드, 사용자 매뉴얼 등은 문서화되어 공식 웹사이트를 통해 고객에게 제공됩니다. Tencent Cloud 는 또한 고객에게 Tencent Cloud 제품 상식 및 관련 전문 능력에 기반한 Tencent Cloud Training and Certification 을 제공하여 고객의 기술 역량과 클라우드 숙련도를 향상시킵니다. 특권 계정의 접근 제어 측면에서, Tencent Cloud 는 또한 Bastion Host (BH)를 제공하여 사용자, 자산, 계정, 운영 권한 등의 차원에 기반한 세분화된 권한 부여를 지원하여, 사용자가 보유한 권한이 자산 접근 및 업무 수행에 필요한 최소한의 권한임을 보장합니다. 베스천 호스트는 통합 진입점으로 내부 자산의 관리 및 유지보수를 수행할 수 있습니다. 베스천 호스트(Bastion Host)도 작업 감사 기능을 지원하여, 사용자의 작업

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		【추가 사항】: 클라우드시스템 접근 절차를 문서화하고 관리 콘솔 관리자 계정의 경우 별도로 분리된 단말에서만 접근하도록 조치	로그를 기록 및 분석하여 보안 사건의 효과적인 추적을 보장합니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 내부적으로 특별 접근 권한의 관리 요구사항 및 관련 권한 부여 메커니즘을 명확히 했습니다. Tencent Cloud 생산 환경에는 베스천 호스트(Bastion Host)가 전면 배포되어 있으며, 이를 통해 백엔드 시스템 구성 요소의 관리자 계정 권한을 중앙 집중식으로 통제합니다. 내부 운영 인원이 베스천 호스트에 접근하려면 권한 부여 승인이 필요하며, 특정 Tencent Cloud 내부 운영 인원만 접근할 수 있고, 베스천 호스트 로그인 시 이중 요소 인증이 필요합니다. 운영 작업 기록은 로깅 플랫폼에 집중 저장되며, Tencent Cloud 내부 감사팀이 정기적으로 로그를 검토합니다.
3	네트워크 보안	【필수 사항】: 제 15 조①3: 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지. 다만, 다음 각 목의 경우에는 그러하지 아니하다. 가. 이용자의 고유식별정보 또는 개인신용정보(「신용정보의 이용 및 보호에 관한 법률」 제 40 조의 2 에 따른 가명처리에 관한 행위규칙을 준수한 가명정보는 제외)를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한한다) 나. 업무상 불가피한 경우로서	고객은 내부 시스템과 클라우드 시스템 간의 데이터 교환을 식별·관리하고, 시스템 간 및 클라우드 서비스 내부의 주요 통신 채널에 암호화를 적용하여야 합니다. 고객의 Tencent Cloud 콘솔 상의 모든 통신은 HTTPS 보안 프로토콜의 암호화 보호를 받습니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스는 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 고객의 비즈니스에 포트 수준의 통신 보안을 제공합니다. 또한, 고객은 다음과 같은 Tencent Cloud 서비스를 사용하여 다양한 시나리오에서의 데이터 안전한 전송을 실현할 수 있습니다: • Direct Connect (DC): 전용성과 높은 보안성을 갖춘 대역폭 네트워크 연결을 제공합니다. 사용자가 네트워크 링크를 독점하여 데이터 유출 위험이

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
4	금융회사 등의 내부시스템과 클라우드 시스템 연계	금융감독원장의 확인을 받은 경우 제 15 조⑥ 1: 무선통신망 이용 업무는 최소한으로 국한하고 법 제 21 조의 2 에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것 제 17 조 1: 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ 구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것 제 18 조: 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP 주소"라 한다)의 안전한 사용을 위하여 주소 체계·할당·관리 등에 대한 내용을 포함한 적절한 대책을 수립·운영하고, 내부 IP 주소 및 외부 IP 주소의 인터넷 접속내용을 1 년 이상 별도로 기록·보관하여야 한다. 【추가 사항】: 시스템간 연계 및 클라우드서비스 내 주요 통신 채널에 대한 암호화 적용	없습니다. • VPN Connection: 네트워크 터널링 기술을 기반으로, 온프레미스 데이터센터와 Tencent Cloud 상의 자원 간의 안전한 전송 연결을 실현합니다. VPN 터널은 IKE(키 교환 프로토콜) 및 IPsec 을 사용하여 전송되는 데이터를 암호화하고, 인터넷 상에 안전하고 신뢰할 수 있는 데이터 터널을 구축하여 전송 과정 중 데이터의 안전을 보장합니다. • Virtual Private Cloud (VPC)는 터널링 기술을 기반으로 물리적 네트워크 위에 가상 네트워크를 구성하며, 가상화 기술을 활용하여 서로 다른 사설 네트워크 간의 완전한 논리적 격리를 구현하여 고객에게 독립적이고 격리된 안전한 클라우드 네트워크를 제공합니다. 사설 네트워크 내의 클라우드 서버에 대해서는 보안 그룹 및 네트워크 ACL 규칙 설정을 통해 인스턴스 수준 및 서브넷의 수신/발신 트래픽을 제어함으로써, 다양한 계층의 네트워크 접근 제어를 달성할 수 있습니다.
		【필수 사항】: 제 12 조 1-4: 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다. 1. 단말기는 인가된 사용자만 사용할 수 있도록 관리할 것 2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것 3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지,	• Cloud Connect Network (CCN)는 클라우드 상의 사설 네트워크(VPC) 간, 그리고 VPC 와 온프레미스 데이터 센터(IDC) 간의 내부 네트워크 상호 연결을 지원하며, 전 네트워크 다중 지점 상호 연결, 라우팅 자동 학습, 링크 최적 선택 및 장애 신속 수렴 등의 능력을 갖추고 있습니다. 클라우드 커넥트 네트워크 내의 네트워크 인스턴스 간 모든 통신 데이터는 공중망을 경유하지 않아 더 우수한 통신

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		정기적인 악성코드 감염여부 확인 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것 4. 정보유출 및 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 등에 접근하는 것을 통제할 것 제 15 조⑤. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것. 다만, 다음 각 목의 경우에는 그러하지 아니하다. 가. 이용자의 고유식별정보 또는 개인신용정보(「신용정보의 이용 및 보호에 관한 법률」 제 40 조의 2 에 따른 가명처리에 관한 행위규칙을 준수한 가명정보는 제외)를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한한다) 나. 업무상 불가피한 경우로서 금융감독원장이 인정하는 경우 제 34 조 1: 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제 36 조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)	품질과 네트워크 가용성, 낮은 지연 시간 및 낮은 패킷 손실률 등의 특성을 가지며, 다중 수준 링크 중복을 통해 통신 품질을 보장하여 데이터를 안전하고 신뢰할 수 있게 합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
5	암호화 및 키 관리	제 60 조① 5: 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용 【 추가 사항 】 : 내부시스템과 클라우드 시스템 간 연계되는 데이터의 식별 및 관리	
		【 필수 사항 】 : 제 19 조: ① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다. ② 금융회사 또는 전자금융업자는 암호 및 인증시스템 등에 적용되는 키(Key)(프로그램 진위 및 무결성 확인에 사용되는 암호 또는 인증시스템 등에 적용되는 키를 포함한다)에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다. 제 19 조의 2: 금융회사 또는 전자금융업자는 비밀번호, 생체정보 등 사용자 인증수단 유출을 방지하기 위하여 인증수단의 발급·보관·주기적 변경 및 인증오류 발생시 처리 절차 등을 포함한 관리방안을 수립·운용하여야 한다. 제 34 조의 3① : 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록	고객은 법규 등 감독 요건에 따라 정보 저장 및 전송에 암호화 조치를 취하고, 키 전체 생명주기에 대한 보안 관리 방안을 수립·이행하여야 합니다. 고객의 데이터 저장 보호를 지원하기 위해 Tencent Cloud 의 여러 저장 및 데이터베이스 제품은 데이터 암호화 기능을 지원하고, 안전한 고강도 암호화 알고리즘을 사용하며, Key Management Service (KMS) 통합을 통해 키 전 생애 주기 관리를 구현하여 데이터의 기밀성을 보장합니다. Tencent Cloud 는 고객이 암호화 키의 전 생애 주기 관리를 구현할 수 있도록 돕기 위해 Key Management Service (KMS)을 제공합니다. 이를 통해 키가 안전한 방식으로 생성, 저장, 분배, 가져오기, 내보내기, 사용, 복구, 아카이빙 및 파기 등의 일련의 작업이 완료되어 키가 유출되지 않도록 보장합니다. 사용자 마스터 키(CMK)는 KMS 의 핵심 자원입니다. CMK 는 사용자의 1 급 키에 속하며, 주로 민감한 데이터의 암호화와 복호화에 사용됩니다. 사용자는 KMS 의 자동 생성 사용자 마스터 키 기능을 이용해 CMK 를 생성하거나, 자체 키를 가져와 CMK 를 구성할 수 있습니다. KMS 는 FIPS-140-2 인증을 받은 하드웨어 보안 모듈(HSM)을 사용하여 사용자 마스터 키를 보호합니다. KMS 는 또한 키의 전달 및 배포 과정에 대해 TLSv1.2 를 활성화하여 암호화 보호를 수행하여

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다. 【추가 사항】: 클라우드서비스 제공자 등 외부자의 키접근 가능성 등을 고려하여 키의 수명주기별 보 안관리 방안 수립	중간자 공격(Man-in-the-Middle)에 의한 가로채기 및 도난을 방지합니다. 키가 해독되거나 악용될 위험을 줄이기 위해 KMS 는 키 순환을 지원하고, 효력을 잃은, 폐기된, 또는 유출된 키를 안전하고 신뢰할 수 있는 방법으로 삭제합니다. 삭제된 키는 복구할 수 없으며, 해당 키로 암호화된 데이터도 더 이상 복호화할 수 없습니다. CloudAudit 서비스는 키 관리 시스템 서비스의 관련 조작 이벤트를 기록할 수 있습니다. 고객은 클라우드 감사 콘솔에 로그인하여 관련 조작 기록을 확인할 수 있습니다. 데이터 전송 보호 측면에서, 고객의 Tencent Cloud 콘솔 상의 모든 통신은 HTTPS 보안 프로토콜의 암호화 보호를 받습니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스는 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 고객의 비즈니스에 포트 수준의 통신 보안을 제공합니다. 또한, 고객은 Virtual Private Cloud (VPC), Direct Connect (DC), VPN Connection 등을 활용하여 다양한 시나리오에서의 데이터 안전한 전송을 실현할 수 있습니다. 데이터 전송 보안과 관련된 자세한 정보는 본 가이드 "제 6.6 장 중 번호 3&4"의 관련 내용을 참조하시기 바랍니다. 고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 내부적으로 키 관리 메커니즘을 구축하고 관련 기준을 제정하여 키의 신청, 생성, 저장, 사용, 전달, 업데이트, 폐기 등 과정을 규범화합니다. 키 생명주기에 관련된 각 작업은 이중 통제, 엄밀한 인수인계, 적절한 보관, 적시 업데이트의 기본 요건을 준수하며, 권한 분리, 담당자 지정, 엄격한 승인, 상세한 기록, 실명

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			운영의 규정을 수립·이행하고, 사업 키 운영 로그를 보존하여 정기적으로 운영 감사를 실시합니다.
			고객은 주요 계정(예: 클라우드 콘솔 관리 계정)의 운영 행위에 대한 로그를 기록하고 정기적으로 검토하여야 합니다.
		【필수 사항】: 제 13 조①9: 정보처리시스템의 가동기록은 금융감독원장이 정하는 사항을 접속의 성공여부와 상관없이 자동적으로 기록·유지하고 1년 이상 보존할 것	운영 로그 수집 및 보존에 대해, 고객은 CloudAudit 를 채택하여 Tencent Cloud 계정 활동에 대한 감독, 규정 준수 점검, 작업 검토 및 위험 검토를 수행할 수 있습니다. CloudAudit 은 최근 90 일 이내의 Tencent Cloud 콘솔 및 클라우드 API 작업 기록(액세스 키, 리전, 오류 코드, 이벤트 ID, 이벤트 이름, 이벤트 소스, 이벤트 시간, 요청 ID, 출발지 IP 주소, 사용자 이름 포함)의 온라인 조회를 지원합니다.
6	로깅	제 18 조: 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP 주소"라 한다)의 안전한 사용을 위하여 주소 체계·할당·관리 등에 대한 내용을 포함한 적절한 대책을 수립·운영하고, 내부 IP 주소 및 외부 IP 주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관하여야 한다.	Tencent Cloud 는 또한 고객에게 Cloud Log Service (CLS) 를 제공합니다. 일원화된 로그 서비스 플랫폼으로서, CLS 는 로그 수집, 로그 저장, 로그 검색 분석, 실시간 소비, 로그 전달 등 다양한 서비스를 제공하여 고객이 비즈니스 운영, 보안 모니터링, 로그 감사, 로그 분석 등의 문제를 해결하도록 돕습니다. Cloud Security Center (CSC) 또한 클라우드 보안 제품 경보 데이터, 클라우드 자산 구성 변경 데이터, 클라우드 상 사용자 작업 행위 데이터 및 일부 클라우드 제품 로그 데이터 등 다양한 클라우드 보안 관련 데이터를 수집하고, 통합 검색 조사 플랫폼을 제공하여 고객이 포괄적인 클라우드 로그 감사 및 검색 조사를 실현하도록 지원합니다.
		제 25 조: 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.	고객의 규제 준수를 지원하기 위해, Tencent Cloud 는 내부적으로 로그 수집
		【추가 사항】: 클라우드 관리 콘솔 관리자 등 주요 계정에 대한 활동 내역 로깅 및 주기적 검토	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			및 관리 규정과 메커니즘을 구축하여, 로그인 로그, 작업 로그, 시스템 일반 로그, 시스템 보안 이벤트 로그 등의 로그 기록, 추출, 저장, 보호, 분석, 감사 등을 통제하여 시스템 활동 이상과 위험을 탐지 및 방지합니다. 로그는 Tencent Cloud 로그 관리 플랫폼에 통합 수집되어 관리되며, 관련 로그 정보에 대해 백업과 엄격한 보호 조치를 취하여 무단 수정 및 삭제로부터 보호합니다. 백업 로그는 1년 이상 보관됩니다. Tencent Cloud 는 운영 보안 자동화 감사 도구와 내부 감사팀을 통해 로그를 감사하며, 시스템 또는 작업 이상을 탐지하여 운영 위험을 방지합니다.
7	가상 보안	【 추가 사항 】 : 가상 이미지 템플릿을 최신 상태로 유지하고, 이미지 무결성 등 보안사항을 주기적으로 점검	고객은 가상 이미지의 보안 상태를 정기적으로 점검하고, 가상 이미지 템플릿이 최신 상태를 유지하도록 보장하여야 합니다. Tencent Cloud 가 고객에게 제공하는 Cloud Virtual Machine (CVM)은 확장 가능한 가상화 컴퓨팅 서비스로, 고객이 CPU, 메모리, 하드 디스크, 네트워크, 보안 등의 리소스를 사용자 정의할 수 있도록 지원합니다. Tencent Cloud 는 고객에게 공식 정품 기반 운영 체제와 Tencent Cloud 가 제공하는 초기화 구성 요소를 포함한 안전한 공식 공용 이미지를 제공합니다. CVM 은 또한 고객이 사용자 정의 이미지를 생성하거나 이미지 가져오기 기능을 통해 가져오고, 사용자 정의 이미지를 공유 및 삭제하는 것을 지원합니다. CVM 의 보안을 보장하기 위해, 고객은 보안 그룹과 네트워크 ACL 을 사용하여 호스트 및 네트워크의 접근 정책을 자체 정의할 수 있으며, 다양한 인스턴스에 대해 유연하게 방화벽을 설정할 수 있습니다. CVM 은 또한

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			민감한 작업 보호 기능을 지원하여, 사용자가 민감한 작업을 수행하기 전에 신원 인증을 받도록 합니다. Tencent Cloud 는 CVM 에 대해 클라우드 모니터링을 제공하여 다양한 실시간 경보를 지원하며, DDoS 방어, DNS 하이재킹 탐지, 침입 탐지, 취약점 스캔, 웹사이트 악성코드 탐지, 로그인 보호 등의 보안 서비스를 제공합니다. 컨테이너 이미지 관리 측면에서, Tencent Cloud Container Registry (TCR) 는 고객에게 안전하고 전용적이며 고성능의 컨테이너 이미지 호스팅 및 배포 서비스를 제공합니다. 고객은 Tencent Cloud Container Security Service (TCSS)를 활용하여 컨테이너 및 이미지 보안을 보호할 수 있습니다. TCSS 는 컨테이너 자산 관리, 이미지 보안 스캔, 런타임 침입 탐지, 보안 기준선 설정 관리 등의 기능을 지원하여, 이미지 생성 · 저장부터 실행까지 컨테이너 전체 생명주기 보호를 제공하고 고객이 컨테이너 보안 방어 체계를 구축할 수 있도록 지원합니다. Tencent Cloud 가상 머신 및 가상 서비스 사용 과정 중 보안 통제를 강화하기 위해, Tencent Cloud 는 내부적으로 가상화 보안 관리 관련 규정을 수립하여 가상 머신 리소스의 관리 책임, 권한 관리, 구성 관리 등 관련 기준을 명확히 했습니다. Tencent Cloud 는 가상 머신 격리 및 리소스 제어, 패치 관리 및 취약점 방어, 하이퍼바이저 보안 강화 등의 기술적 수단을 통해 다양한 측면에서 가상화 보안 방어 체계를 구축합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
8	보안 모니터링 및 취약점 분석/평가	【필수 사항】: 제 14 조 1: 다음 각 목을 작성·보관 할 것 가. 주요 정보처리시스템에 대한 운영매뉴얼 나. 주요 정보처리시스템에 대한 정기적인 유지보수 실시 내용을 기록한 유지보수관리대장 다. 정보처리시스템에 대한 책임자명부 및 장애상황기록부 제 14 조 4: 정보처리시스템의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할 것 제 15 조 ① 1-2: 1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영 2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시 제 15 조 ② - ③ : ② 제 1 항제 1 호의 규정에 따른 정보보호시스템의 안전한 운영을 위하여 금융감독원장이 정하는 사항을 준수하여야 한다. ③ 제 1 항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1 년 이상 보존하여야 한다. 제 16 조: 금융회사 또는 전자금융업자는 악성코드 감염·확산 방지, 피해 최소화 및 복구를 위한 대책을	고객은 클라우드 서비스 내 주요 변경 사항에 실시간 경보를 설정하고 모니터링을 실시하며, 주요 정보처리시스템에 통합 보안 운영 관리를 적용하여야 합니다. Tencent Cloud 가 고객에게 제공하는 클라우드 서비스는 각 서비스별로 약정된 서비스 수준 계약에 기반하여 제공되며, 각 서비스의 성능 지표, 측정 기준 및 보고 요구사항은 각 제품의 서비스 수준 계약에 명확히 기재되어 Tencent Cloud 공식 웹사이트에 게시됩니다. 각 클라우드 서비스의 성능과 가용성은 지속적으로 추적되며, 관련 지표는 관리 콘솔을 통해 고객이 실시간으로 모니터링할 수 있습니다. Tencent Cloud 는 또한 고객에게 Tencent Cloud Observability Platform (TCOP) 을 제공하여 클라우드 제품/서비스 모니터링을 지원합니다. TCOP 는 클라우드 서버, 클라우드 데이터베이스 등 클라우드 제품이 자체 보고하는 다양한 모니터링 지표와 고객이 사용자 정의 구성하여 보고하는 모니터링 지표를 수집 및 시각화 차트로 표시하여, 고객이 클라우드 제품 자원 사용률, 애플리케이션 성능 및 클라우드 제품 운영 상태를 실시간으로 파악할 수 있도록 돕습니다. TCOP 는 지표에 대한 경보 설정을 지원하며, 설정된 경보 규칙에 따라 메시지 푸시 등을 통해 비즈니스 이상 상황을 고객에게 적시에 통지합니다. Tencent Cloud 는 또한 고객의 보안 운영을 지원하기 위해 일련의 관련 제품 및 서비스를 제공합니다. 이는 다음과 같습니다: • Cloud Security Center (CSC): 통합 보안 관리 플랫폼으로서, 자산 센터, 리스크 센터, 경보

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		수립·운용하여야 한다.	센터, 고급 보안 관리를 통해
제 37 조의 2: ①	전자금융기반시설의 취약점 분석·평가는 총자산이 2 조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300 명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1 회 이상(홈페이지에 대해서는 6 개월에 1 회 이상) 실시하여야 한다.	② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한)를 포함하여 5 인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100 분의 30 이상은 「정보보호산업의 진흥에 관한 법률 시행규칙」 제 8 조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제 37 조의 3 제 1 항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다.	고객이 사전 위협 탐지, 사중 대응·처리, 사후 추적 분석의 보안 운영 클로즈드 루프를 실현할 수 있도록 지원합니다. CSC 는 클라우드 자산에 대한 통합 보안 관리를 지원하며, 자산 자동화 실사, 보안 리스크 탐지·식별, 보안 리스크 자동화 대응·처리 기능을 포함합니다. CSC 는 클라우드 방화벽, 웹 애플리케이션 방화벽의 위협 경보 및 로그를 수집하고, Tencent Cloud 위협 인텔리전스 및 자체 보안 지식 데이터베이스를 활용하여 데이터에 대한 자동화된 분석·조사를 수행하여 고객에게 집중화된 위협 탐지, 조사, 처리 역량을 제공합니다.
		③ 제 1 항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1 회 이상(홈페이지에	• Threat Intelligence Center (TIX): 통합 인텔리전스 서비스 플랫폼으로서, 기초 인텔리전스, 공격면 인텔리전스, 비즈니스 인텔리전스 등 세 가지 핵심 인텔리전스 역량을 제공하며, 인텔리전스 조회, IOC 분석·판단, 공격면 관리 등의 기능을 지원합니다. 이를 통해 고객이 보안 사고를 보다 효율적으로 분석·판단하고 기업 자산의 노출 리스크를 보다 전면적으로 평가할 수 있도록 지원하여, 기업의 효율적인 입체적 보안 방어 체계 구축을 돕습니다. • Cloud Log Service (CLS) : 일원화된 로그 서비스 플랫폼으로서 CLS 는 로그 수집, 로그 저장, 로그 검색 분석, 실시간 소비, 로그 전달 등 다양한 서비스를 지원하여 고객이 비즈니스 운영, 보안 모니터링,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		대해서는 6 개월에 1 회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석·평가의 내용은 금융감독원장이 정한다. ④ 금융회사 및 전자금융업자는 해당 주기 내에 평가 대상 시설과 평가기간을 나누어 평가할 수 있다. ⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다. 1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행 2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것 3. 이행계획의 시행 결과는 최고경영자에게 보고할 것 ⑥ 금융회사 또는 전자금융업자는 제 1 항 또는 제 3 항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다. 【추가 사항】: 클라우드서비스 내 주요 변경 사항에 대한 실시간 경보 설정 및 모니터링 실시 【 추가 사항 】 : 주요 정보처리시스템의 경우 침해사고 대응 기관의 통합보안관제 적용	로그 감사, 로그 분석 등의 문제를 해결하는 데 도움을 줍니다. CLS 는 고객이 "로그 다운로드", "로그 내보내기", "로그 전달" 등의 기능을 통해 자신의 클라우드 로그를 로컬에 다운로드하여 확인하거나, 지정된 제 3 자 시스템(고객의 온프레미스 SIEM/SOC 플랫폼 포함)으로 전달할 수 있도록 지원합니다. 고객의 규제 준수를 지원하기 위해 Tencent Cloud 보안팀은 7*24 시간 운영되는 보안 운영 체계를 기반으로 취약점 모니터링, 침입 추적, 공격 차단 등의 핵심 시나리오에 집중하여, 보안 경보에 실시간으로 대응하고 공격 추적 및 비상 대응 계획을 신속히 수립함으로써 보안 사건의 확산을 효과적으로 억제합니다. 고객에게 영향을 미칠 수 있는 운영 변경 작업에 대해서는, Tencent Cloud 가 공식 웹사이트, 사이트 내 메시지 등의 채널을 통해 관련 고객에게 변경 통지를 적시에 발표합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
9	인적보안	【필수 사항】: 제 8 조① 2: 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것 【추가 사항】: 클라우드서비스 제공자 및 클라우드서비스운동을 위탁받은 관리형 서비스 제공자 등의 권한과 책임을 식별하고 관리	고객은 클라우드 서비스 제공자 및 관리형 클라우드 서비스 제공자 등의 권한과 책임을 식별·관리하여야 합니다. Tencent Cloud 는 클라우드 컴퓨팅 서비스의 개방 및 공유 특성을 견지하며, 지속적으로 클라우드 플랫폼과 클라우드 서비스의 보안 능력을 향상시키고, 고객과 함께 클라우드 비즈니스와 데이터를 위해 더 좋고 완벽한 보안 보장 체계를 구축합니다. Tencent Cloud 는 클라우드 서비스 제공자로서 데이터센터의 인프라와 클라우드 플랫폼의 보안을 책임집니다. 고객이 서로 다른 클라우드 서비스 범주(예: IaaS, PaaS 및 SaaS 서비스)를 선택할 때 다양한 구성 요소에 대한 통제권 또한 다르다는 점을 고려하여, Tencent Cloud 는 서로 다른 클라우드 서비스 범주에 기반한 클라우드 보안 책임 공유 모델을 구축했습니다. 자세한 내용은 본 가이드 제 3 장 Tencent Cloud 보안 책임 공유 모델을 참조하시기 바랍니다. 클라우드 서비스 제공업체로서 Tencent Cloud 는 국제 사이트 공식 웹사이트에 온라인 본서비스 General Service Level Agreement 데이터 개인 정보 보호 및 보안 계약등 법적 문서를 제공하여 Tencent Cloud 가 제공하는 서비스 내용과 서비스 수준, 사용자 데이터 및 지식 재산권 보호, 고객과 Tencent Cloud 양측의 보안 책임과 의무 등을 명확히 합니다. 고객은 또한 Tencent Cloud 와 오프라인 계약을 체결하여 계약 내 조항 및 세부사항을 협의할 수 있습니다. 데이터센터 운영 관리 측면에서, 현재 Tencent Cloud 는 한국에 두 개의 임대형 데이터센터를 구축했습니다. 데이터센터의 탄력성과 안전성을

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			보장하기 위해 Tencent Cloud 는 데이터 공급업체 선정, 계약상의 제약부터 지속적인 감독에 이르기까지 전 과정에 걸쳐 엄격한 관리 체계를 구축했습니다 : - 공급업체 선정 단계에서, Tencent Cloud 는 엄격한 공급업체 보안 평가 메커니즘 및 자격 기준을 구축하여, 데이터센터 공급업체의 물리적 환경 보안, 정보 보안 관리 체계 및 비즈니스 연속성 보장 역량에 대한 포괄적인 실사와 위험 평가를 수행하여 선정된 공급업체가 높은 보안 기준 요구사항을 충족하도록 보장합니다. - 협력 계약 체결 단계에서, Tencent Cloud 와 데이터센터 운영사는 표준화된 계약 문서를 통해 상호 권리와 책임의 경계를 명확히 하고, 데이터센터 운영사의 서비스 범위를 명시하며, 서비스 가용성 수준 등의 핵심 서비스 기준을 정량적으로 정의하여 서비스 품질에 대한 계약적 보장을 제공합니다. - 데이터센터 운영 단계에서, Tencent Cloud 는 정례적 감시 및 평가 메커니즘을 구축하여, 정기적으로 데이터센터 운영사의 기술 역량, 서비스 응답 효율성 및 위험 관리 효과를 종합적으로 평가하여, 데이터센터 운영사의 위험 관리 결함으로 인해 Tencent Cloud 의 고객에 대한 핵심 서비스 제공 역량이 영향을 받지 않도록 보장합니다. 또한, Tencent Cloud 는 고객의 아웃소싱 관리 요구사항에 적극 협력하며, 전담 인력을 제공하여 고객 측에서 시작한 감사 또는 평가 활동을 지원하고

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			협조하며, 고객에게 다양한 보안 보호 조치 및 관련 클라우드 제품/서비스를 제공하여 고객의 클라우드 데이터 기밀성과 무결성을 보장합니다.

6.7 클라우드컴퓨팅서비스 위수탁 계약서 주요 기재사항

"<별표 2의 5>클라우드컴퓨팅서비스 위수탁 계약서 주요 기재사항"에는 금융회사 또는 전자금융 서비스 제공자가 클라우드 컴퓨팅 서비스 제공자와 위탁 계약을 체결할 때 반드시 포함해야 할 사항이 명시되어 있으며, 이는 "기본 포함사항"과 "추가 포함사항"으로 구분됩니다.

기본 포함사항:

- 클라우드서비스 이용 대상 업무 및 시스템 개요
- 위탁하는 업무 데이터에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 통보필요 사항
- 감독당국 또는 내외부 감사인의 조사·접근 수용 의무
- 비상대응훈련, 취약점 분석·평가, 침해사고 대응훈련 등 협조 사항
- 클라우드서비스 제공자의 보안관리 수준 등에 관한 사항
- 정보보호 의무 및 서비스 연속성 보장 등 보안 요구사항
- 서비스에 악영향을 미칠 수 있는 경우 계약 해지 권한 보유
- 서비스 제공 수준(SLA) 모니터링 및 시정조치 권리
- 고객정보보호 및 비밀유지
- 위탁계약 종료 시 데이터 파기
- 관련 법률 준수 및 보고 관련 의무
- 데이터에 대한 접근통제
- 전산사고 등에 따른 이용자 피해에 대한 위·수탁회사간의 책임관계

- 수탁회사의 분쟁해결 과정에서의 재판관할

추가 포함사항:

- 금융회사 등이 위탁한 정보처리가 실제 수행되는 위치
- 서비스 제공 중단 시 데이터 접근권한 등 비상대책에 관한 사항
- 위탁업무를 다른 수탁자나 금융회사로 이전할 경우 지원의무 및 전환 계획
- 합병·분할, 계약상 지위의 양도, 재위탁 등 중요 상황 발생시 대책
- 재위탁 또는 재위탁의 변경 등 금융회사의 동의가 필요한 사항
- 재위탁 관련 클라우드서비스 제공자의 관리·감독 의무

본 규정 제 14 조의 2 제 1 항 제 1 호에 따르면, 사용되는 클라우드 컴퓨팅 서비스가 중요 업무로 분류되는 경우, 관련 계약에는 "기본 포함사항"과 "추가 포함사항"이 모두 포함되어야 합니다. 사용되는 클라우드 컴퓨팅 서비스가 비중요 업무로 분류되는 경우, "기본 포함사항"만 포함하면 됩니다.

클라우드 서비스 제공업체로서 Tencent Cloud 는 국제 사이트 공식 웹사이트에 온라인 [본서비스 General Service Level Agreement](#) [데이터 개인 정보 보호 및 보안 계약](#) 등 법적 문서를 제공하여, Tencent Cloud 가 제공하는 서비스 내용 및 서비스 수준, 사용자 데이터 및 지식 재산권 보호, 고객과 Tencent Cloud 양측의 보안 책임과 의무, 서비스 기간 및 계약 종료 시나리오, 분쟁 해결 메커니즘, 통지 메커니즘 등을 명확히 합니다. 고객은 또한 오프라인 계약을 Tencent Cloud 와 체결하여 계약 내 조항 및 세부사항을 협의할 수 있습니다.

Tencent Cloud 가 고객에게 제공하는 클라우드 서비스는 각 서비스별로 약정된 서비스 수준 계약에 기반하여 제공되며, 각 서비스의 성능 지표, 측정 기준 및 보고 요구사항은 각 제품의 서비스 수준 계약에 명확히 기재되어 Tencent Cloud 공식 웹사이트에 게시됩니다. 각 클라우드 서비스의 성능과 가용성은 지속적으로 추적되며, 관련 지표는 관리 콘솔을 통해 고객이 실시간으로 모니터링할 수 있습니다.

하도급 처리에 대해, [데이터 개인 정보 보호 및 보안 계약](#) 등 계약에는 하도급 처리에 대한 사전 동의, 하도급 업체 추가 또는 변경 사항에 대한 사전 통지, 데이터 보호 의무 등의 조항이 명확히 규정되어 있습니다. 고객의 사전 동의 없이

Tencent Cloud 는 계약/합의에 따라 고객을 대행하여 수행하는 어떠한 처리 작업도 하도급하지 않습니다. 하도급 처리 업체 추가 또는 변경과 관련된 예정된 변경사항은 Tencent Cloud 가 이메일 등의 채널을 통해 고객에게 통지합니다. 하도급업체 관리 측면에서 Tencent Cloud 는 완비된 공급망 보안 관리 체계를 구축하여, 엄격한 공급업체 보안 평가 및 자격 심사, 정기적인 감독 및 평가, 명확한 아웃소싱 서비스 계약 등의 조치를 통해 공급업체를 효과적으로 통제하고, 하도급 처리가 Tencent Cloud 의 고객에 대한 서비스 제공 능력, 고객 정보 처리 과정의 기밀성과 무결성, 그리고 고객 또는 관련 규제 기관의 감독 및 감사 권리에 영향을 미치지 않도록 보장합니다. 또한, Tencent Cloud 는 고객 측에서 시작하는 감사 또는 평가 활동에 적극적으로 대응 및 협조합니다.

규정 준수 및 데이터 주권 측면에서, Tencent Cloud 는 내부적으로 완비된 정보 보안 및 개인정보 보호 관리 체계를 구축하고, 사업을 운영하는 관할권의 사이버 보안, 사용자 개인정보 및 데이터 보안 관련 법률 및 규정을 엄격히 준수합니다. Tencent Cloud 는 "데이터 기밀성" 원칙을 준수하여, 서비스 제공 또는 문제 해결의 필요가 있고 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 기관의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 경우가 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 적극적으로 접촉하지 않습니다. 법률적 강제 요구로 인해 고객 데이터를 공개해야 할 경우, Tencent Cloud 는 관련 법적 요구사항을 따르며 고객에게 적시에 통지합니다. Tencent Cloud 는 데이터 접근 권한에 대해 전 노드 실명제 심사 및 유지 관리를 시행하여 데이터 자산의 무결성과 비즈니스 서비스의 신뢰성을 보호하며, 실시간 모니터링 및 차단 메커니즘을 구축하여 비정상적인 데이터 접근 행위를 탐지하고 차단합니다. Tencent Cloud 는 공개적이고 투명한 원칙을 견지하며, 고객이 데이터 저장 위치 등의 정보, 즉 데이터가 저장된 데이터센터 위치, 데이터 콜드 백업 상황 및 콜드 백업 데이터의 저장 위치 등을 알아야 할 경우, Tencent Cloud 는 적절한 채널을 통해 고객에게 정보를 적시에 제공합니다.

비즈니스 연속성 및 비상 대응 측면에서, Tencent Cloud 는 전 세계 여러 지역에서 관련 국제 표준과 현지 안전 요구사항에 따라 데이터센터를 건설하거나 임대하여, 고객에게 다중 지역(region) 및 다중 가용 영역(zone) 선택을 제공합니다. 또한, 사업 운영 관할권의 사용자 개인정보 보호 및 데이터 보안 관련 법률 규정을 엄격히 준수하며, 지속적으로 현지 규제 동향을 주의 깊게

모니터링합니다. 고객은 사업 발전 요구와 데이터 보안 요구사항에 따라 데이터와 시스템을 다른 지역 또는 다른 가용 영역에 자유롭게 유연하게 배포할 수 있습니다. 현재 Tencent Cloud 는 한국에 두 개의 데이터센터를 보유하고 있으며, 클라우드 서버, 클라우드 데이터베이스, 클라우드 스토리지 등을 포함한 다양한 클라우드 컴퓨팅 서비스를 제공합니다. 한국 고객은 한국 현지에서 자신의 데이터를 저장, 처리 및 백업할 수 있습니다. Tencent Cloud 가 제공하는 컴퓨팅 서비스, 네트워크 서비스, 스토리지 서비스, 데이터베이스 서비스, 컨테이너 및 미들웨어 서비스, 보안 서비스 등 다양한 클라우드 제품/서비스는 모두 고가용성 특성을 갖추고 있으며, 이에 상응하는 재해 복구 및 복원 계획을 마련하고 있습니다. Tencent Cloud 는 내부적으로 포괄적인 비즈니스 연속성 관리 체계를 구축했으며, 이미 ISO/IEC 22301 비즈니스 연속성 관리 체계의 국제 표준 인증을 획득했습니다.

사건 보고 측면에서, Tencent Cloud 는 정보 보안 사건 대응, 사건 에스컬레이션, 사건 통지 등의 관련 절차를 구축하여 사고의 영향을 받을 수 있거나 이미 받은 회사 내부 인원 및 고객 등 이해관계자들에게 적시에 경보 또는 통지를 제공하고, 모든 당사자가 질서 있고 적시에 효율적으로 소통과 협업을 할 수 있도록 합니다. 고객에게 영향을 미칠 수 있는 보안 사건의 경우 Tencent Cloud 는 정보 보안 사건의 영향 범위와 정도에 따라 내부 검토를 거친 후, 적절한 방법으로 고객에게 정보 보안 사건 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.

고객의 아웃소싱 평가 및 검사 요구사항에 부합하기 위해, Tencent Cloud 는 전담 인력을 배치하여 고객이 시작한 감사 또는 검토 활동에 적극적으로 대응할 수 있습니다. Tencent Cloud 보안팀은 매년 최소 한 차례 이상 내부 보안 감사를 실시하며, 클라우드 플랫폼 및 내부 시스템의 상황을 지속적으로 모니터링하여 양호한 보안 태세를 유지하고 관련 법률 규정 및 보안 관리 표준의 규정과 요구사항을 준수하도록 합니다. Tencent Cloud 는 또한 정기적으로 독립된 제 3 자의 전문 감사 및 평가를 받습니다. 현재 Tencent Cloud 는 제 3 자 독립 감사 또는 평가 방식을 통해 다수의 보안 및 개인정보 보호 규정 준수 인증 또는 자격을 취득했으며, 고객 요구에 기반하여 검증된 성격의 시스템 및 조직 통제 보고서를 제공함으로써, 클라우드 사용 기관, 독립 감사인, 규제 기관, 회사 주주

및 기타 이해 관계자에게 Tencent Cloud 의 최신 서비스 조직 내부 통제 상황을 공개하고 있습니다.

고객이 비즈니스 변경 또는 향후 IT 계획 수립으로 인해 계약 합의를 종료해야 할 경우, 언제든지 클라우드 데이터와 생산 환경에 대해 백업 및 마이그레이션을 선택할 수 있습니다. Tencent Cloud 는 고객이 일반적인 표준 형식을 사용하여 데이터를 백업하거나 마이그레이션할 수 있도록 지원합니다. 따라서 고객은 클라우드 도입 단계와 동일한 전송 방식 및 프로토콜을 사용하거나, [Direct Connect \(DC\)](#), [VPN Connection](#) 등의 네트워크 서비스 제품을 활용하여 데이터의 클라우드 이탈 시에도 안전성과 신뢰성을 보장할 수 있습니다. 고객의 서비스가 종료된 후 Tencent Cloud 는 엄격한 데이터 삭제 방식을 따릅니다. 보존 기간 만료 후 복제본 및 백업을 포함한 고객 데이터를 완전히 삭제하며, 삭제된 데이터는 복원할 수 없습니다.

07

Tencent Cloud

「금융회사 업무 위탁
규정」을 어떻게
준수하고 고객이 이를
충족하도록 지원하는가

「금융기관의 업무위탁 등에 관한 규정」은 금융회사가 「금융위원회의 설치 등에 관한 법률」 제 17 조 제 3 항에 따라 인가·허가·등록을 받은 업무를 위탁할 때 준수해야 할 관리 규정을 명확히 합니다.

본 장에서는 Tencent Cloud 가 「금융기관의 업무위탁 등에 관한 규정」에서 클라우드 서비스 제공자와 관련된 통제 요건을 추출 및 종합하고, 클라우드 서비스 제공자로서 Tencent Cloud 가 금융회사가 관련 요건을 어떻게 준수하도록 지원하는지 설명합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
3	업무위탁 등	① 금융기관은 인가등을 받은 업무를 영위함에 있어 제 3 자에게 업무를 위탁하거나 제 3 자의 업무를 수탁할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 사항은 그러하지 아니하다.	고객은 위탁 또는 수탁 시 제 3 자의 능력과 자격, 위탁이 금융 소비자 및 금융 질서에 미치는 영향, 관련 법규 요건 등 요소를 종합적으로 고려하여 업무가 적절하게 처리될 수 있도록 보장하여야 합니다. 또한, 고객은 위탁 시나리오에서 자신의 책임을 명확히 하여야 합니다.
		③ 금융기관이 제 1 항의 규정에 따라 제 3 자에게 업무를 위탁하거나 제 3 자로부터 업무를 수탁하는 경우에는 다음 각 호의 사항을 고려하여 동 업무가 적정하게 처리될 수 있도록 하여야 한다.	클라우드 서비스 제공업체로서 Tencent Cloud 는 국제 사이트 공식 웹사이트에 온라인 본서비스 General Service Level Agreement 데이터 개인 정보 보호 및 보안 계약 등 법적 문서를 제공하여, Tencent Cloud 가 제공하는 서비스 내용 및 서비스 수준, 사용자 데이터 및 지식 재산권 보호, 고객과 Tencent Cloud 양측의 보안 책임과 의무, 서비스 기간 및 계약 종료 시나리오, 분쟁 해결 메커니즘, 통지 메커니즘 등을 명확히 합니다. 고객은 또한 오프라인 계약을 Tencent Cloud 와 체결하여 계약 내 조항 및 세부사항을 협의할 수 있습니다.
		1. 업무위탁 또는 수탁에 따른 비용·편익분석	Tencent Cloud 는 클라우드 컴퓨팅 서비스의 개방 및 공유 특성을 견지하며, 지속적으로 클라우드 플랫폼과 클라우드 서비스의 보안 능력을 향상시키고, 고객과 함께 클라우드 비즈니스와 데이터를 위해 더 좋고 완벽한 보안 보장 체계를 구축합니다. Tencent Cloud 는 클라우드 서비스 제공자로서 데이터센터의 인프라와 클라우드
		2. 금융이용자 피해발생 및 금융질서 문란 여부	
		3. 제 3 자가 관련 법규(다만, 제 3 자가 외국인인 경우에는 국제사법 제 3 조)에 따라 업무수탁이 가능한지의 여부	
		4. 제 3 자가 수탁업무를 적절히 수행할 수 있는지의 여부	
		5. 「 금융실명거래 및 비밀보장에 관한 법률」 등	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
		관련 법령에의 저촉 여부	플랫폼의 보안을 책임집니다. 고객이 서로 다른 클라우드 서비스 범주(예: IaaS, PaaS 및 SaaS 서비스)를 선택할 때 다양한 구성 요소에 대한 통제권 또한 다르다는 점을 고려하여, Tencent Cloud는 서로 다른 클라우드 서비스 범주에 기반한 클라우드 보안 책임 공유 모델을 구축했습니다. 자세한 내용은 본 가이드 제 3 장 Tencent Cloud 보안 책임 공유 모델 을 참조하시기 바랍니다.
④	제 1 항에 따라 금융기관의 업무를 위탁받은 자는 위탁자의 동의를 얻어 위탁받은 업무를 제 3 자에게 재위탁할 수 있다. 이 경우 제 2 조, 본조 제 1 항·제 2 항·제 3 항, 제 4 조, 제 5 조, 제 6 조를 준용하되, 재위탁시 보고의 주체는 원위탁 금융회사로 한다.	제 1 항에 따라 업무를 위탁하는 경우(제 4 항에 따라 재위탁하는 경우를 포함한다) 위탁회사는 수탁회사가 이 규정 등 금융관련법령 및 제 3 조의 2 에 따른 업무위수탁기준상의 의무를 위반하여 발생하는 손해에 대해서 수탁회사와 연대하여 배상책임을 진다.	역량과 규모 측면에서, Tencent Cloud는 중국 인터넷 산업의 선도 기업인 Tencent의 클라우드 컴퓨팅 브랜드로서, 운영 능력과 규모가 업계에서 선도적 지위를 차지하고 있으며, 다수의 업계 기관으로부터 전문 인증을 획득했습니다. Tencent Cloud 데이터 센터는 중국 본토, 아시아 태평양 지역, 북미 지역, 유럽 지역을 포괄하며, 리전(Region)과 가용 존(Availability Zone)으로 구성되어 전 세계 여러 지역에 분포되어 있습니다. 또한 11,000 개 이상의 파트너와 협력하여 30 개 이상의 업종의 기업 고객에게 400 개 이상의 업종별 솔루션을 제공했습니다.
			규정 준수 측면에서 Tencent Cloud는 국제적으로 인정받는 정보 보안 및 IT 통제 표준에 따라 클라우드 서비스를 기획 및 구축하고, 사업 운영 관할권의 법률 및 규정을 엄격히 준수하며, 보안 및 규정 준수 관련 절차를 마련하여 관련 법률, 규정, 표준 및 절차의 요구사항을 충족하도록 보장합니다. Tencent Cloud는 매년 정보 시스템에 대한 보안 테스트, 위험 평가 및 내부 감사를 수행하여 보안 방어 역량이 항상 적정 수준에 있도록 하고 관련 보안 관리 및 표준의 규정과 요구사항을 준수합니다.
			Tencent Cloud는 매년 독립된 제3기관의 전문 감사를 받으며, 검증보고서 성격의

번호	통제 영역	통제 요구사항 요약	Tencent Cloud의 대응
			시스템 및 조직 통제 보고서를 제공하여 클라우드 이용 기관, 독립 감사인, 규제 기관, 회사 주주 및 기타 이해관계자에게 Tencent Cloud 서비스 조직의 최신 내부 통제 현황을 투명하게 공개하고 있습니다. 하도급 처리에 대해, 계약에는 하도급 사전 동의, 하도급업체 추가 또는 변경 전 통지, 데이터 보호 의무 등 조항이 명시되어 있습니다. 고객의 사전 동의 없이 Tencent Cloud는 계약/합의에 따라 고객을 대행하여 수행하는 어떠한 처리 작업도 하도급하지 않습니다. 하도급 처리 업체 추가 또는 변경과 관련된 예정된 변경사항은 Tencent Cloud가 이메일 등의 채널을 통해 고객에게 통지합니다. 하도급업체 관리 측면에서 Tencent Cloud는 완비된 공급망 보안 관리 체계를 구축하여, 엄격한 공급업체 보안 평가 및 자격 심사, 정기적인 감독 및 평가, 명확한 아웃소싱 서비스 계약 등의 조치를 통해 공급업체를 효과적으로 통제하고, 하도급 처리가 Tencent Cloud의 고객에 대한 서비스 제공 능력, 고객 정보 처리 과정의 기밀성과 무결성, 그리고 고객 또는 관련 규제 기관의 감독 및 감사 권리에 영향을 미치지 않도록 보장합니다. 또한, Tencent Cloud는 고객 측에서 시작하는 감사 또는 평가 활동에 적극적으로 대응 및 협조합니다.

08

Tencent Cloud

「금융회사의 정보처리
업무 위탁에 관한
규정」을 어떻게
준수하고 고객이 이를
충족하도록 지원하는가

「금융회사의 정보처리 업무 위탁에 관한 규정」은 금융회사가「금융위원회의 설치 등에 관한 법률」제 17 조 제 3 항에 따른 인가·허가·등록 등을 받아 금융업을 영위하는 과정에서 정보처리 업무를 위탁할 때 준수해야 할 관리 규정을 명확히 합니다.

본 장에서는 Tencent Cloud 가 「금융회사의 정보처리 업무 위탁에 관한 규정」에서 클라우드 서비스 제공자와 관련된 통제 요건을 정리 및 요약하고, Tencent Cloud 가 클라우드 서비스 제공자로서 어떻게 금융회사가 관련 요건을 준수하도록 지원하는지 설명합니다.

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
4	정보처리의 위탁	① 금융회사는 인가등을 받은 업무를 영위함에 있어 정보처리가 요구되는 경우 이를 제 3 자에게 위탁할 수 있다. ② 제 1 항의 규정에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우는 정보처리를 위탁할 수 없다. 다만, 다음 제 2 호의 경우 금융감독원장이 허용하는 방식에 따라 코스콤 또는 저축은행중앙회에 원장 등의 관리를 위탁하는 경우는 제외한다. 1. 관련 법령에서 해당 업무의 위탁을 금지하고 있는 경우 2. 최근 3 년 이내에 금융이용자의 정보관리, 감독관련 자료 제출 등 감독기관의 검사와 관련한 사항으로 기관경고 이상의 제재 또는 형사처벌을 2 회 이상 받은 경우 3. 기타 업무의 위탁으로 인하여 당해 금융회사의 건전성 또는 신인도를 크게 저해하거나, 금융질서의 문란 또는 금융이용자의 피해	고객이 정보처리 업무를 제 3 자에게 위탁하고 정보처리 위탁 계약을 체결할 때, 계약에는 데이터 접근 통제, 컴퓨터 사고 등으로 인한 이용자 피해 발생 시 양측의 책임 분담, 수탁자의 감독 기관 검사 및 감사 수용 의무, 분쟁 해결 과정에서 수탁자의 관할 법원 등의 내용을 반드시 명확히 기재하여야 합니다. 클라우드 서비스 제공업체로서 Tencent Cloud 는 국제 사이트 공식 웹사이트에 온라인 본서비스 General Service Level Agreement 데이터 개인 정보 보호 및 보안 계약 등 법적 문서를 제공하여, Tencent Cloud 가 제공하는 서비스 내용 및 서비스 수준, 사용자 데이터 및 지식 재산권 보호, 고객과 Tencent Cloud 양측의 보안 책임과 의무, 서비스 기간 및 계약 종료 시나리오, 분쟁 해결 메커니즘, 통지 메커니즘 등을 명확히 합니다. 고객은 또한 오프라인 계약을 Tencent Cloud 와 체결하여 계약 내 조항 및 세부사항을 협의할 수 있습니다. 규정 준수 및 데이터 주권 측면에서, Tencent Cloud 는 내부적으로 완비된 정보 보안 및 개인정보 보호 관리 체계를 구축하고, 사업을 운영하는 관할권의 사이버 보안, 사용자 개인정보

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		발생이 심히 우려되는 경우	및 데이터 보안 관련 법률 및 규정을 엄격히 준수합니다. Tencent Cloud 는 "데이터 기밀성" 원칙을 준수하여, 서비스 제공 또는 문제 해결의 필요가 있고 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 기관의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 경우가 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 적극적으로 접촉하지 않습니다. Tencent Cloud 는 데이터 접근 권한에 대해 전 노드 실명제 심사 및 유지 관리를 시행하여 데이터 자산의 무결성과 비즈니스 서비스의 신뢰성을 보호하며, 실시간 모니터링 및 차단 메커니즘을 구축하여 비정상적인 데이터 접근 행위를 탐지하고 차단합니다.
③	금융회사는 제 1 항에 따른 정보처리 위탁계약을 체결할 경우 데이터에 대한 접근통제, 전산사고 등에 따른 이용자 피해에 대한 위·수탁회사간의 책임관계, 수탁회사에 대한 감독·검사 수용의무, 수탁회사의 분쟁해결 과정에서의 재판관할 등을 계약 내용에 반드시 포함하여 위탁에 따라 발생할 수 있는 책임관계를 명확히 하여야 한다.		
④	제 1 항에 따라 정보처리를 위탁받은 자는 위탁받은 업무를 제 3 자에게 재위탁할 수 있다. 이 경우 본조 제 2 항·제 3 항·제 5 항·제 6 항, 제 5 조, 제 7 조, 제 8 조를 준용한다.		인적 자원 측면에서, Tencent 는 서로 다른 기능과 분야별 전문 팀을 설립하고 업계의 베테랑 전문가 서비스 팀을 결집하여 고객에게 안전하고 신뢰할 수 있으며 전문적이며 규정을 준수하는 제품과 서비스를 제공하기 위해 노력합니다.
⑤	제 1 항에 따라 정보처리를 위탁받은 자는 정보처리 과정에서 이전받은 정보를 당초 위탁의 범위를 초과하여 다른 목적으로 활용할 수 없다. 다만, 해당 정보 주체의 동의를 얻은 경우는 동意的 범위 내에서 활용할 수 있다.		하도급 처리에 대해, <u>데이터 개인 정보 보호 및 보안 계약</u> 등 계약에는 하도급 처리에 대한 사전 동의, 하도급 업체 추가 또는 변경 사항에 대한 사전 통지, 데이터 보호 의무 등의 조항이 명확히 규정되어 있습니다. 고객의 사전 동의 없이 Tencent Cloud 는 계약/합의에 따라 고객을 대행하여 수행하는 어떠한 처리 작업도 하도급하지 않습니다. 하도급 처리 업체 추가 또는 변경과 관련된 예정된 변경사항은 Tencent Cloud 가 이메일 등의 채널을 통해 고객에게 통지합니다.
⑥	제 1 항에 따라 정보처리를 위탁하는 경우 위탁된 처리와 관련한 전산설비 및 인력 등은 관련 법령상 인허가를 위한 전산설비 및 인력 구비 요건 등의 충족 여부를 판단시 고려한다.		하도급업체 관리 측면에서 Tencent Cloud 는 완비된 공급망 보안 관리 체계를 구축하여, 엄격한 공급업체 보안 평가 및 자격 심사, 정기적인 감독 및
⑦	제 1 항에 따라 정보처리를 위탁하는 경우(제 4 항에 따라 재위탁하는 경우를 포함한다) 위탁회사는 수탁회사가 이		

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		규정 등 관계법령 및 제 3 항에 따른 위탁계약 내용상의 의무를 위반하여 발생하는 정보주체 및 이용자의 손해에 대하여 수탁회사와 연대하여 책임을 진다.	평가, 명확한 아웃소싱 서비스 계약 등의 조치를 통해 공급업체를 효과적으로 통제하고, 하도급 처리가 Tencent Cloud 의 고객에 대한 서비스 제공 능력, 고객 정보 처리 과정의 기밀성과 무결성, 그리고 고객 또는 관련 규제 기관의 감독 및 감사 권리에 영향을 미치지 않도록 보장합니다. 또한, Tencent Cloud 는 고객 측에서 시작하는 감사 또는 평가 활동에 적극적으로 대응 및 협조합니다.
5	특정정보의 보호	① 제 4 조에 따라 정보처리를 위탁하는 경우 금융회사는 각 관련 법령상의 안전성 확보조치를 충실히 이행하여야 한다. 이 때 개인정보의 고유식별정보는 암호화 등의 보호 조치를 하여야 하며, 특히 국외로 이전되지 않도록 하여야 한다. ② 금융회사는 위탁 처리되는 정보의 보호를 위한 안전성 확보조치의 구체적 내용을 홈페이지 등을 통해 공시하여야 한다. 또한 민감정보의 처리를 위탁할 경우에는 정보주체에게 금융감독원장이 정하는 방법에 따라 개별 고지하여야 한다.	고객은 정보 처리를 위탁할 때 관련 법규 요구사항에 따라 (개인 식별 정보 암호화 및 국외 이전 제한 등을 포함한) 보안 보장 조치를 시행하고, 웹사이트 등을 통해 시행된 보안 보장 조치를 공개해야 합니다. 민감한 정보 처리에 대해서는, 고객은 정보 주체에게 별도로 고지해야 합니다. 고객의 데이터 저장 보호를 지원하기 위해 Tencent Cloud 의 여러 저장 및 데이터베이스 제품은 데이터 암호화 기능을 지원하고, 안전한 고강도 암호화 알고리즘을 사용하며, Key Management Service (KMS)통합을 통해 키 전 생애 주기 관리를 구현하여 데이터의 기밀성을 보장합니다. KMS 는 FIPS-140-2 인증을 받은 하드웨어 보안 모듈(HSM)을 사용하여 키를 생성하고 보호하며, 고객의 암호화 키 전 생애 주기 관리를 지원할 수 있습니다. 키가 해독되거나 악용될 위험을 줄이기 위해 KMS 는 키 순환을 지원하고, 효력을 잃은, 폐기된, 또는 유출된 키를 안전하고 신뢰할 수 있는 방법으로 삭제합니다. 삭제된 키는 복구할 수 없으며, 해당 키로 암호화된 데이터도 더 이상 복호화할 수 없습니다. 데이터 전송 보호 측면에서, 고객의 Tencent Cloud 콘솔 상의 모든 통신은 HTTPS 보안 프로토콜의 암호화 보호를

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			받습니다. Tencent Cloud 클라우드 제품이 제공하는 클라우드 API 인터페이스는 HTTPS 암호화, 서명 검증, 상태 모니터링 등의 보안 능력을 갖추어 고객의 비즈니스에 포트 수준의 통신 보안을 제공합니다. 또한, 고객은 다음과 같은 Tencent Cloud 서비스를 사용하여 다양한 시나리오에서의 데이터 안전한 전송을 실현할 수 있습니다: • Direct Connect (DC): 전용성과 높은 보안성을 갖춘 대역폭 네트워크 연결을 제공합니다. 사용자가 네트워크 링크를 독점하여 데이터 유출 위험이 없습니다. • VPN Connection: 네트워크 터널링 기술을 기반으로, 온프레미스 데이터센터와 Tencent Cloud 상의 자원 간의 안전한 전송 연결을 실현합니다. VPN 터널은 IKE(키 교환 프로토콜) 및 IPsec 을 사용하여 전송되는 데이터를 암호화하고, 인터넷 상에 안전하고 신뢰할 수 있는 데이터 터널을 구축하여 전송 과정 중 데이터의 안전을 보장합니다. 고객의 데이터 현지화 요구를 충족하기 위해, Tencent Cloud 는 전 세계 여러 지역에서 관련 국제 표준과 현지 안전 요구사항에 따라 데이터센터를 건설하거나 임대하여, 고객에게 다중 지역(region) 및 다중 가용 영역(zone) 선택을 제공합니다. 또한, 사업 운영 관할권의 사용자 개인정보 보호 및 데이터 보안 관련 법률 규정을 엄격히 준수하며, 지속적으로 현지 규제 동향을 주의 깊게 모니터링합니다. 현재 Tencent Cloud 는 한국에 두 개의 데이터센터를 보유하고 있으며, 클라우드 서버, 클라우드 데이터베이스,

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
			클라우드 스토리지 등을 포함한 다양한 클라우드 컴퓨팅 서비스를 제공합니다. 한국 고객은 한국 현지에서 자신의 데이터를 저장, 처리 및 백업할 수 있습니다. 또한 Tencent Cloud 의 개인정보 수집, 처리 및 공유에 관한 자세한 정보는 개인 정보 처리 방침을 참조하시기 바랍니다. Tencent Cloud 는 데이터 보안 관련 관리 절차를 수립하여 데이터 분류 및 등급화와 데이터 보호 원칙을 명확히 했으며, 데이터 소유자가 데이터 분류 및 등급화 요구에 따라 데이터 수집, 전송, 접근 통제, 백업, 거래 보호, 그리고 제 3 자와의 정보 전송 관리 전 생애 주기 동안 상응하는 보안 보호 조치를 시행하여 데이터의 기밀성, 무결성 및 가용성을 보호하도록 요구합니다. 고객 데이터는 Tencent Cloud 내에서 최고 수준의 보안 등급으로 분류되며, 고객은 자신의 데이터 콘텐츠에 대한 유일한 소유권과 통제권을 보유합니다. 서비스 제공 또는 문제 해결의 필요성이 있고, 고객의 명시적 승인을 받았거나 국가 또는 지방 정부 부처의 범죄 사건 조사 등 국가 법률 및 규정에 부합하는 상황이 아닌 한, Tencent Cloud 내부 직원은 어떠한 고객 데이터도 절대 직접 접촉하지 않습니다.
7	보고	① 금융회사가 제 4 조제 1 항에 따라 개인고객의 금융거래정보(금융거래의 내용이 누구의 것인지를 알 수 없는 경우를 제외한다) 처리업무를 위탁하고자 하는 경우로서 업무를 수탁받는 자가 국외에 소재하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은	고객은 수탁자가 규정에 따라 정해진 기한 내에 금융감독원에 적절한 서류를 제출하고, 금융감독원의 감독과 검사를 수용하도록 보장해야 합니다. 감독 및 검토 협력 측면에서, Tencent Cloud 는 전담 인력을 제공하여 고객 또는 관련 규제 기관이 시작한 감사/검토 활동에 적극적으로 대응하거나 관련 자료를 적시에 제출할

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		업무를 실제로 수행하려는 날의 30 영업일 이전에 다음 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.	수 있습니다. Tencent Cloud 는 매년 독립된 제 3 기관의 전문 감사를 받으며, 검증보고서 성격의 시스템 및 조직 통제 보고서를 제공하여 클라우드 이용 기관, 독립 감사인, 규제 기관, 회사 주주 및 기타 이해관계자에게 Tencent Cloud 서비스 조직의 최신 내부 통제 현황을 투명하게 공개하고 있습니다.
		1. 위탁계약서(안) 사본	Tencent Cloud 는 정보 보안 연락 담당자를 지정하며, 각 지역의 정보 보안 연락 담당자는 규정 준수 및 업무 요구사항에 따라 현지 규제 기관 및 고객과 원활한 소통을 유지하여 Tencent Cloud 가 법률, 규제 및 계약 합의를 준수하도록 합니다.
		2. 「금융기관의 업무위탁 등에 관한 규정」 제 3 조의 2 에 따라 금융기관이 마련하고 준수하여야 할 '업무위탁 운영기준'	
		3. 업무위탁 계약이 이 규정 등 관련법령에 위배되지 아니한다는 준법감시인(준법감시인이 없는 경우, 감사 등 이에 준하는 자)의 검토의견 및 관련자료 사본	고객 또는 관련 규제 기관이 발견한 문제점 또는 제안사항에 대해, Tencent Cloud 는 고객에 미칠 수 있는 영향을 평가하고 문제 발생의 근본 원인을 심층 분석하며, 이에 따라 상응하는 시정 조치를 수립 및 시행합니다. 해당 문제가 금융 기관 고객의 업무 운영 또는 데이터 보안에 영향을 미칠 수 있는 경우, Tencent Cloud 는 관련 금융 기관에 적시에 통보합니다. 동시에, 경영진은 시정 계획 및 구체적 조치의 이행 상황을 정기적으로 추적하고 지속적으로 모니터링하여 문제가 효과적으로 해결되도록 보장합니다.
		4. 위탁의 필요성 및 기대효과	
		5. 위탁에 따른 업무처리절차의 주요 변경내용	사건 대응 및 처리 측면에서 Tencent Cloud 는 정보 보안 사건 관리 규정을 수립하고, 정보 보안 보고, 대응 및 처리 메커니즘과 관련 절차를 마련하였으며, 사건 처리 절차에서 각 팀의 역할과 구체적인 책임을 명확히 하였습니다.
		6. 정보처리업무 운영에 대한 감독기관의 실질적 감독가능성을 확인할 수 있는 서류	
		7. 위탁계약 상대방(재위탁 예정시 재위탁계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)	Tencent Cloud 는 내부 보안 운영 시스템을 사용하여 보안 사건을 기록합니다. 탐지 및 식별된 보안 사건에 대해 Tencent Cloud 는 사건의
		8. 전산사고 및 정보유출 등 발생시 피해자 구제절차	
		② 금융회사가 제 4 조제 1 항에 따라 개인고객의 금융거래정보(금융거래의 내용이 누구의 것인지를 알 수 없는 경우를 제외한다) 처리업무를 위탁하고자 하는	

번호	통제 영역	통제 요구사항 요약	Tencent Cloud 의 대응
		경우로서 업무를 수탁받는 자가 국내에 소재하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은 업무를 실제로 수행하려는 날의 7 영업일 이전에 제 1 항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다. ③ 금융회사가 제 1 항 및 제 2 항에 따른 보고의 대상이 되는 금융거래정보를 제외한 금융거래정보의 처리를 위탁하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은 업무를 실제로 수행하는 날로부터 10 영업일 이내에 제 1 항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.	성격, 데이터 민감도, 영향 범위 등의 요소를 고려하여 보안 사건을 분석 및 등급 분류하고, 적시에 해당 책임자에게 알려 사건을 추적 처리하도록 합니다. 고객에게 영향을 미칠 수 있는 보안 사건의 경우 Tencent Cloud 는 정보 보안 사건의 영향 범위와 정도에 따라 내부 검토를 거친 후, 적절한 방법으로 고객에게 정보 보안 사건 처리 및 분석 결과를 통지하고, 해당 기술 지원을 제공하여 고객이 손실을 최소화하기 위한 보완 조치를 취할 수 있도록 지원합니다.
8	감독 및 검사	① 위탁 금융회사 및 해당 업무의 수탁회사는 제 4 조에 따라 위탁 운영되는 정보처리 업무와 관련하여 금융감독원장의 자료 제출 등 감독 및 검사를 위한 요구에 응하여야 한다.	

09

결론

Tencent Cloud 는 Tencent 그룹이 전력을 다해 구축한 클라우드 컴퓨팅 브랜드로, Tencent 의 다년간 기술 축적과 보안 실무 역량을 계승하고 있습니다. Tencent Cloud 는 고객에게 지속적이며 안전하고 신뢰할 수 있으며 지능적인 클라우드를 제공하고, 더 많은 기업이 효율적으로 디지털화의 물결을 맞이하고 기업의 안전한 발전을 추진하도록 지원하는 데 전념하고 있습니다.

본 가이드는 한국 금융위원회의 중요한 규제 요구사항에 기반하여, 고객에게 Tencent Cloud 가 어떻게 고객의 클라우드 시스템 및 데이터의 규정 준수를 지원하는지 포괄적이고 투명하게 보여주며, 기업 고객이 시스템과 데이터를 클라우드에 안심하고 위탁할 수 있도록 지원합니다. Tencent Cloud 는 본 가이드를 통해 기업 고객이 규제 기관의 준수 기준을 효과적으로 충족하고, 동시에 효율적으로 디지털 전환과 비즈니스 혁신 발전을 실현하도록 지원하기를 희망합니다.

본 가이드는 참고용으로만 제공됩니다. 본 가이드의 정보에 대해, 고객은 자체 실제 상황에 따라 적절히 사용하여 Tencent Cloud 서비스 사용 과정에서의 규제 준수를 보장할 수 있습니다.

10 버전 히스토리

날짜	버전	자세한 정보
2026 년 4 월	V1.0	초기 릴리스