华为云泰国金融行业监管遵从性指南

文档版本 2.0

发布日期 2022-05-16

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 背景与发布目的

在科技发展的浪潮中，越来越多的金融机构在逐渐寻求业务转型并希望借助先进的技术以降低成本、提升运营效率、实现业务模式的创新。为了规范金融行业对于信息科技的运用，泰国央行（BoT）、证券交易委员会办公室（OSEC）发布了一系列监管要求和指南，针对泰国金融机构科技风险管理、科技外包管理以及云计算实施等方面提出了相关监管要求。

华为云作为云服务供应商，致力于协助金融客户满足这些监管要求，持续为金融客户提供遵从金融行业标准要求的云服务及业务运行环境。本文将针对泰国金融机构在使用云服务时通常需遵循的监管要求和指南，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的泰国金融监管要求简介

泰国央行（BoT）

- **No. FPG 8/2557 金融机构外包管理规定**（Regulations on Outsourcing of Financial Institutions）：针对利用服务供应商提供外包服务的金融机构，提出金融机构需要遵守的外包管理相关要求，为金融机构外包活动的风险管理提供指导。
- **No. FPG 21/2562 金融机构信息科技风险管理规定**（Information Technology Risk Regulations of Financial Institutions）：规定了科技风险管理原则和实施指引，指导金融机构建立健全、可靠的科技风险管理框架。

证券交易委员会办公室（OSEC）

- **No. Sor Thor. 37/2559 信息技术系统建设细则**（Rules in Detail on Establishment of Information Technology System）：为从事证券服务的中介机构提供在信息技术系统建设中应当遵循的企业 IT 治理和信息安全管理要求。
- **No. Nor Por. 3/2559 信息技术系统建设指南**（Guidelines for Establishment of Information Technology System）： 是对《信息技术系统建设细则》中企业 IT 治理和信息安全管理要求的解读，提供满足企业 IT 治理和信息安全管理要求的注意事项和最佳实践。

- **云计算实施指南**（Cloud Computing Practice Guide）： 旨在指导金融机构了解云计算潜在的风险，以及如何在使用云计算时进行风险管理和安全控制。

注：在泰国，保险公司由保险委员会办公室（OIC）监管。针对泰国金融机构使用云服务的场景，OIC 目前仅在《保险公司第三方（外包）服务使用指南》（Guidelines on the use of services from third parties (Outsourcing) of insurance companies）规定“保险公司必须对其信息技术服务供应商实行内部控制”，除此之外未公开发布其他要求。同时考虑到遵循上述要求完全属于泰国金融机构的责任，本白皮书将聚焦于 BoT 和 OSEC 发布的监管要求。

1.3 名词定义

- **华为云**

  华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。

- **客户**

  指与华为云达成商业关系的注册用户。

- **外包**

  指利用其他服务供应商履行通常全部或部分由金融机构自行履行的职能。

- **服务供应商**

  指通过订立合同，履行通常由金融机构自行履行的职能的其他法人，包括任何从原始服务供应商或分包商分包或转包服务的法人。

- **云计算**

  根据美国国家标准技术研究院（NIST）的定义，是指一种基于互联网，能够按需提供共享计算机处理资源和数据的计算模式。

2 华为云安全与隐私合规

华为云继承了华为公司完备的管理体系以及 IT 系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全与合规，主要包括：

全球性标准类认证

认证	描述
ISO 20000-1:2011	ISO 20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的 IT 服务来满足客户和业务的需求。
ISO 27001:2013	ISO 27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO 27017:2015	ISO 27017 是针对云计算信息安全的国际认证。ISO 27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 22301:2012	ISO 22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
SOC 审计	SOC 审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
PCI DSS 认证	支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
CSA STAR 金牌认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和

认证	描述
	CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
国际通用准则 CC EAL3+	CC(Common Criteria)认证是一种信息技术产品和系统安全性的评估标准，它提供了一组通用的安全功能要求和安全保证要求，并在这些保证要求的基础上提供衡量 IT 安全性的尺度（即评估保证级 EAL），使得独立的安全评估结果可以互相比较。
ISO 27018:2014	ISO 27018 是专注于云中个人数据保护的国际行为准则。ISO 27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
ISO 29151:2017	ISO 29151 是国际个人身份信息保护实践指南。ISO 29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
ISO 27701:2019	ISO 27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS 10012 是 BSI 发布的个人信息数据管理体系标准，BS10012 认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。

地区性标准类认证

认证	描述
网络安全等级保护	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键 Region、节点通过了网络安全等级保护四级。
新加坡 MTCS Level 3 认证	MTCS 多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求 CSP 在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得 MTCS 最高安全评级的 Level 3 等级认证。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
云服务用户数据保护能力认证	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。

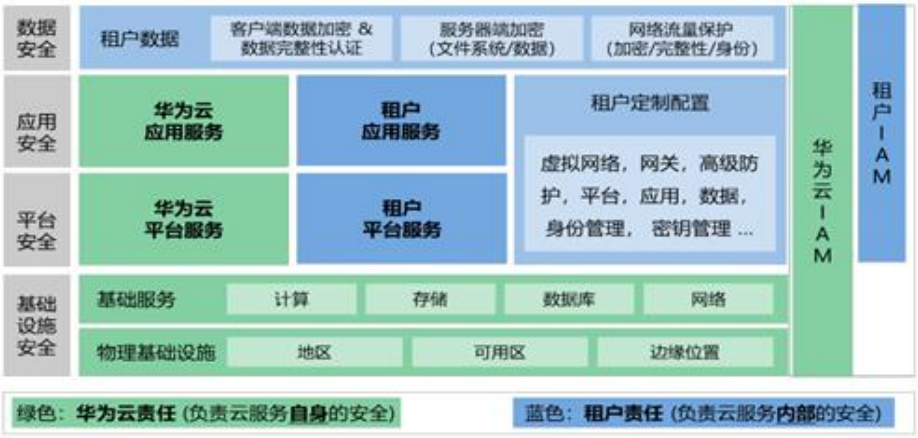
认证	描述
工信部云计算服务能力 评估	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。
可信云评估	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。
网信办网络安全审查	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。

关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网“信任中心-安全合规”。

3 华为云安全责任共担模型

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

图3-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和 IAM 层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与租户的安全责任详情，可参考华为云已发布的《华为云安全白皮书》。

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网“全球基础设施”。

5 华为云如何遵从 BoT《金融机构外包管理规定》的要求

《金融机构外包管理规定》：泰国央行按照工作职能对外包服务进行分类，并明确金融机构对不同类型外包的许可条件，并从金融机构的董事会的职责、服务供应商的选择、消费者保护、服务供应商的业务连续性管理、合同和协议等方面提出对金融机构外包管理相关要求，为金融机构外包活动的管理提供指导。

金融机构在遵循《金融机构外包管理规定》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《金融机构外包管理规定》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

5.1 服务供应商的选择

《金融机构外包管理规定》附件 3 第 2 条要求金融机构应当制定服务供应商选择标准，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
附件 3 第 2 条	服务供应商的选择	选择服务供应商金融机构在签订新合同或续签合同之前，必须具备适当的服务供应商选择标准，包括以下关键问题。 （1）技术能力、专业知识和操作经验； （2）财力； （3）商业信誉、投诉或诉讼记录； （4）适合金融机构的组织文化和服务政	客户应建立制定服务供应商的选择标准。 **（1）技术能力：**华为云用在线提供云服务的方式，将华为 30 多年在 ICT 基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在 AI 领域，华为云 AI 已在城市、制造、物流、互联网、医疗、园区等 10 大行业的 300+个项目进行落地。在多元架构方面，华为云打造了基于 X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的

原文编号	控制域	具体控制要求	华为云的应答
		策； （5）对新发展作出反应的能力； （6）集中度风险。 （7）为董事会和高级管理人员考虑外包服务制订了清晰的规则。	算力之上，实现客户价值最大化。 **（2）财力：**华为云是华为的云服务品牌，自 2017 年正式上线以来,华为云一直处于快速发展中，收入保持强劲增长态势。全球权威咨询机构 Gartner 发布的《Market Share: IT Services, worldwide 2019》报告显示，华为云全球 IaaS 市场排名第六，中国市场排名前三，全球增速最快，高达 222.2%。 **（3）商业声誉：**华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现大突破。在海外市场，华为云香港、俄罗斯、泰国、南非、新加坡大区相继开服。 **（4）适合金融机构的企业文化和服务政策：**华为云在产品和服务规划和阶段会根据客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。 **（5）对新发展作出反应的能力：**自上线以来，华为云一直坚持技术创新，发布了一系列业界领先的新品和升级，覆盖云安全、DevOps、云容器引擎和微服务引擎、服务网格、计算、云存储、网络、云容灾等多个领域，让产品始终保持先进性。 **（6）风险管理能力：**华为云继承了华为公司的风险管理能力，建立了风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中有效控制风险，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。 **（7）运营能力：**华为云遵循 ISO27001、ISO20000、ISO22301 等国

原文编号	控制域	具体控制要求	华为云的应答
			际标准建立信息安全管理体系、IT 服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。

5.2 消费者保护

《金融机构外包管理规定》附件 3 第 3 条提到“金融机构必须始终意识到，外包只是将服务委托给服务供应商。金融机构继续对消费者负责，就像金融机构自己提供服务一样。”华为云若作为金融机构的云服务供应商，仅对金融机构负责。《金融机构外包管理规定》附件 3 第 3 条要求金融机构应当制定消费者的保护机制，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
附件 3 第 3 条（1）	客户数据机密性	必须确保服务供应商能够提供良好的系统来维护客户信息和金融机构信息的安全和保密。	华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，并遵守泰国《个人数据保护法》所述的数据保护原则。同时，在与金融行业客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。 此外，华为云各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。
附件 3 第 3 条（2）	问题和事件管理	必须通过记录和监控客户投诉（包括客户信息泄露问题），配备足够的系统来处理客户投诉和解决问题，金融机构必须指定适当的指导方针来	客户应建立问题管理机制。 华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选

原文编号	控制域	具体控制要求	华为云的应答
		解决此类问题。	择适用的支持计划，获取由 IM 企业群、技术服务经理（TAM）、服务经理等组成的专属支持。 为配合客户满足事件快速响应的要求，华为云内部制定了事件管理流程，根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。
附件 3 第 3 条（3）	性能监控及容量规划	必须确保为客户提供的服务质量不会恶化并且通常由金融机构负担的成本不会由客户承担。	客户应建立性能监控及容量规划机制。 《华为云服务等级协议》约定了华为云各项产品/服务的服务等级，包括对服务可用性的承诺，以及未达到承诺的服务补偿。 为配合客户满足合规要求，华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对租户云服务的系统性能造成影响。 同时，华为云的云监控服务（Cloud Eye Service，简称 CES）为用户提供一个针对弹性云服务器（Elastic Cloud Server，简称 ECS）、带宽等资源的立体化监控平台。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。
附件 3 第 3 条（5）	客户数据删除	无论出于何种原因终止或取消合同，金融机构必须确保客户信息被销毁或完全从服	在服务协议终止时，客户可通过华为云提供的对象存储迁移服务（Object Storage Migration Service，简称 OMS）和主机迁移服务（Server Migration Service，简称 SMS），将内

原文编号	控制域	具体控制要求	华为云的应答
		务供应商处移除。	容数据从华为云中迁移出去，如迁移至本地数据中心。 在客户确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。

5.3 服务供应商的业务连续性管理

《金融机构外包管理规定》附件 3 第 4 条要求金融机构应当对与服务供应商相关的业务连续性进行管理，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
附件 3 第 4 条（1）	业务影响分析与风险评估	金融机构必须通过评估服务中断可能产生的风险和影响，明确外包活动的重要程度。	为向客户提供持续、稳定的云服务，华为云遵循 ISO22301 业务连续性管理国际标准的要求，建立了一套业务连续性管理体系。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。
附件 3 第 4 条（2）	业务连续性计划的制定和测试	金融机构必须要求服务供应商制定业务连续性计划，特别是针对重大活动或影响广泛的活动，并为此类活动分配足够的资源，在符合金融机构自身业务连续性的情况下，应用泰国央行关于金融机构业务连续性管理（BCM）和	华为云遵循 ISO22301 业务连续性管理国际标准，建立了一套业务连续性管理体系。在该体系框架下，定期进行业务影响分析和风险评估，制定了业务连续性计划和灾难恢复计划。 华为云作为客户的供应商，会积极配合客户发起的测试需求，协助客户测试其业务连续性计划的有效性。 同时，华为云根据内部业务连续性管理体系的要求，每年对业务连续性计划和灾难恢复计划进行测试，所有的

原文编号	控制域	具体控制要求	华为云的应答
		业务连续性计划（BCP）的指导方针。 金融机构必须与关键服务供应商定期对业务连续性计划进行测试，并且必须以书面形式记录测试结果，供泰国央行审查。	应急响应人员，包括后备人员均需参与。测试的类型包括桌面演练、功能演练和全面演练三种，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，若测试结果表明业务连续性计划、恢复策略或应急预案等存在不足之处，将对相关文件进行更新。

5.4 合同与协议

《金融机构外包管理规定》附件 3 第 5 条要求金融机构必须与服务供应商签订书面合同和协议，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
附件 3 第 4 条	合同与协议	金融机构必须与服务供应商签订书面合同和协议，至少考虑以下关键问题： （1）金融机构的服务类型、职责范围、风险管理、内部控制流程、信息和资产安全保障体系； （2）服务水平协议，规定服务供应商在正常和异常情况下必须执行的最低操作标准； （3）服务供应商的业务连续性计划，以支持外包服务中断或无法提供连续服务的情况； （4） 监控、审核和评估服务供应商性能	华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。

原文编号	控制域	具体控制要求	华为云的应答
		的过程； （6）合同期限、规定和合同终止条件，包括金融机构修改或延长合同的权利； （7）服务延误、差错等问题发生时对方的责任范围，以及解决问题的准则或赔偿损失； （8）信息安全，维护客户信息、金融机构信息的机密性和保密性，以及访问权和信息所有权，以及数据传输、数据维护，客户信息、金融机构信息泄露的明确处罚；鉴于此，服务供应商应将金融机构客户的数据库与服务提供商或服务提供商其他客户的数据分开。 （12） 遵守监管条例； （13）赋予泰国央行、金融机构、外部审计师或其他政府机构检查运营、内部控制流程以及向服务供应商或分包商（如有）索取相关信息的权利。	

5.5 外包活动的管控

《金融机构外包管理规定》附件 3 第 6 条要求金融机构应当监控、评估、审计和管理外包服务供应商的风险，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答

原文编号	控制域	具体控制要求	华为云的应答
附件 3 第 6 条 (2)(4)(5)	外包活动的管控	（2）安排或要求服务供应商编制操作手册和相关文件，并定期更新，以监测、评估和管理金融机构的风险； （4）安排好书面的记录，包括问题或风险、数据丢失事件以及从外包服务相关管理部门接受到的指令，供泰国央行审查； （5）根据职能分类的需要，安排定期审查所提供的服务。	华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT 服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。为配合客户满足合规要求，华为云根据内部管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。另外，华为云有专门的团队对云服务的产品说明和操作手册进行维护，在国际站上将至少提供英文版的文档。 同时，华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。 此外，华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由 IM 企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

6 华为云如何遵从 BoT《金融机构信息科技风险管理规定》的要求

泰国央行于 2019 年 11 月发布了《金融机构信息科技风险管理规定》，该规定针对金融机构提出在信息科技风险管理方面需要遵循的准则，并提供信息科技风险管理和第三方风险管理的实施指南。

金融机构在遵循《金融机构信息科技风险管理规定》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《金融机构信息科技风险管理规定》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

原文编号	控制域	具体控制要求	华为云的应答
5.3.2(2)	数据安全	金融机构必须维护数据安全，包括通过通信网络的数据存储，信息系统和各种介质的数据存储及传输。 对信息分类和分级，通过适当的安全措施保存和销毁数据，包括使用国际标准的加密算法进行加解密，以维护信息安全	客户应考虑对所有存储信息的介质（包括纸质和电子）进行保护。客户在使用加密措施保护数据时，应考虑采用业内认可的加密算法和密钥管理机制。 针对存储金融行业客户内容数据的存储介质，华为云制定了介质管理流程，确保存储在介质中的数据的安全。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。实现方式如下：当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不

原文编号	控制域	具体控制要求	华为云的应答
			可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。 目前，华为云云硬盘（Elastic Volume Service，简称 EVS）、对象存储服务（Object Storage Service，简称 OBS）、镜像服务（Image Management Service，简称 IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 华为云为客户提供了数据加密服务（Data Encryption Workshop，简称 DEW）的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW 采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，HSM 拥有 FIPS 140-2（2 级和 3 级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取客户根密钥。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。
5.3.2(3)	访问控制	金融机构必须对操作系统和数据库系统进行权限的管理和审计。基于风险级别进行权限管理和身份验证，防止	客户应建立信息系统的身份认证与访问控制管理机制，对访问系统的行为进行权限限制和监督。

原文编号	控制域	具体控制要求	华为云的应答
		未授权的访问和系统或数据篡改。	客户可通过华为云的统一身份认证服务（Identity and Access Management，简称 IAM）对使用云资源的用户账号进行管理。IAM 除了支持密码认证之外还支持多因子认证，客户可自主选择是否启用。如果租户有安全可靠的外部身份认证服务商，可以将 IAM 服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。 此外，华为云的云审计服务（Cloud Trace Service，简称 CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 为配合客户满足合规要求，华为云内部建立了运维和运营账号管理机制。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证。所有运维账号由 LDAP 集中管理，通过统一运维审计平台集中监控并进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。
5.3.2(4)	物理和环境安全	金融机构必须确保数据中心、办公场所、关键系统区域的安全。必须要对计算机设备和支持性设施建立保护	客户应当制定和实施物理和环境安全管理机制。 华为云已制定并实施了物理和环境安全防护策略、规程和措

原文编号	控制域	具体控制要求	华为云的应答
		体系和维护流程，防止非法入侵或自然灾害造成的损害，保证持续地支持业务运行。	施，满足 GB50174《电子信息机房设计规范》A 类和 TIA942《数据中心机房通信基础设施标准》中的 T3+标准。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急响应等措施。更多关于内容请参见《华为云安全白皮书》5.1 物理与环境安全。
5.3.2(5)	通信安全	金融机构必须对其通信系统进行安全控制，以确保通过其传输的系统和数据受到安全保护，并免受任何可能的攻击或威胁。	客户应当建立网络安全管理机制，确保网络中的信息及信息处理设施得到保护。 华为云一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。 华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，进一步排除单点故障的风险。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

原文编号	控制域	具体控制要求	华为云的应答
			华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。
5.3.2(6)	运行安全	金融机构必须对其信息技术业务进行安全控制，以确保信息技术业务的安全，这必须包括但不限于以下内容： （6.1）信息技术系统和设施系统的能力管理，例如对信息技术资源的未来需求进行评估，以便对信息技术资源进行适当管理，因为这些资源能够充分支持业务运营，而金融机构则可以管理信息技术资源以满足其未来需求； （6.2）服务器和用户设备（终端设备）的安全控制，如安装防病毒或防恶意软件，以防止数据泄露或未经授权的访问； （6.3）数据备份-必须在适当的时间范围内（如每天）使用适当的方法备份数据，以便在原始数据不可用或损坏时随时可以使用备份数据； （6.4）保存服务器和重要网络硬件的日志，如保存和审查访问日志和活动日志，以监测和检查系统或数据的访问和使用； （6.5）安全监控-必须有监控可能影响关键 IT 系统的可疑事件或威胁的流程或工具，例如安装监控和分析网络威胁的系统，以便金融机构能够及时发现、预防和处理可疑事件或威胁； （6.6）根据风险水平管理系	**1.容量和性能管理：**客户可通过华为云的云监控服务（CES）对弹性云服务器（ECS）、带宽等资源进行的立体化监控。云监控服务的监控对象是基础设施、平台及应用服务的资源使用数据，不监控或触碰租户数据。云监控服务目前可以监控多个云服务的相关指标，用户可以通过这些指标，设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。 同时，华为云内部也制定了性能与容量管理流程，通过提前识别资源需求以及对平台资源容量和设备库存进行统筹管理，对资源使用率和资源可用性水平的不断优化，最终保证云资源满足用户的业务正常需求。 **2.主机安全管理：**客户可用通过使用华为云的企业主机安全服务（Host Security Service，简称 HSS）来保护主机安全。企业主机安全服务提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。 **3.备份管理：**华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用对象存储服务（OBS）的版本控制、云硬盘备份（Volume Backup Service，简称 VBS）、云服务器备份

原文编号	控制域	具体控制要求	华为云的应答
		统漏洞-以便发现漏洞，金融机构能够迅速采取进一步行动防止可能的威胁；关键 IT 系统的漏洞评估必须至少每年或在相关技术标准发生重大变化时进行一次； （6.7）渗透测试，可由独立的内部或外部专家进行；测试必须覆盖面向互联网的系统，并且至少每年或在出现任何重大变化时进行一次，以便发现漏洞，并且金融机构能够迅速作出改进，以防止可能的威胁； （6.8）变更管理-必须有一个安全和充分的过程来管理和控制变更，可以是系统部署、系统配置、补丁安装等形式，以确保变更正确和完全地达到规定的目标，并防止未经授权的变更； （6.9）系统配置管理-生产系统的配置必须有一个控制过程，并且必须定期审查配置，以防止操作错误； （6.10）补丁管理-必须有一个在生产系统上安装补丁的控制过程，以便及时安装重要的安全补丁。	（Cloud Server Backup Service，简称 CSBS）等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保证在灾难发生时数据不丢失。 **4.日志和监控管理：**华为云的云审计服务（CTS）为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触发的操作。CTS 会对各服务发送过来的日志数据进行检视，确保数据本身不含敏感信息；在传输阶段，通过身份认证、格式校验、白名单校验以及单向接收机制等手段，确保日志信息传输和保存的准确；在保存阶段，采取多重备份，并根据华为网络安全规范要求，对数据库自身安全进行安全加固，杜绝仿冒、抵赖、篡改以及信息泄露等风险；最后，CTS 支持数据以加密的方式保存到 OBS 桶。同时，华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以确保支撑网络安全事件回溯和合规。 **5.漏洞和补丁管理：**华为产品安全事件响应团队（PSIRT – Product Security Incident Response Team）于 2010 年正式成为国际应急响应论坛 FIRST 成员之一，通过该组织可实现与 471 个成员交流业界最佳实践和安全信息；华为 PSIRT 已经建立成熟的漏洞响应机制，

原文编号	控制域	具体控制要求	华为云的应答
			针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。同时，华为 PSIRT 和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对租户业务造成影响。此外，华为云镜像服务（IMS）简单方便的镜像自助管理功能。客户可通过服务控制台或 API 对自己的镜像进行管理。 华为云负责公共镜像的定期更新与维护向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息以便用户在部署测试 、故障排除等运维活动时参考 。 **6.渗透测试：**为配合客户满足合规要求，华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。 **7.变更管理：**为配合客户满足合规要求，华为云制定了规范的变更管理流程，生产环境的各要素发生变更，都需要通过有序的活动进行变更管理。所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产环境测试、灰色

原文编号	控制域	具体控制要求	华为云的应答
			发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。同时华为云制定了更细粒度的变更操作规范，指导整个变更的实施、跟踪以及变更执行后的验证，确保变更达到预期目的。 **8.配置管理：**华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的配置管理。华为云设置配置经理对所有业务单元进行配置管理，包括提取配置模型(配置项类型、各类配置项属性、配置项间的关系等)、记录配置信息等，并通过专业的配置管理数据库工具（CMDB – Configuration Management Database）对配置项、配置项的属性和配置项之间的关系进行管理。
5.3.2(7)	系统获取、开发和维护	（7.1）系统采集：金融机构必须为选择系统和服务供应商制定明确和适当的标准，其中应包括系统或服务供应商的信誉、认证（根据国际标准或公认的 IT 标准）、系统安全、系统支持和维护，确保系统和服务供应商能够响应金融机构的业务需求。其他关键问题还包括服务供应商更换的灵活性、技术变化或金融机构未来业务战略的变化； （7.2）系统开发：金融机构必须对系统进行设计、开发和测试，以确保系统准确、安全、可靠、随时可用，并具有足够的灵活性，以适应未来的任何变化。	华为的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。为配合客户满足合规要求，华为云通过制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。 华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据

原文编号	控制域	具体控制要求	华为云的应答
			公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。 华为云严格遵从华为公司对内发布的多种编程语言的安全编码规范。使用静态代码扫描工具例行检查，其结果数据进入云服务工具链，以评估编码的质量。所有云服务在发布前，均须完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。 华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，确保发布的云服务满足安全要求，测试在与生产环境隔离的测试环境中进行，并避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱敏，使用完成后需要进行数据清理。
5.3.2(8)	IT 事件和问题管理	金融机构必须妥善、及时地管理信息技术事件和问题，对事件和问题必须及时记录、分析并报告董事会、指定委员会或高级管理层。此外，金融机构必须找出这些问题的根源，才能解决实际问题，防止异常事件再次发生。	华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的事件和变更管理。华为云制定了事件和管理流程并定期对其评审和更新。华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。
5.3.2(9)	业务连续性计	（9.1）金融机构必须成立一个工作组或指定一个特定单	客户应建立自身的业务连续性机制，并制定保证其关键业务

原文编号	控制域	具体控制要求	华为云的应答
	划	位负责编制一份信息技术业务连续性计划，该计划必须是书面的，并符合规定的政策； （9.3）信息技术业务连续性计划必须切实可行，因为它可以有效地用于减少损失，并且必须符合泰国央行的政策声明：业务连续性管理（BCM）和金融机构的业务连续性计划（BCP）。计划必须规定恢复时间目标（RTO）和恢复点目标（RPO），这将取决于系统的重要性，以及最长中断容忍期（MTPD），以确保金融机构业务运营的连续性，并确保该计划能够处理可能导致系统中断或损坏的事件，如网络威胁、自然灾害。该计划还将确保金融机构能够迅速恢复系统并恢复正常运作； （9.5）IT 业务连续性计划必须至少每年或在发生任何重大变化时审查和测试一次； （9.6）金融机构必须建立灾难恢复站点，以便在主站点遇到中断时随时可以运行。灾难恢复站点应远离主站点，以确保它们不会共享相同的中断或同时受到相同原因（如断电、自然灾害）的影响。	连续的 RTO、RPO 指标。如果金融机构在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。 为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得 IS022301 认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。为配合客户满足合规要求，华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了恢复策略。 华为云作为客户的供应商，会积极配合客户发起的测试需求，协助客户测试其业务连续性计划的有效性。 同时，华为云根据内部业务连续性管理体系的要求，每年对业务连续性计划和灾难恢复计划进行测试，所有的应急响应人员，包括后备人员均需参与。测试的类型包括桌面演练、功能演练和全面演练三种，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，若测试结果表明业务连续性计划、恢复策略或应急预案等存

原文编号	控制域	具体控制要求	华为云的应答
			在不足之处，将对相关文件进行更新。 为配合客户满足合规要求，华为云根据内部业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。 业务连续性计划、突发事件应急预案、灾难恢复操作手册等文件通过电子和纸质的方式保留多个副本，并分发给相应的管理层及其他主要人员。 客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。
5.3.2(10)	第三方风险管理	（10.1）明确并书面定义金融机构与第三方之间的角色和责任，并规定泰国央行有权检查第三方运行情况的条件； （10.2）监控和管理在使用服务时连接第三方或从第三方获取信息而引起的风险； （10.3）确保第三方信息安全符合金融机构的信息技术安全标准和公认的网络安全国际标准的网络安全； （10.4）及时响应可能发生的事件，以及对金融机构有	华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。华为云会安排专人积极配合客户发起的审计要求。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR

原文编号	控制域	具体控制要求	华为云的应答
		重大影响的事件，以保证能够持续开展业务。	等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。 另外，华为云制定了突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。

7 华为云如何遵从 OSEC《信息技术系统建设细则》和《信息技术系统建设指南》的要求

《信息技术系统建设细则》是泰国证券交易委员会办公室（OSEC）为从事证券服务的中介机构（以下简称“中介机构”）提供在信息技术系统建设中应当遵循的企业 IT 治理和信息安全的管理要求。《信息技术系统建设指南》是对《信息技术系统建设细则》的管理要求的进一步解读， 提供满足管理要求的注意事项和最佳实践。

中介机构在遵循上述法规要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《信息技术系统建设细则》和《信息技术系统建设指南》中与云服务供应商相关的控制要求，并阐述华为云会作为云服务供应商，如何帮助中介机构满足这些控制要求。

7.1 信息安全策略

《信息技术系统建设细则》第 5 条要求中介机构应当制定信息安全政策和措施，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
5（3）	信息安全策略	中介机构应当制定书面的信息技术治理政策，至少包括下列事项： （3）根据第 8 条和第 9 条制定信息安全政策和措施。	客户应建立正式的信息安全政策和流程，并定期对其进行审查。 华为云参照 ISO27001 构建了信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性等。全方位保护客户系统和数据的保密性、完整性和可用性。此外，华为云重点关注员工以及外包

原文编号	控制域	具体控制要求	华为云的应答
			人员的安全意识培养，制定了可落地的安全意识培训计划并定期执行。

7.2 信息安全组织

《信息技术系统建设细则》第 9-10 条要求中介机构应当做好信息安全组织安排，制定使用云计算的信息安全政策，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
10(1)(2)	内部组织	中介机构应当按照下列标准做好信息安全组织管理安排： （1）定义和记录信息安全角色和职责，并为中介人员制定操作指南； （2）建立信息安全运行交叉检查，防范潜在风险。	客户应明确信息安全组织，定义信息安全角色和职责，并建立信息安全职责分离或交叉检查的机制。 华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。在组织方面，全球网络安全与隐私保护委员会（GSPC - Global Security & Privacy Committee）作为最高网络安全管理机构，决策和批准公司总体网络安全战略。全球网络安全与用户隐私保护官（GSPO - Global Security & Privacy Officer）及其办公室负责制定和执行华为端到端网络安全保障体系。GSPO 直接向公司首席执行官汇报。华为云信息安全管理体系已建立职责分离机制，实现内部职责权限分离。华为云对于内部人员实行基于角色的访问控制权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下使用网络分析和监控工具。
9（2）	移动设备和远程工作	中介机构应当建立信息安全机制，至少解决下列事项： （2）根据第 8（1）条制定的政策使用云计算的措施，包括： （a）云服务供应商与	客户应建立云服务供应商的信息安全管理机制，明确在使用云服务时对云服务供应商的信息安全要求。 华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为

原文编号	控制域	具体控制要求	华为云的应答
		中介机构之间的协议，其中至少包含以下事项： 1.云服务供应商的角色和责任，以及在云服务供应商未能遵守本协议的情况下对中介机构的责任； 2.符合国际公认的信息安全标准的操作程序； 3.信息技术安全、访问控制和信息披露措施； 4.由独立审计师对云服务供应商的运营进行审计； 5.云服务供应商转包给其他云服务供应商的条件，以及因该云服务供应商的运营而可能产生的损害赔偿； （b）分包云服务供应商在信息安全方面的资质与云服务供应商相当或符合国际标准； （c）监测、评估和审查云服务供应商的服务性能； （d）在替换云提供程序时迁移到新云提供程序的过程。	云也制定了线下合同模板，可根据不同客户的需求进行定制化。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。 华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立信息安全管理体系、IT 服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。 华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。 在服务协议终止时，客户可通过华为云提供的对象存储迁移服务（OMS）和主机迁移服务（SMS），将内容数据从华为云中迁移出去，如迁移至本地数据中心。

7.3 访问控制

《信息技术系统建设细则》第 20 条要求中介机构应当对信息和信息系统实施访问控制，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
20（1）	用户访问管理	中介机构应当按照下列标准对信息和信息系统实施访问控制： （1）应建立用户管理，以限制授权用户的访问，如下所示： （a）正式的用户注册过程，以允许访问权的分配； （b）应限制和控制特权访问权的分配和使用； （c）密码的分配应通过正式的管理过程加以控制； （d）定期监控和检查用户的访问权限。	客户应建立用户访问管理机制，对访问系统的行为进行权限限制和监督。 客户可通过华为云的统一身份认证服务（IAM）对使用云资源的用户账号进行管理。IAM 除了支持密码认证之外还支持多因子认证，客户可自主选择是否启用。如果租户有安全可靠的外部身份认证服务商，可以将 IAM 服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。 此外，华为云的云审计服务（CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 为配合客户满足合规要求，华为云内部建立了运维和运营账号管理机制。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证。所有运维账号由 LDAP 集中管理，通过统一运维审计平台集中监控并进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。
20（3）	系统和应用的访问控制	中介机构应当按照下列标准对信息和信息系统实施访问控制： （3）对未经授权访问信息系统和应用程序的控制如下： （a）根据定义的访问权限控制用户和系统管理员对信息和应用	客户应制定系统和应用的访问管理机制，管控其员工对系统和应用的访问。 华为云的统一身份认证服务（IAM）为客户提供云上资源访问控制。使用 IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用 IAM 可以避免与其他用户共享账号

原文编号	控制域	具体控制要求	华为云的应答
		系统功能的访问； （b）通过安全登录程序控制对信息系统和应用程序的访问； （c）建立密码管理制度，确保密码安全；	密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过云审计服务（CTS）作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。 同时，华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，如 USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。

7.4 密码管理

《信息技术系统建设细则》第 8（2）条要求中介机构应当制定并实施密码控制和密钥管理机制，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
8（2）	密码控制	中介机构应当建立文件化的信息安全政策，该政策至少覆盖下列事项：（2）使用密码控制和密钥管理保护敏感和关键信息的政策。	客户在使用加密措施保护数据时，应考虑采用业内认可的加密算法和密钥管理机制。 目前，华为云云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 华为云为客户提供了数据加密服务（DEW）的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW 采用分层密钥管

原文编号	控制域	具体控制要求	华为云的应答
			理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，HSM 拥有 FIPS 140-2（2 级和 3 级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取客户根密钥。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。 更多信息请参见《华为云安全白皮书》6.8.2 数据加密（DEW）服务。

7.5 物理和环境安全

《信息技术系统建设细则》第 18-19 条要求中介机构应当制定物理和环境安全管理机制，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
18(1)(2) &19	物理和环境安全	中介机构应当按照下列标准制定实物和环境安全措施，保护其资产： （1）根据风险评估的结果和重要性评估 IT 资产的安全需求; （2）定义安全区域和关键 IT 资产的位置，以确保安全并防止未经授权的物理访问。 除第 18 条规定之物理及环境安全措施外，中介机构应防止设备资产的遗失、损坏、盗窃或损害，以	客户应当制定和实施物理和环境安全管理机制。 华为云已制定并实施了物理和环境安全防护策略、规程和措施，满足 GB50174《电子信息机房设计规范》A 类和 TIA942《数据中心机房通信基础设施标准》中的 T3+标准。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急

原文编号	控制域	具体控制要求	华为云的应答
		及被不相关人士进行操作。	响应等措施。更多关于内容请参见《华为云安全白皮书》5.1 物理与环境安全。

7.6 运行安全

《信息技术系统建设细则》第 23 条要求中介机构应当制定与信息系统有关的操作安全措施，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
23（1）	运行规程与责任	中介机构应当按照下列标准制定与信息系统有关的操作安全措施：（1）规定与信息系统有关的操作程序，确保操作的正确、安全。	客户应考虑通过正式的程序来管理变更，建立正式的容量管理程序，对其云资源进行监控，确保云资源能够满足业务增长的需要。客户在部署开发环境、测试环境和生产环境时，应保证环境间物理和逻辑层面都实现隔离，并严格管理对环境的访问。 **变更管理：** 为配合客户满足合规要求，华为云制定了规范的变更管理流程，生产环境的各要素发生变更，都需要通过有序的活动进行变更管理。所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。同时华为云制定了更细粒度的变更操作规范，指导整个变更的实施、跟踪以及变更执行后的验证，确保变更达到预期目的。 **容量管理：** 客户可通过华为云的云监控服务（CES）对弹性云服务器（ECS）、带宽等资源进行的立体化监控。云监控服务的监控对象是基础设施、平台及应用服务的资源使用数据。云监控服务目前可以监控下列云服务的相关指标：弹性云

原文编号	控制域	具体控制要求	华为云的应答
			服务器、云硬盘服务（EVS）、虚拟私有云服务（VPC）、关系型数据库服务（RDS）、分布式缓存服务（DCS）、分布式消息服务（DMS）、弹性负载均衡（ELB）、弹性伸缩服务（AS）、网站应用防火墙（WAF）、主机漏洞检测服务（HVD）、云桌面服务（Workspace）、机器学习服务（MLS）、网页防篡改服务（WTP）、数据仓库服务（DWS）、人工智能服务（AIS）等。用户可以通过这些指标，设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。 同时，华为云内部也制定了性能与容量管理流程，通过提前识别资源需求以及对平台资源容量和设备库存进行统筹管理，对资源使用率和资源可用性水平的不断优化，最终保证云资源满足用户的业务正常需求。 **开发、测试与运行环境的分离：** 华为的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。
23（2）	恶意软件防范	中介机构应当按照下列标准制定与信息系统有关的操作安全措施：（2）制定防范、检测恶意软件的措施和恢复信息系统免受恶意软件攻击的措施。	客户应制定防范、检测恶意软件的措施。 华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。华为云对引入的开源及第三方软件制定了明确的安全要求和流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。 为了保证华为云平台以及网络的安全、稳定运行，华为云采取了一系列管理措施，包括：漏洞分析和处理，日志监控和事件响应、云产品默认安全配置优化、安全补丁部署、防病毒软件部署以及定期备份系统和设备配置文件并测试其有效性。 华为 PSIRT 和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。同时，华为云会积极实施云产品和云平台的安全质量保证工作，每年会开展内部和第三方渗透测试和安全评估，

原文编号	控制域	具体控制要求	华为云的应答
			以保证华为云云环境的安全性。
23（3）	备份	中介机构应当按照下列标准制定与信息系统有关的操作安全措施：（3）备份关键业务信息、计算机操作系统、应用软件，并且至少每年进行一次数据备份测试。	客户应制定备份管理机制，对关键业务数据、操作系统、应用软件进行备份。 华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用对象存储服务（OBS）的版本控制、云硬盘备份（VBS）、云服务器备份（CSBS）等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保证在灾难发生时数据不丢失。 同时，客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。
23（4）	日志和监控	中介机构应当按照下列标准制定与信息系统有关的操作安全措施：（4）完整、充分地存储和记录日志，用于检查组织中的利益冲突，按照分配的角色和职责使用信息和信息系统、未经授权的访问、信息系统的非正常和/或非法使用等。 应根据组织的风险评估，监测和分析使用关键信息系统所记录的日志。	客户应建立日志管理机制，对关键信息系统的日志进行完整、充分地存储和记录，以及监测和分析。 华为云的云审计服务（CTS）为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触发的操作。CTS 会对各服务发送过来的日志数据进行检视，确保数据本身不含敏感信息；在传输阶段，通过身份认证、格式校验、白名单校验以及单向接收机制等手段，确保日志信息传输和保存的准确；在保存阶段，采取多重备份，并根据华为网络安全规范要求，对数据库自身安全进行安全加固，杜绝仿冒、抵赖、篡改以及信息泄露等风险；最后，CTS 支持数据以加密的方式保存到 OBS 桶。

原文编号	控制域	具体控制要求	华为云的应答
			同时，华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源 ID(如：源 IP、主机 ID、用户 ID 等)、事件类型、日期时间、受影响的数据/组件/资源的 ID（如目的 IP、主机 ID、服务 ID 等）、成功或失败等信息，以确保支撑网络安全事件回溯和合规。该日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间超过 180 天，90 天内可以实时查询。华为云设置独立的内审部门，定期对运维流程各项活动进行审计，以及时发现、纠正违规行为。
23（6）	技术漏洞管理	中介机构应当按照下列标准制定与信息系统有关的业务安全措施：（6）建立有效的技术漏洞管理流程如下： （a）根据风险评估结果和业务影响分析，由独立于各单位并负责信息技术的人员对与不受信任网络相连的关键信息系统进行渗透测试； （b）每年至少对所有关键信息系统进行一次漏洞评估，并在此类系统发生任何重大变化时进行评估，并立即将评估结果报告给合规部门或内部审计部门。	客户建立有效的漏洞管理机制，并定期对关键信息系统进行渗透测试。 为配合客户满足合规要求，华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。 华为产品安全事件响应团队（PSIRT - Product Security Incident Response Team）于 2010 年正式成为国际应急响应论坛 FIRST 成员之一，通过该组织可实现与 471 个成员交流业界最佳实践和安全信息；华为 PSIRT 已经建立成熟的漏洞响应机制，针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。同时，华为 PSIRT 和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。 更多信息请参见《华为云安全白皮书》8.2 漏洞管理。

7.7 通信安全

《信息技术系统建设细则》第 22 条要求中介机构应建立通信安全措施，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
22(2)(3)	网络安全管理	中介机构应当按照下列标准制定通信安全措施： （2）与供应商签订网络服务协议（包括所有网络服务的服务级别、管理要求和安全机制）； （3）正确隔离网络域，明确定义每个域的边界，并以安全的方式控制对每个域的访问。	客户建立网络安全管理机制，确保网络中的信息及信息处理设施得到保护。 为配合客户行使对云服务供应商的监管，华为云线上的《华为云用户协议》对客户和华为的安全职责进行划分，《华为云服务等级协议》约定了华为云各项产品/服务的服务等级，包括对服务可用性的承诺，以及未达到承诺的服务补偿。 华为云一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。 客户可以使用华为云提供的虚拟私有云（Virtual Private Cloud，简称 VPC）、**弹性负载均衡（Elastic Load Balance，简称 ELB）**服务，实现不同区域之间网络隔离和负载平衡。其中 VPC 可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络 ACL 和安全组规则，对进出子网以和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。ELB 将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。另外，华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相

原文编号	控制域	具体控制要求	华为云的应答
			连，进一步排除单点故障的风险。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。 华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。
22(4)(5)	信息传输	中介机构应当按照下列标准制定通信安全措施： （4）建立保护计算机网络系统信息传输的程序； （5）安排业务执行人或外包商（如有）的人员签订保密协议或保密协议。	客户应制定数据管理机制，保证数据的机密性、完整性，采取协议约束、审查监督等方式确保服务供应商的安全政策、程序和控制措施将使机构能够保护其客户信息的保密性和安全性。 客户可通过华为云的数据存储加密服务实现对数据的加密，华为云将复杂的数据加解密、密钥管理逻辑进行封装，使得客户的数据加密操作变得简单易行。目前，云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能，采用高强度的算法对存储的数据进行加密。服务端加密功能集成了华为云数据加密服务（DEW）的密钥管理功能，其中使用的硬件安全模块（HSM）经过严格的国际安全认证，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取客户根密钥。对于传输中的数据，当客户通过互联网提供 Web 网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给 Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。客户可以使用华为云提供的虚拟专用网络（Virtual Private Network，简称 VPN）、**云专线（Direct Connect，简称 DC）**、**云连接（Cloud Connect，简称 CC）**等服务，实现不同区域之间业务的互联互通和

原文编号	控制域	具体控制要求	华为云的应答
			数据传输安全。VPN 服务采用华为公司专业设备，基于 IKE 和 IPsec 协议在 Internet 网络上虚拟出私有网络，在本地数据中心和华为云 VPC 之间、华为云不同区域的 VPC 之间构建安全可靠的加密传输通道。云专线服务基于运营商多种类型的专线网络，在本地数据中心与华为云 VPC 之间构建专享的加密传输通道，各客户专线之间物理隔离，满足更高的安全性、稳定性要求。云连接服务能够快速在多个本地数据中心与多个云上 VPC 之间建立私有通信网络，支持跨云 VPC 的互连，大大提升了客户业务向全球拓展的安全性和速度。 华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令。华为云会安排专人积极配合客户发起的保密要求。华为云避免未经授权的信息披露的责任和行动、违反或终止协议时应采取的预期行动、客户对华为云的审计和监督权利等内容，会根据实际情况在与客户签订的协议中进行约定。 华为云已通过 ISO27001、ISO27017、ISO27018、SOC、CSA STAR 等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。此外，华为云制定了供应商管理机制，定期对供应商（包括外包人员）的表现进行考核，考核结果作为下次采购的关键参考。华为云也会与供应商（包括外包人员个人）签订安全合规和保密协议。

7.8 系统获取、开发和维护

《信息技术系统建设细则》第 24 条要求中介机构应当建立安全开发管理规范，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
24(3)(4)	开发和支持过程的安全	中介机构应确保信息系统的系统获取、开发及维护符合下列标准： （3）按照既定的变更控制程序，建立对现有信息系统的开发或变更的控制； （4）对开发或变更后的信息系统进行测试，确保信息系统能够高效运行、准确处理，满足用户的需求。	客户应考虑通过正式的程序来管理变更。 为配合客户满足合规要求，华为云制定了规范的变更管理流程，生产环境的各要素发生变更，都需要通过有序的活动进行变更管理。所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。同时华为云制定了更细粒度的变更操作规范，指导整个变更的实施、跟踪以及变更执行后的验证，确保变更达到预期目的。另外，华为云也制定了规范的紧急变更管理流程。若紧急变更影响到用户，会按规定的时限提前通过公告、邮件、电话、会议等方式与用户沟通；若紧急变更不满足提前规定的通知时限，变更将升级至华为云高层领导，并在变更实施后及时对用户公告。变更均留有记录，在变更执行前保留旧的程序版本及数据，在变更过程中通过双人操作等机制保证变更顺利进行，尽量减少对生产环境的影响。变更实施后，有专人进行验证，确保变更达到预期的目的。
24(6)(8)	开发和支持过程的安全	中介机构应确保信息系统的系统获取、开发及维护符合下列标准： （6）控制与信息系统开发相关的人员、流程和技术，以确保整个开发生命周期中的信息安全； （8）由用户或独立测试人员对开发的信息系统进行测试。	客户应建立安全开发管理机制。 华为的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。为配合客户满足合规要求，华为云通过制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。 华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场

原文编号	控制域	具体控制要求	华为云的应答
			景、数据流图、组网模型进行威胁分析。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。 华为云严格遵从华为公司对内发布的多种编程语言的安全编码规范。使用静态代码扫描工具例行检查，其结果数据进入云服务工具链，以评估编码的质量。所有云服务在发布前，均须完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。 华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，确保发布的云服务满足安全要求，测试在与生产环境隔离的测试环境中进行，并避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱敏，使用完成后需要进行数据清理。

7.9 IT 外包

《信息技术系统建设细则》第 8 条和第 25 条要求中介机构应当建立 IT 外包安全管理机制，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
8(5) 25(1)(6)(7)	IT 外包的信息安全	中介机构应当建立文件化的信息安全政策，该政策至少涉及以下事项：（5）信息技术外包的使用政策，包括外包商的选择和评估、外包商资质的审查，以及提供	客户应在与供应商签署的协议中确立与信息安全相关的要求和措施，应在选择服务供应商前进行尽职调查，特别是敏感信息的保密性、信息和信息系统的完整性以及信息系统的可用性。客户应定期审查外包商的财务状况和服务能力。

原文编号	控制域	具体控制要求	华为云的应答
		与使用服务相关的服务，以确保减轻外包商获取组织 IT 资产的风险； 中介机构委托外包机构从事信息系统业务的，应当符合下列条件： （1）在双方签署的协议中确立与信息安全相关的条件和控制措施； （6）明确中介机构检查外包商经营情况的权利，以确保遵守约定的条款。除外包商有限制外，中介方应制定另一措施，确保外包商的经营符合约定的期限； （7）确定外包商同意的条款，允许证券交易委员会办公室调用和检查相关文件，或进入和检查外包商的运营。	华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。 华为云会安排专人积极配合客户发起的审计要求和尽职调查。华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界标准，在身份认证与访问控制、权限管理、数据隔离、传输安全、存储安全、数据删除、物理销毁、数据备份恢复等方面，采用主流技术、实践和流程，保证用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。另外，华为云制定了突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。 华为每年会发布年报，会包含华为云的营收情况，并对外公开。自 2017 年正式上线以来,华为云一直处于快速发展中，收入保持强劲增长态势。全球权威咨询机构 Gartner 发布的《Market Share: IT Services, worldwide 2019》报告显示，华为云全球 IaaS 市场排名第六，中国市场排名前三，全球增速最快，高达 222.2%。 华为云用在线提供云服务的方式，将华为 30 多年在 ICT 基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在 AI 领域，华为云 AI 已在城市、制造、物流、互联网、医疗、园区等 10 大行业的 300+个项目进行落地。在多元架构方面，华为云打造了基于 X86+鲲鹏+

原文编号	控制域	具体控制要求	华为云的应答
			昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。
25(2)(3)	供应商服务交付管理	中介机构委托外包商从事信息系统业务的，应当符合下列条件： （2）定期对外包商的服务提供情况进行监测、评估、审查和审计； （3）当与信息安全相关的过程、程序和控制发生变化或外包商发生变化时，重新评估和管理风险。	客户应定期对其外包服务供应商执行独立审计或专家评估。 华为云会安排专人积极配合客户发起的审计要求。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR 等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。此外，华为云制定了供应商管理机制，定期对供应商（包括外包人员）的表现进行考核，考核结果作为下次采购的关键参考。华为云也会与供应商（包括外包人员个人）签订安全合规和保密协议。

7.10 信息安全事件管理

《信息技术系统建设细则》第 11 条要求中介机构应当建立信息安全事件管理机制，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
11(1)(2)(3) (4)(5)(7)	信息安全事件管理	中介机构应当按照下列标准建立信息安全事件管理制度： （1）建立管理信息安全事件的程序和流程； （2）明确信息安全事件管理责任人； （3）立即向第（2）项下的负责人和证券交易委员会办公室报告任何信息安全事件； （4）每年至少对	客户应当建立信息安全事件管理机制。 华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM – Security Information and Event Management）系统如 ArcSight、Splunk 对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持

原文编号	控制域	具体控制要求	华为云的应答
		（1）项下的信息安全事件管理程序和流程进行一次测试，测试应至少涵盖网络安全威胁管理（网络安全演习）； （5）审查信息安全事件管理中的程序和过程，对于可能影响信息系统安全的情形按照（4）项至少每年进行一次测试； （7）保存与信息安全事件管理相关的所有文件，保存期限至少为自发布之日起两年。	续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有 7*24 的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。 华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。测试场景将结合当下常见的网络安全威胁，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，若测试结果表明信息安全事件管理程序和流程等存在不足之处，将对相关文件进行更新。同时，根据内部信息安全管理体系和业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。

7.11 业务连续性的信息安全管理方面

《信息技术系统建设细则》第 12 条要求中介机构应当建立业务连续性管理的信息安全管理机制，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
12(1)(2)(3)(4)	业务连续性的信息安全管理方面	中介机构应当按照下列标准建立业务连续性管理的信息安全： （1）确定不利情况下信息安全的要求和信息安全管理的连续性； （2）建立程序、过程和控制，以确保信息安全所需的连续性水平； （3）根据信息系统的关键性和潜在影响，定义信息系统的恢复时间目标（RTO）及其要恢复的优先级； （4）如有必要，考虑冗余信息系统，以确保（3）中要求的可用性。	客户应建立自身的业务连续性机制，并制定保证其关键业务连续的 RTO、RPO 指标。如果金融机构在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。 为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得 IS022301 认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。为配合客户满足合规要求，华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了恢复策略。 客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

8 华为云如何遵从 OSEC《云计算实施指南》的要求

泰国证券交易委员会办公室于 2019 年 11 月发布了《云计算实施指南》，该指南为金融机构提供了关于使用云计算服务的治理和云服务供应商管理要考虑的做法，其中对于云服务供应商管理包括：评估和选择服务供应商、服务协议、使用云计算、服务跟踪和评估、取消或终止服务使用。

金融机构在遵循《云计算实施指南》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《云计算实施指南》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

8.1 评估和选择服务供应商

原文编号	控制域	具体控制要求	华为云的应答
2.2.1	服务供应商的选择	金融机构应明确选择云服务供应商的流程和标准，并检查服务供应商的准备情况和适用性。通过考虑重要因素，例如知识，经验，财务能力等。	客户应建立制定服务供应商的选择标准。 **（1）技术能力：**华为云用在线提供云服务的方式，将华为 30 多年在 ICT 基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在 AI 领域，华为云 AI 已在城市、制造、物流、互联网、医疗、园区等 10 大行业的 300+个项目进行落地。在多元架构方面，华为云打造了基于 X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 **（2）财务状况：**华为云是华为的云服

原文编号	控制域	具体控制要求	华为云的应答
			务品牌，自 2017 年正式上线以来,华为云一直处于快速发展中，收入保持强劲增长态势。全球权威咨询机构 Gartner 发布的《Market Share: IT Services, worldwide 2019》报告显示，华为云全球 IaaS 市场排名第六，中国市场排名前三，全球增速最快，高达 222.2%。 **（3）商业声誉：**华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现大突破。在海外市场，华为云香港、俄罗斯、泰国、南非、新加坡大区相继开服。 **（4）适合金融机构的企业文化和服务政策：**华为云在产品和服务规划和阶段会根据客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。
2.2.1	评估信息技术安全标准	评估信息技术安全标准，包括数据保密性、信息系统的完整性、服务的可用性，例如国际公认的安全标准评估结果，如 ISO27001、ISO27017，PCI-DSS 等。	华为云已获得众多国际和行业安全合规资质认证，包括 ISO27001、ISO27017、ISO27018、PCI-DSS、CSA STAR 等。华为云遵循国际标准建立信息安全管理体系、IT 服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。
2.2.1	独立审计	由独立审核员提供评估检查报告，并提供技术安全标准领域报告，例如系统和组织控制（SOC）报告，报告中应包含审计范围、审计区间、审核	华为云会安排专人积极配合客户发起的审计要求。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过 ISO27001、ISO27017、ISO27018、SOC、CSA STAR 等多项国际安全与隐私保护认证，并且每年会接受第三

原文编号	控制域	具体控制要求	华为云的应答
		结果中的关键问题。	方的审计。
2.2.1	评估持续服务能力	评估云服务供应商的连续性实践和对将在云计算系统上使用的系统的业务影响分析的一致性，包括最大可容忍停机时间（MTD）、可接受的恢复时间目标（RTO） 和恢复点目标（RPO）。	为向客户提供持续、稳定的云服务，华为云遵循 ISO22301 业务连续性管理国际标准的要求，建立了一套业务连续性管理体系。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。

8.2 服务协议

原文编号	控制域	具体控制要求	华为云的应答
2.2.2	服务协议	金融机构在与供应商签订的服务协议中，应考虑以下重要的条件： A.服务供应商与服务用户之间的协议至少具有以下详细信息： 1.服务供应商的职责，以及在服务商未能遵守本协议的情况下对中介机构的责任； 2. 符合国际公认的信息安全标准的操作程序； 3. 信息技术安全、访问控制和信息披露措施； 4. 由独立审计师对云服务供应商的运营进行审计； 5. 云服务供应商转包给其他服务供应商的	客户应建立云服务供应商的信息安全管理机制，明确在使用云服务时对云服务供应商的信息安全要求。 华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。 华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立信息安全管理体系、IT 服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。 华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。 在服务协议终止时，客户可通过华为

原文编号	控制域	具体控制要求	华为云的应答
		条件，以及其他服务供应商的运营可能造成的损害赔偿责任条款。 B. 分包云服务供应商在信息安全方面的资质与云服务供应商相当或符合国际标准； C. 监测、评估和审查云服务供应商的服务性能； D. 在替换云提供程序时迁移到新云提供程序的过程。	云提供的对象存储迁移服务（OMS）和主机迁移服务（SMS），将内容数据从华为云中迁移出去，如迁移至本地数据中心。

8.3 使用云计算

原文编号	控制域	具体控制要求	华为云的应答
2.2.3	组织架构（内部组织）	金融机构应有多种渠道可以联系服务供应商应对使用问题和信息安全事件。	华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由 IM 企业群、技术服务经理（TAM）、服务经理等组成的专属支持。
2.2.3	访问控制	金融机构应： （1）制定适当的身份验证方法，如在访问管理员页面时的多因素身份验证； （2）密码的分配应通过正式的管理过程加以控制； （3）基于职责分配访问权限，并根据定义	客户可通过华为云的统一身份认证服务（IAM）对使用云资源的用户账号进行管理。IAM 除了支持密码认证之外还支持多因子认证，客户可自主选择是否启用。如果租户有安全可靠的外部身份认证服务商，可以将 IAM 服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置

原文编号	控制域	具体控制要求	华为云的应答
		的访问权限控制用户对信息和应用系统功能的访问； （4）监控和检查用户的访问权限。	用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。 此外，华为云的云审计服务（CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。
2.2.3	密码管理	在管理由服务供应商提供的加密时，金融机构应收集以下信息： • 加密算法的类型； • 密钥的创建、编辑、存储、访问、撤消和销毁不应向服务供应商授予访问、存储和管理密钥的权限。	目前，华为云云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 华为云为客户提供了数据加密服务（DEW）的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW 采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，HSM 拥有 FIPS 140-2（2 级和 3 级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取客户根密钥。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。
2.2.3	物理和环境安全	金融机构应审查销毁程序，以重复使用服务供应商的设备或信息存储资源。	针对存储金融行业客户内容数据的存储介质，华为云制定了介质管理流程，确保存储在介质中的数据的安全。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循适用的法律法规，以及与客户之间的协议约定，按照数据销毁标准清除客户的数据。实现方式如下：当客户确认删除操作后，华为云首先删除客户与数据之间的索引

原文编号	控制域	具体控制要求	华为云的应答
			关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。
2.2.3	运营安全	若就备份活动由服务供应商负责，金融机构与服务供应商达成协议，金融机构应按照协议要求对服务供应商执行备份程序进行审查。 金融机构应确定记录与云计算服务相关的事件的要求，并对事件日志进行监控和存储。 金融机构应检查和评估服务供应商漏洞管理准则并安装服务供应商的补丁。	华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用对象存储服务（OBS）的版本控制、云硬盘备份（VBS）、云服务器备份（CSBS）等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保证在灾难发生时数据不丢失。 华为云的云审计服务（CTS）为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触发的操作。CTS 会对各服务发送过来的日志数据进行检视，确保数据本身不含敏感信息；在传输阶段，通过身份认证、格式校验、白名单校验以及单向接收机制等手段，确保日志信息传输和保存的准确；在保存阶段，采取多重备份，并根据华为网络安全规范要求，对数据库自身安全进行安全加固，杜绝仿冒、抵赖、篡改以及信息泄露等风险；最后，CTS 支持数据以加密的方式保存到 OBS 桶。 华为云建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。对于涉及云平台、租户服务等的漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，向最终用户/租户及时推送漏洞规避和修复方案和建议，

原文编号	控制域	具体控制要求	华为云的应答
			与租户共同面对安全漏洞带来的挑战。
2.2.3	通信安全	金融机构应评估并确定在云环境中进行网络分段和租户隔离的需求，并根据服务协议检查服务供应商的行为。	为配合客户行使对云服务供应商的监管，华为云线上的《华为云用户协议》对客户和华为的安全职责进行划分，《华为云服务等级协议》约定了华为云各项产品/服务的服务等级，包括对服务可用性的承诺，以及未达到承诺的服务补偿。 华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。客户可以使用华为云提供的虚拟私有云（VPC）服务，实现不同区域之间网络隔离。VPC 可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络 ACL 和安全组规则，对进出子网以和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。
2.2.3	系统获取、开发和维护	金融机构应对云计算应用程序进行信息安全评估，并将其作为尽职调查活动的一部分来评估和检查云服务供应商的能力。 在使用 SaaS 的情况下，金融机构应评估和检查服务供应商以建立安全的开发程序。	华为的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。为配合客户满足合规要求，华为云通过制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。
2.2.3	信息安全事件管理	金融机构应在事件管理规定中明确以下内容： • 将报告给云计算用户的事件类型； • 详细信息和事件	华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM – Security Information and

原文编号	控制域	具体控制要求	华为云的应答
		响应； • 向用户通知事件的时间范围和过程； • 联系渠道和联系人的详细信息； • 解决问题的方法。	Event Management）系统如 ArcSight、Splunk 对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有 7*24 的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。

8.4 服务跟踪和评估

原文编号	控制域	具体控制要求	华为云的应答
2.2.4	服务跟踪和评估	金融机构应明确负责跟进、评估和审查服务的角色和职责，以确保服务合同和服务质量履行以及识别使用服务的潜在风险。 金融机构应根据其与服务供应商之间的协议条款（以下简称“云服务协议”）进行监控、评估和审查服务供应商的服务。	华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT 服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。 同时，华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。 此外，华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通

原文编号	控制域	具体控制要求	华为云的应答
			过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由 IM 企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

8.5 取消或终止服务使用

原文编号	控制域	具体控制要求	华为云的应答
2.2.5	取消或终止服务使用	在取消和终止云服务的使用时，金融机构应全面制定策略和计划以适当选择退出服务，以防止或消除可能产生的不良影响的风险。例如：服务中断的风险、信息安全和存储风险等。	在服务协议终止时，客户可通过华为云提供的对象存储迁移服务（OMS）和主机迁移服务（SMS），将内容数据从华为云中迁移出去，如迁移至本地数据中心。 在客户确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。

9 结语

本文描述了华为云如何为客户提供遵从泰国金融行业监管要求的云服务，并表明华为云遵守泰国央行（BoT）、证券交易委员会办公室（OSEC）发布的重点监管要求，有助于客户详细了解华为云对于泰国金融行业监管要求方面的合规性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署遵从泰国金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对相关泰国金融行业监管要求的遵从性。

10 版本历史

日期	版本	描述
2022 年 4 月	1.1	例行刷新
2020 年 7 月	1.0	首次发布

