华为云智利金融行业监管要求遵从性指南

文档版本 1.0

发布日期 2025-05-23

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

随着技术的发展，对云计算技术及服务的使用已逐步在智利金融机构间常态化应用。云计算技术及服务为金融机构的发展带来巨大的便利的同时，也为金融机构创造了更为复杂的业务运营环境。为了规范金融行业对于信息科技的运用，智利金融监管机构针对金融机构如何进行外包管理、业务连续性、网络安全管理等方面提出了一系列监管要求和指引。

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。本文将针对智利金融机构在使用云服务时通常需遵循的监管要求，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的金融监管要求简介

金融市场委员会（Financial Market Commission，以下简称 “CMF”）是智利负责监管和管理金融市场的公共机构，旨在监督和规范银行、证券、保险和其他金融活动，以确保金融市场的正常运行、发展和稳定。CMF 通过制定和执行相关法规，确保受监管的个体或实体从成立到清算期间遵守法律、法规、章程和其他规定，同时推动金融市场的健康发展。

- 《RAN20-7 服务外包》：CMF 于 2014 年 10 月 7 日发布了《RAN20-7 服务外包》，该章节规则涉及银行机构与外部服务提供者签订合同，以开展一项或多项业务活动，这些业务活动也可以由机构利用自己的人力和技术资源在内部开展。规则就如何管理外包服务提出了要求，在任何情况下，金融机构必须始终将此类外包服务视为其一般运营风险评估和管理流程的一部分，智利金融市场委员会会对实体服务外包的风险管理进行审查。
- 《RAN20-8 运营事件信息》：CMF 于 2018 年 8 月 31 日发布了《RAN20-8 运营事件信息》，该章节规则要求金融机构在发生业务事故时必须向监管局提交的信息、在特定事件中向客户提供适当信息，以及银行有责任分享与网络安全有关的攻击信息。
- 《RAN20-9 业务连续性管理》：CMF 于 2016 年 11 月 3 日发布了《RAN20-9 业务连续性管理》，该章节规则规定了银行公司业务连续性管理的最低准则，监管局的管理

评估将考虑这些准则。该规则补充了第 10-13 章第二部分 3.2 中有关操作风险评估的内容，以及 20-7 章关于服务外包风险的规定。

- 《RAN20-10 信息安全和网络安全管理》：CMF 于 2020 年 7 月 6 日发布了《RAN20-10 信息安全和网络安全管理》，该章节包括基于良好实践的规定，这些规定应被视为各实体在信息安全和网络安全管理方面应遵循的最低准则，并补充了第 1-13 章第二章第 3.2 c 段中关于运营风险管理评价的规定、第 20-7 章关于实体在外包服务中承担的风险的规定、第 20-8 章关于运营事件报告、第 20-9 章关于业务连续性管理。该规则将是金融市场委员会在操作风险领域对银行进行管理评估的一部分。

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。

- **云计算或云**

  是指用一种模式，用于通过自助服务配置和按需管理，使网络能够访问可扩展且弹性的可共享物理或虚拟资源池（例如服务器、操作系统、网络、软件、应用程序和存储设备）。

- **服务外包**

  是指由外部供应商持续或偶尔提供的服务或活动，这些服务或活动通常可以由订约方完成。

- **分包**

  是指外包安排下的服务提供商将外包职能进一步转移给另一方的情况服务提供商。

- **外包服务链**

  由第三方组成的服务链，由上游服务提供商分包，从事与上游服务提供商签订的大部分合同活动（第三方分包）。

- **重大或战略性（关键）活动**

  i. 重大活动，在这些活动中，服务的提供或执行的任何不足或失败都会对合规性、业务连续性、信息安全（自己或客户）以及服务、产品、信息和形象的质量产生重大影响。

  ii. 任何涉及处理根据智利《银行法》受到保密或银行保密的数据的活动。

  iii. 对风险管理有重大影响的任何活动。

  iv. 与市场有高度系统互动关系的活动，或涉及承包商的重大风险的活动。

- **主站点或中心（生产）**

  集中计算资源以提供日常运营所需的技术的物理基础设施。

2 华为云安全合规

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，华为云已获得众多全球性、区域性和行业特定的安全合规的权威认证，全力保障客户部署业务的安全。

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-合规中心”

华为云部分标准类认证/鉴证示例：

认证	描述
ISO27001	ISO27001 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。
ISO27017	ISO27017 是针对云计算信息安全的国际认证。ISO27017 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。
ISO27018	ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 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。
TL 9000& ISO 9001	ISO 9001 是 ISO 9000 族标准所包括的一组质量管理体系核心标准之一，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。 TL 9000 是一个建立在 ISO9001 基础上的，由全球电信业优质供应商联盟（QuEST Forum）针对全球信息和通讯技术（ICT）行业特定设计的、为 ICT 产品和服务供方提供的一套通用的质量管理体系要求。它包括了 ISO9001 的所有要求，ISO9001 将来的任何改动也会导致 TL9000 的改动。 华为云取得了 ISO9001 / TL9000 认证证书，表明华为云可以为您提供更快，更好和更具成本效益的服务。
ISO20000-1	ISO20000 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。
ISO22301	ISO22301 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。
CSA STAR 认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 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。
ISO27701	ISO27701 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	BS10012 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。
ISO 29151	ISO29151 是国际个人身份信息保护实践指南。ISO29151 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。
PCI DSS	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。
PCI 3DS	PCI 3DS 标准，旨在保护执行特定 3DS 功能或者存储 3DS 数据的 3DS 环境，支持 3DS 的实施。PCI 3DS 的评估对象为 3D 协议执行环境，包括访问控制服务器、目录服务器或 3DS 服务器功能；以及 3D 执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估 3D 协议执行环境的过程、流程、人员管理等。
ISO 27799	ISO/IEC 27799 是专注于医疗行业的信息安全管理体系，为医疗行业和其相关机构提供了关于如何更好地保护个人健康信息的保密性、完整性、可审计性和可用性的指导。 华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。
ISO 27034	ISO/IEC 27034 是国际标准化组织 ISO 通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得 ISO/IEC 27034 认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。
SOC 审计报告	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。

3 华为云责任共担模型

客户在云上业务的安全性与合规性是华为云与客户的共同责任。与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。也正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与客户共同努力。

云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如下图所示，客户可以基于自身的业务需求选择不同的云服务类别（例如 IaaS、PaaS、SaaS 服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

在隐私保护要求可能适用于客户内容的情况下，“责任共担”模型帮助华为云和客户双方理解各自角色以及责任。

图3-1 华为云责任共担模型

华为云的责任：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在 PaaS、SaaS 场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。

客户的责任：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

在 On-prem 场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。

在 IaaS 场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。

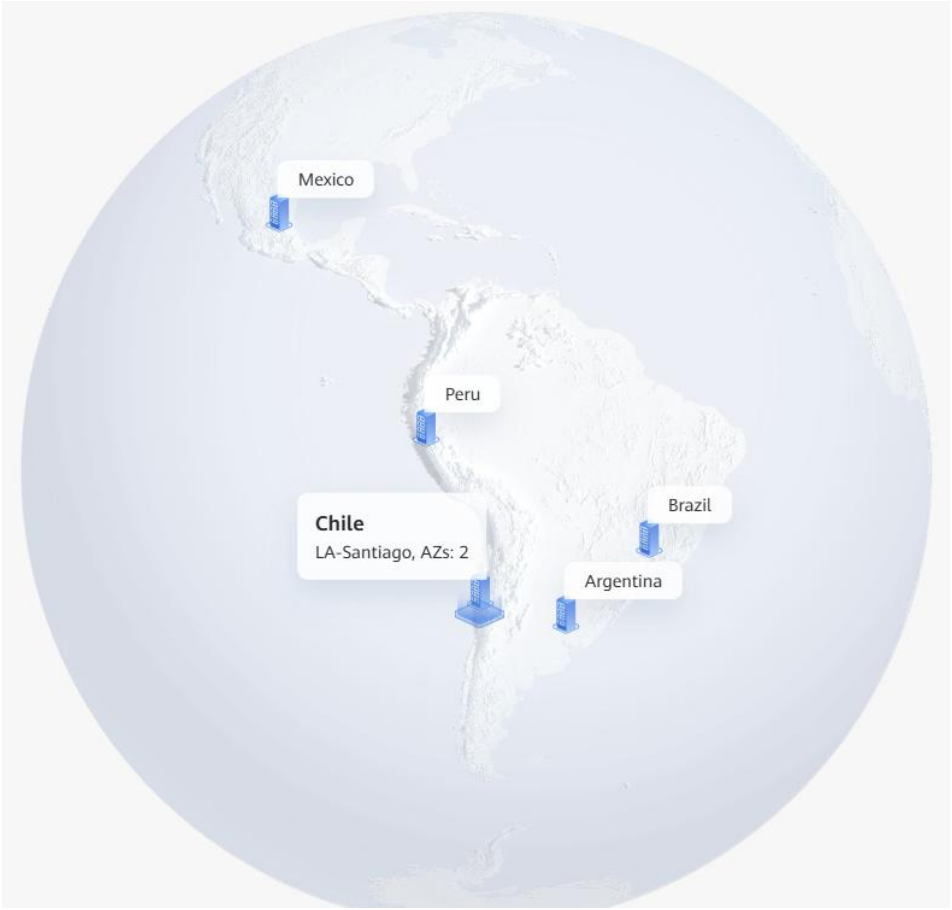
在 PaaS 场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。

在 SaaS 场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

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。在智利，华为云已部署“LA-Santiago” Region，拥有多个可用区（AZ）。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。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”。

图4-1 智利 Region 和可用区（AZ）示例



5 华为云如何遵从及协助客户满足 CMF《RAN20-7 服务外包》

CMF 于 2014 年 10 月 7 日发布了《RAN20-7 服务外包》，该规则涉及银行机构与外部服务提供者签订合同，以开展一项或多项业务活动，这些业务活动也可以由机构利用自己的人力和技术资源在内部开展。规则就如何管理外包服务提出了要求，在任何情况下，金融机构必须始终将此类外包服务视为其一般运营风险评估和管理流程的一部分，智利金融市场委员会会对实体服务外包的风险管理进行审查。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

5.1 服务外包时必须遵守的条件

编号	具体控制要求	客户关注点	华为云的内部实践
III. 服务外包应满足的条件 1. 一般条件	d) 建立供应商选择、聘用和监控的正式程序。 h) 确保对供应商选择、招聘和跟进过程进行独立审计，并配备专门负责各种风险审计的工作人员。 i) 确保供应商根据其结构和组织规模定期对其服务进行内部审计报告或独立审查，并及时与机构分享相关发现。 j) 要求服务提供者确保与合同服务相关的业务、行政和技术程序得到适当记录、更新并永久提供给委员会审查。 l) 该实体必须在其为董事会或代替其行事的人准备的运营风险报告中包括有关该机构对外包风险的管理的信息，包括供应商风险状况的变化，以及被认为是关键服务的风险。	客户应该建立外包管理机制，持续监控并定期审查外包服务。	华为云已通过 ISO27001、ISO27017、ISO27018、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，华为云将积极配合金融机构满足监管机构相关的要求。 ●安全管理：华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立完善的信息安全管理体系、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。 ●合规审计：华为云已获得 SOC 1 Type II，SOC 2 Type II 和 SOC 3 鉴证审计报告，其中 SOC 2 五大控制属性（安全性、可用性 、进程完整性、保密性、隐私性）审计全部通

附件1：服务外包所要考虑的最低限度方面 2. 服务提供商选择	机构必须根据其要求评估收到的建议书，并进行尽职调查，以证实从潜在供应商处收到的信息。	在开展外包活动前，客户应对服务提供商开展尽职调查，了解其专业能力、财务、供应商管理、业绩情况、合规情况以及信息安全管理等情况。	过，且每年例行邀请第三方机构进行两期 SOC 审计并输出报告,以方便客户及时了解华为云的内部控制水平。如有必要，客户可以通过官方渠道向华为云申请获取审计报告的副本。 ●监控与服务支持：在客户开展外包活动前，华为云配合客户对服务提供商的尽职调查。华为云参与客户外包活动后，为满足客户对云外包管理的要求，华为云对外提供了统一的电话热线、邮箱地址以及工单系统处理客户的服务请求。同时，华为云向客户提供云监控服务，供客户监控自身云资源的使用情况，并且可以根据客户的需求按照 SLA 提供定制化服务报告，但此服务可能会涉及费用。 ●分包商管理：华为云制定了自身的供应商管理机制，从供应商的产品和供应商本身的内部管理都提出了安全需求。此外，华为云会对供应商进行定期的稽核，对有风险的供应商会到现场进行审核。此外会与涉及网络安全的供应商签署网络安全协议，在服务过程中也会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应商进行合作降级处理。
III. 服务外包应满足的条件 1. 一般条件	m）外包服务中要使用的数据、技术平台和应用程序必须位于特定的处理地点，如果是在国外处理，则必须位于一个确定的和已知的司法管辖区。除了辖区，您还应该了解数据中心运营的城市。	客户应对外包供应商数据中心运营的城市进行了解与要求。	华为云在智利的实体 Sparkoo Technologies Chile SpA，是一家根据智利法律注册的公司，并在智利圣地亚哥部署本地数据中心，拥有多个可用区，可支持客户高可用、低时延的服务部署，以及数据本地化存储和容灾备份。 另外，华为云在全球布局多个数据中心，部署多个地理区域（Region）和多可用区（AZ），客户可以通过华为云官网“全球基础设施”，查看华为云全球基础设施的具体站点和产品部署分布。客户可以根据需求自主选择华为云的区域购买服务并进行业务部署。未经客户同意，华为云不会将客户的内容数据从所选服务器区域迁出。
III. 服务外包应满	g）建立程序，以确保及时、充分地履行对客户的承诺。 k）考虑外包服务链产生的风险，这些风险应事先反映在各	客户应在与服务提供商的书面外包合同中规定各自的权利和义务，并包括合同服务	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

足的条件 1. 一般条件	自的合同中，注意在分包的情况下，分包的企业还必须符合实体与原服务提供者之间约定的条件。分包公司对实体外包服务的责任和义务也应在各自的合同中明确说明。	水平协议、业务连续性和信息安全条款、否决权条款、终止条款等。	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。 金融机构对华为云的审计和监督权益会根据实际情况在与金融机构签订的协议中进行承诺。华为云会遵从与金融机构签订的协议中约定的要求，并会安排专人积极配合金融机构和金融交易实体监管/监管指定的代理人对华为云的审计和监督。 华为云的云服务和平台已获得ISO27001、ISO27017、ISO27018、SOC、CSA STAR 等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。并每年接受第三方审计。并提供专人协助，积极响应及配合客户方发起的审计活动。如有必要，客户可以通过官方渠道向华为云申请获取证书以及审计报告的副本。
附 件 1：服务外包所要考虑的最低限度方面 3. 合同	实体应确保合同明确界定双方的权利和义务，包括明确和可衡量的合同服务水平的协议、合同关系的提前终止条款，以及适合具体合同的定价方法。 如果以单一价格购买多项服务，则必须包含每项服务的收费详细信息。 还应包括业务连续性和信息安全条款，特别是关于您和您的客户信息的所有权和保密性；限制使用软件；在适用时安全删除客户数据；此外，还应建立一个永久授权，允许委员会和被审计实体在现场或远程根据需要随时检查合同服务的所有方面。 此外，机构在主供应商选择第三方分包时，还必须考虑否决权条款。 在合同中，必须明确说明与提供服务的公司人员的适合性和责任有关的所有事项，以及适用于此类合同的国内或国外的所有法律和劳动方面。		
III. 服务外包应满足的条件 1. 一般条件	c）验证供应商是否有机制防止其他客户执行的操作对实体外包的服务产生负面影响。	客户应确保服务提供商采取了适当的技术和组织措施来保护资产的安全性。	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。

III. 服务外包应满足的条件 3. 业务连续性	实体应验证其关键服务提供商是否有适当的计划以确保合同服务的连续性。此外，该实体必须验证其关键供应商是否确保其分包的服务具有适当的业务连续性计划。此类计划必须至少每年测试一次，包括（如果适用）不同处理地点的灾难情景。实体必须了解此类活动并验证所获得的结果。此外，该实体还必须有经过验证的计划，以确保在此类外部服务不可用的情况下的运营连续性。	客户应制定业务连续性计划，并定期测试和更新计划。	如果客户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。 华为云取得了 ISO/IEC 22301 国际业务连续性管理体系认证证书，证明华为云具备连续稳定的服务能力，可以持续为客户提供成熟和高质量的产品与服务。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，以保障华为云服务的业务连续性能力一直处于业界领先水平。
III. 服务外包应满足的条件 3. 业务连续性	该实体必须在此类供应商违约的情况下制定退出计划，考虑提前终止合同关系，并允许以自己的方式或通过其他供应商恢复运营。 该机构必须确保供应商对可能中断或影响提供产品、服务或活动的事件有一个正式和系统的管理流程。	客户应在在签订外包协议中明确相关退出计划的规定。	华为云线上的《华为云用户协议》对客户和华为云的安全职责进行划分，华为云《华为云服务等级协议》规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中与客户共同约定相应退出要求。华为云在一定程度上会遵从客户的合同流程。
III. 服务外包应满足的条件 4. 在适当情况下，保护自己和客户的信息安全	实体必须确保服务提供商维护信息安全计划，以确保其及其客户信息资产的机密性、完整性、可追溯性和可用性。这些条件必须与实体采用的政策和标准一致，并纳入服务合同中。	客户应确保服务提供商采取了适当的技术和组织措施来保护数据全生命周期的机密性、完整性和可用性，并通过合同、协议明确。	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。华为云遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。华为云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，并严格遵守各国数据保护相关规定。同时，在与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。

III. 服务外包应满足的条件 4. 在适当情况下，保护自己和客户的信息安全	实体必须控制和监控提供商提供的信息安全基础设施，以保护外包关键服务中存在的信息资产，而不管提供商提供的控制措施如何。同样，它必须控制和监控与此类关键服务相关的信息的身份管理和访问控制。 采购实体和服务提供商之间的通信连接必须具有确保端到端的数据机密性和完整性的加密级别。 实体必须确保供应商对导致所购买服务不可用的外部攻击（如拒绝服务）有有效的控制和保护措施。此外，对于外包关键服务，实体必须检查供应商是否定期对其技术基础设施进行脆弱性评估和渗透测试。 信息一旦处理就必须以加密形式存储和传输，解密密钥将由实体保管。此外，还应定义服务提供商和机构之间的密钥交换程序，并定义参与安全管理的人员的角色和职责。 在实体文件处理的情况下，实体应具有控制程序，以确保本标题所述的条件得到适当遵守。除上述规定外，还必须建立程序，以确保供应商向该实体适当地传递信息，并且在合同关系结束后，供应商不保留其持有的任何信息。	客户应在云外包书面协议中设定信息安全要求，并持续监控对这些要求的遵守情况。	华为云会识别相关的监管要求，遵守其外包规则和规定： a.信息安全组织：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。 b.身份和访问管理： 华为云绝不允许运维运营人员在未经授权的情况下访问客户的系统和数据。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，如 USBkey、SmartCard 等。华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。在客户授权访问系统的情况下，华为云通过严格的安全运维规范和流程，确保远程运维中的安全。针对运维场景，华为云通过在数据中心部署的 VPN 和堡垒机实现运维管理平台的统一运维管理和审计。数据中心外网运维人员和内网运维人员对网络、服务器等设备的本地及远程操作全部集中管理，实现用户对设备资源操作管理的统一接入、统一认证、统一授权、统一审计。 c.加密和密钥管理：华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。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。 d.业务连续性和灾难恢复：华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。 e.数据位置：华为云目前已陆续在全

			球多个国家或地区提供云服务，其基础设施部署在全球多个地理区域（Region）和多个可用区（AZ）。通过该部署模式，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和存储实例资源。每个可用区都是一个独立故障维护域，即各可用区在物理上是隔离的，用户可充分利用这些地理区域和可用区规划、部署和运行云上应用系统。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应用系统都能持续运行。关于更多华为云基础设施信息，参见华为云官网“全球基础设施”。华为云以区域（Region）为单位向客户提供服务。区域即客户内容数据的存储位置，华为云绝不会在未经用户授权的情况下，跨区域移动客户的内容数据。客户在使用云服务时，建议根据就近接入原则并遵从不同地域的法律法规要求选择区域，确保其内容数据存储在目标位置。对于区域服务，客户可以在购买服务初期按需选择区域，其服务部署位置及数据留存地可以通过华为云门户进行变更。 f.合规与监控：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。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。 g. 安全演练与渗透测试：华为云定期会开展内部网络安全实战演练（如红蓝对抗）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。 h. 网络边界防护：华为云建立了稳固、完善的边界和多层立体的安全防护系统，部署了 Anti-DDoS、IDS/IPS、WAF 等防护机制。Anti-DDoS 快速发现和防护 DDoS 攻击，实时对流量型攻击和应用层攻击进行全面防护；WAF 实时检测和防御 Web 攻

			击，对高危攻击进行告警并立刻自动阻断；IDS/IPS 实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。
III. 服务外包应满足的条件 5. 国家危险	服务只能外包给具有投资级国家风险评级的司法管辖区。但是，董事会或代替其行事的机构可以放弃这一要求，前提是服务外包所在的国家有充分的法律保护和个人数据的安全，并且必须记录为此进行的分析。上述规定不应妨碍本章第三编第 2 款（i）项和第四编第 1 款（b）项的规定。	客户应确保外包服务供应商来自有投资级国家风险评级的司法管辖区，或供应商所在的国家有充分的法律保护和个人数据的安全。	华为云在智利的实体 Sparkoo Technologies Chile SpA，是一家根据智利法律注册的公司，将积极配合金融机构满足监管机构相关的要求。
III. 服务外包应满足的条件 7. 主管访问信息	采购实体应确保委员会能够通过访问服务提供者的场所或远程获取通过外部提供者处理、维护和生成的所有记录、数据和信息，无论该外部提供者是在本国还是国外设立的。 作为在国外设立的服务提供者，应特别注意东道国的任何法律限制，这些限制可能阻止委员会访问提供者或获取上款所述的信息和数据。	客户应该建立外包管理机制，保证在合同期内可持续监控并审查外包服务。	华为云已通过 ISO27001、ISO27017、ISO27018、CSASTAR 等多项国际安全与隐私保护认证，并且每年例行邀请第三方机构进行两期 SOC 审计并输出报告,以方便客户及时了解华为云的内部控制水平。如有必要，客户可以通过官方渠道向华为云申请获取审计报告的副本。。此外，华为云将积极配合金融机构满足监管机构相关的要求。
附件 1：服务外包所要考虑的最低限度方面 4. 永久监视	供应商：机构必须在合同期内监控供应商的表现和机构要求的可能变化。控制应至少包括：对供应商最新财务状况的了解和分析，以及对外部公司整体控制环境的观察等方面。 服务：机构必须有程序来监督合同条款的遵守情况。监控必须至少包括：服务水平协议、合同条款、与合同服务相关的运营风险的管理，以及由于外部环境可能发生的变化。		

5.2 数据处理服务外包时需要考虑的因素

编号	具体控制要求	客户关注点	华为云的内部实践

IV. 数据处理服务外包时需要考虑的因素 1. 供应商的地理位置	a）国内服务 当数据处理服务全部或部分由位于该国的公司提供时，该机构应验证用于数据通信、存储和处理的技术基础设施和系统是否提供足够的安全性，以永久性地保障业务连续性、机密性、完整性、准确性和信息质量。应急数据处理中心必须符合与主数据处理中心的位置和距离条件，以确保业务连续性。 b）在国外提供的服务 如果实体将数据处理服务外包到境外，则必须始终具有签约公司的背景。特别是，它必须保持一个记录，以支持服务提供商的财务稳健性，并且服务提供商保持质量认证、安全认证和适当的控制系统。此外，实体必须有项目的背景，服务合同，如果与第三方有分包合同，也必须合并。 为确保金融市场的所有参与者（包括客户、在国外开展重大或战略性活动的机构）能够正常运作，并遵守服务外包的下列条件： i）必须在智利设立一个应急数据处理中心，并且必须证明与外包服务的重要性相适应的恢复时间。此外，对于事务性和批处理流程，实体必须至少每年评估一次恢复时间。	1. 客户应确保国内外包供应商的应急数据处理中心满足与主数据处理中心的位置和距离要求，以确保业务连续性。 2. 客户应确保与国外外包供应商签订服务合同，记录服务提供商财务状况、服务质量及安全性，并确保其在智利拥有应急数据处理中心，并定期评估恢复情况，确保业务连续性。	1. 华为云在智利的实体 Sparkoo Technologies Chile SpA，是一家根据智利法律注册的公司，并在智利部署本地数据中心，拥有多个可用区，可支持客户高可用、低时延的服务部署，以及数据本地化存储和容灾备份 2. 作为云服务提供商： （1）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，建立了一套完善的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。 （2）华为云根据内部业务连续性管理体系的要求，定期开展风险评估，识别并分析支撑云服务持续运行的关键资源所面临的潜在风险。针对突出风险，进一步考虑突发事件发生的场景，并制定应对各种突发事件场景的危机管理程序，以最大程度地降低突发事件的影响。危机管理程序中详细规定了突发事件的预警和报告流程、事件升级流程、应急预案启动的条件、事件进展的通报流程、内外部沟通流程等。

6 华为云如何遵从及协助客户满足 CMF《RAN20-8 运营事件信息》

CMF 于 2018 年 8 月 31 日发布了《RAN20-8 运营事件信息》，该章节规则要求金融机构在发生业务事故时必须向监管局提交的信息、在特定事件中向客户提供适当信息，以及银行有责任分享与网络安全有关的攻击信息。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

编号	具体控制要求	客户关注点	华为云内部实践
1.运营事件的通报	各金融机构必须具有识别、记录、评估、控制、缓解、监测和报告运营事件的系统、程序和管理机制，特别是与网络安全相关的事件。 金融机构应向 CMF 报告影响或危害业务连续性、机构或其客户的资金或资源、服务质量或机构形象的运营事件，包括报告关键供应商的服务故障。 1.1 通知 CMF 运营事件信息必须在发生后最多 30 分钟内，发送。 1.2 通知客户或用户 如果发生影响向客户提供服务的质量或连续性的事件，或者是已知的事件，金融机构应及时通知客户或用户此类事件的发生。	一旦意识到发生了重大事件后，客户应立即通知监管机构，并向其提供当时可获得的任何信息。监管机构可能要求有关金融机构提供进一步的信息或更新。	为配合客户满足通知的要求，华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：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。根据内部的客户通知通报流程，在底层基础平台发生严重事件，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。

7 华为云如何遵从及协助客户满足 CMF《RAN20-9 业务连续性管理》

CMF 于 2016 年 11 月 3 日发布了《RAN20-9 业务连续性管理》，该章节规则规定了银行公司业务连续性管理的最低准则，监管局的管理评估将考虑这些准则。该规则补充了第 10-13 章第二部分 3.2 中有关操作风险评估的内容，以及 20-7 章关于服务外包风险的规定。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

7.1 一般管理要素

编号	具体控制要求	客户关注点	华为云的内部实践
I. 一般管理要素	-董事会提供了一个机制，使董事会能够定期和适当地了解该实体所面临的业务连续性管理问题。该实体维护董事会批准的政策，用于业务连续性管理，与业务量和其操作的复杂性。这些政策传达给所有人并至少每年进行一次审查。 -该机构对业务连续性管理流程进行了内部审计，这些审计在覆盖面和范围上都是充分和充分的。 -该实体有记录在案的运营和灾难恢复应急计划，以应对灾害风险的发生定义的应急方案，至少每年更新一次。这包括在突发事件结束后恢复和恢复正常业务活动的程序	客户应考虑定期对业务连续性计划进行维护和审查，以确保其响应和恢复安排的可靠性，并使其能够在中断后及时继续提供关键业务服务。	作为云服务提供商，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。 灾难恢复测试： 华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。

I. 一般管理要素	-在推出新产品、开展新活动或建立新的流程和系统之前，企业必须确保对可能存在的业务连续性风险进行评估。 -有关实体要产生足够、充分和及时了解与此事相关的风险，这些风险是必要时向决策者报告。	客户应建立业务影响分析和风险评估机制。	作为云服务提供商： （1）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，建立了一套完善的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。 （2）华为云根据内部业务连续性管理体系的要求，定期开展风险评估，识别并分析支撑云服务持续运行的关键资源所面临的潜在风险。针对突出风险，进一步考虑突发事件发生的场景，并制定应对各种突发事件场景的危机管理程序，以最大程度地降低突发事件的影响。危机管理程序中详细规定了突发事件的预警和报告流程、事件升级流程、应急预案启动的条件、事件进展的通报流程、内外部沟通流程等。
I. 一般管理要素	-公司拥有董事会批准的业务连续性管理策略，该策略与业务需求和所承诺的服务质量相一致。 -该机构开发了一套正式的业务影响评估方法（BIA），该方法考虑了业务领域定义的目标恢复时间（RTO），以确定最关键的流程。此外，它还分析了业务连续性风险（RIA），以降低风险发生的可能性。这些分析至少每年进行一次。 -实体至少考虑应急方案与技术系统的全部或部分缺失有关的；关键人员；无法进入和/或使用实体设施；以及未能提供合同约定的服务供应商。此外，根据自身的风险状况，实体考虑其他可能影响其的意外情况，如数据完整性故障、服务中断等影响网络安全的攻击。 -该机构有一套正式、系统的事件处理流程，用于处理可能中断或影响供应的事件产品、服务或活动。	1. 客户应考虑针对业务影响分析和风险评估的结果制定恢复策略。 2. 客户应制定业务连续性计划灾难恢复计划，制定保证其关键业务连续的 RTO、RPO 指标，并每年进行测试。客户应建立异地灾备中心，保障业务连续性。	如果客户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。 华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定业务连续性计划，并每年对其进行测试，该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。 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。华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联，满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。
I. 一般管理要素	-该实体至少每年进行一次测试，测试运营和灾难恢复应急计划，以支持所有场景中的关键流程，以确保其充分性和有效性。根据确定的测试类型进行练习，在任何情况下，都要不断提高到更复杂的测试，例如桌面测试、模拟测试、关键活动测试等。这些测试的结果将反映在一份报告中，该报告可以清楚地说明测试的范围、条件和纠正计划（如果适用的话）。 -该实体至少每年对灾难恢复计划（DRP）进行一次测试，以模拟灾难恢复计划的不同的处理位置，包括在事务处理执行期间和批处理执行期间。 -组织有培训和辅导计划，使各级员工都能够理解和理解该组织的工作维护业务连续性模型的责任。 -该实体确保有足够的工作人员和处理突发情况所需的专业知识由实体定义。	客户应建立业务连续性计划的测试和培训机制。	华为云作为云服务提供商，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在不足之处，将对相关文件进行更新。
I. 一般管理要素	-该机构有一个应急沟通计划，覆盖所有利益相关方，包括内部或外部。	客户应与内外部利益相关方建立沟通机制。	作为云服务提供商： （1）华为云会积极配合金融客户主动发起的沟通。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、热线电话等联络到华为云的支持团队。 （2）华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。 （3）为配合客户满足通知的要求，华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生

			影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：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。根据内部的客户通知通报流程，在底层基础平台发生严重事件，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。

7.2 技术基础设施

编号	具体控制要求	客户关注点	华为云的内部实践
II. 技术基础设施	加强运营韧性的重要方面之一的实体是数据处理站点的维护和强大的技术基础设施，这应该是评估的结果定期对他们进行专门化。在这方面，妥善管理与这体现在以下事实中： -数据处理中心，主中心或应急中心在基础设施方面不断更新技术和软件版本，最好在双活模式。 -数据处理站点已通过认证可建造性术语和由专业和独立的。 -数据处理站点的基础设施具有并行维护能力，可用性至少为 99.98%或每年 1.6 小时的停机时间。 -站点配置允许电信和冗余计算机设备避免单点故障所必需的；布线连接；在其路径中的不同分布；以及由专家管理，以提供支持 24x7 全天候工作。 -主要和应急地点位于不同的地点以不暴露在相同风险中的方式，除其他因素外，考虑到设施。 -实体具有支持性基础设施和程序，允许恢复数据、基础软件和应用程序，根据在发生突发事件或信息损坏时定义的 RTO。	1. 客户应设置数据主中心和数据应急中心，通过对数据中心的安全资质、运维能力、恢复能力等方面要求，确保数据极其备份的安全性。 2. 客户应制定灾难恢复计划，制定保证其关键业务连续的 RTO、RPO 指标，并每年进行测试。客户应建立异地灾备中心，保障业务连续性。	1. 华为云在智利的实体 Sparkoo Technologies Chile SpA，是一家根据智利法律注册的公司，并在智利部署本地数据中心，拥有多个可用区，可支持客户高可用、低时延的服务部署，以及数据本地化存储和容灾备份。 2. 如果客户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。 华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定业务连续性计划，并每年对其进行测试，该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。 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。华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联，满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。

8 华为云如何遵从及协助客户满足 CMF《RAN20-10 信息安全和网络安全管理》

CMF 于 2020 年 7 月 6 日发布了《RAN20-10 信息安全和网络安全管理》，该章节包括基于良好实践的规定，这些规定应被视为各实体在信息安全和网络安全管理方面应遵循的最低准则，并补充了第 1-13 章第二章第 3.2 c 段中关于运营风险管理评价的规定，第 20-7 章关于实体在外包服务中承担的风险的规定，第 20-8 章关于运营事件报告，第 20-9 章关于业务连续性管理。该规则将是金融市场委员会在操作风险领域对银行进行管理评估的一部分。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

8.1 一般管理要素

编号	具体控制要求	客户关注点	华为云的内部实践

2. 一般管理要素	以下方面将被视为适当管理制度的必要要素： - 董事会已批准管理信息安全和网络安全风险的政策，这些政策至少定义了实体针对这些事项的范围和目标，以及每项事项的具体风险容忍度；要持有的信息资产的明确定义；信息的分类标准；以及与实体的流程图一致的持续更新的信息资产清单。这些政策应在组织内广泛传播，组织应至少每年审查和批准一次。 - 董事会通过了内部行为政策，以便所有为实体提供服务的员工和/或外部人员负责任地使用提供给他们的信息和通信技术。 - 实体的信息资产在物理和环境安全方面得到充分保护，例如保护数据中心所在的敏感业务、运营和技术领域。 - 作为其外包关键服务管理的一部分，该实体实施了对其信息安全和网络安全政策的实施和合规性的定期验证流程，以确保第三方供应商使用或管理的信息资产得到适当保护。它还持续监控与第三方供应商连接的基础设施，并分析和实施措施，以检测和缓解实体网络安全的潜在威胁。 - 该实体确保及时评估在引入新产品、新系统、开展新活动和/或定义新流程时可能承担的信息安全和网络安全风险。 - 该实体管理其信息安全和网络安全警报或威胁和事件，以检测、调查和减轻这些事件的影响，并保护其信息资产的机密性、可用性和完整性。 - 该实体对信息安全和网络安全管理流程进行审计，审计的深度和范围应足够大，并考虑政策的合规性以及这些事项中定义的程序和控制的有效性等方面。	客户应制定信息安全政策，包含信息安全的总体责任、相关方应遵守的基本的信息安全要求以及信息安全领域的安全流程等。	根据 ISO 27001 标准，华为云构建了完善的信息安全管理体系，制定了华为云的整体信息安全战略，明确了信息安全管理机构的结构和职责、信息安全系统文件的管理方法、关键方向和目标，包括资产安全、访问控制、密码学、物理安全、运营安全、通信安全、系统开发安全、供应商管理、信息安全事件管理和业务连续性。 网络安全政策和程序发布前需得到管理者审批，员工可根据授权查看已发布的信息安全政策和程序。

8.2 信息安全和网络安全风险管理流程

编号	具体控制要求	客户关注点	华为云的内部实践

3. 信息安全和网络安全风险管理流程	- 根据信息安全和网络安全政策中包含的定义和范围识别您的资产。在识别和描述资产特征时使用的详细程度应足以适当管理相关风险，特别是考虑其实际位置和功能。	客户应对资产进行管理，并实施资产的配置管理。	作为云服务提供商： 1.华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享，确保资产按照其对组织的重要程度受到适当水平的保护。华为云通过 CAM 资产管理系统实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。 2.华为云每年会对建立的资产处置流程与要求进行审阅和更新，同时华为云网络安全与隐私团队定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。3.通过制定办公场所及办公计算机等设备的信息安全管理规定，华为云规范和维护安全的办公环境，并通过在终端设备上统一部署和管理防病毒软件和数据防泄漏（DLP）软件，保护信息资产和数据安全。
3. 信息安全和网络安全风险管理流程	- 识别可能损坏信息资产的威胁及其相对于已知威胁和现有控制的漏洞。通过从内部和外部不同来源获得的信息，可以加强对威胁和漏洞的识别。	客户应建立有效的补丁和漏洞管理机制，对所有技术资产进行漏洞识别和风险评估，对关键补丁进行测试，制定补丁更新周期以及补丁修复的工作流程。	作为云服务提供商： 1.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。 2.华为云安全运营中心（SOC）已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，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，降低对用户业务造成影响的风险。同时，华为 PSIRT 和华为云 SOC 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，使基础设施、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用户业务的风险。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用户业务造成影响。 3.此外，华为云会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为云相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。

3. 信息安全和网络安全风险管理流程	- 该实体执行风险分析过程，该过程考虑评估事件发生的可能性及其对信息资产的后果或影响等要素，以信息安全和网络安全事件造成的损害程度或成本为基础，从而确定风险级别。 - 实体执行风险评估流程，将风险评估流程理解为将先前确定的风险水平与先前定义的估值和容忍标准进行比较的活动。 - 对现有控制措施进行评估，以确定其有效性和充分性。 - 实体制定风险管理计划，风险管理计划被理解为在估值阶段确定优先级的风险允许建立控制以减少、接受、避免或转移风险的活动。 - 实体遵循一个正式的流程，以确保所产生的风险与定义的风险承受能力一致。 - 实体通过一个正式的流程向组织传达风险。 - 该实体至少每年审查一次其信息安全和网络安全风险管理流程，以便及时确定对所使用的方法和/或工具进行调整的必要性。	1. 客户应建立有效的风险管理框架，制定适当的网络风险管理措施。 2. 客户应定期开展风险评估，识别其 IT 环境的威胁，分析风险造成的影响。客户应对其外包业务的服务提供商进行风险评估，以识别潜在风险。 3. 客户应定期对网络安全的风险处置计划的实施情况进行跟踪监测。	华为云制定了信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。华为云至少每年进行一次正式风险评估，并制定了风险计算和分类的流程，以确定已识别风险的可能性和影响。此外，华为云至少每月组织一次会议，讨论网络安全和隐私保护风险评估。华为云采取并记录相应的后续行动，以确保风险按照华为风险管理要求得到适当管理。 风险评估涵盖信息安全的各方面，包括数据保护和分类、数据留存和传输位置、数据保存时间对法律法规的符合等。同时，华为云根据制定的风险计算和分类的流程，确定已识别风险的可能性和影响。每种风险相关的可能性和影响是独立确定的，应考虑每种风险类别。根据风险标准，将风险降低到可接受的水平包括解决时间，都应该由管理层制定、记录和批准。风险评估的目的是识别华为云的威胁和漏洞，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。风险评估报告完成后由高级管理层进行审批。

8.3 网络安全管理需要考虑的特殊要素

编号	具体控制要求	客户关注点	华为云的内部实践
4.1 保护关键网络安全资产，	- 机构维护从机密性、完整性和可用性角度分类的关键网络安全资产的清单。 - 确定机密性、完整性和可用性的损失对信息资产的影响。	客户应对资产进行管理，并实施资产的配置管理。	1.华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享，确保资产按照其对组织的重要程度受到适当水平的保

检测威胁和漏洞	- 实体拥有足够的工具来控制、记录和监控用户对关键资产以及拥有特殊特权的用户的活动。		护。华为云通过CAM资产管理系统实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。 2.华为云每年会对建立的资产处置流程与要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 该实体具有变更管理流程，确保以安全和受控的方式对信息技术（IT）基础设施进行变更，并控制和监控所做的变更。	客户应建立变更管理程序，根据信息资产的重要性，对变更进行识别、分类和优先级排序。	华为云制定了变更管理程序，管理应用变更和基础设施变更。华为云，定义了涵盖变更实施前、实施中及实施后应遵循的网络安全要求，以防止未授权变更。例如，变更前，各项变更均需通过多个环节的审核；变更实施中，会通过日志记录、操作监控及双人操作等方式确保变更安全实施，并确保变更过程可追溯；变更后，对变更实施专人验证，确保变更达到预期效果，不会造成网络安全风险。 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，都需通过类生产坏境测试、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。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 该实体具有适当的容量管理流程，使其能够确保 IT 基础设施满足当前和未来的需求，同时考虑到该实体运营的数量和复杂性。	客户应建立正式的容量管理程序，对其 IT 基础设施进行监控，确保资源能够满足业务增长的需要。	客户应考虑通过正式的程序来管理系统容量。为配合客户遵从监管要求，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，客户可通过华为云的云监控服务（Cloud Eye Service， 简称CES）对弹性云服务器、带宽等资源进行立体化监控，精准掌握业务资源状态。
4.1 保护关键网络安全资	- 该实体拥有一个技术过时管理流程，使其能够维护一个 IT 基础设施，其安全性能标准适合该实体的目标和需求。 - 该实体具有配置管理流	客户应监控和验证配置设置，并在检测到偏离基线配置时采取改进措施。	客户应就其云环境制定适当的安全配置基线。华为云在官网信任中心提供《华为云安全配置基线指南》，供客户参考。客户可通过华为云的配置审计（Config）服务配置合规规则来对资源进行合规性检查，保障云上资源配置变更符合预期。

产，检测威胁和漏洞	程，以确保对 IT 基础设施的可配置元素进行适当控制，并控制和监控对这些元素的访问。		客户可使用华为云的企业主机安全服务（Host Security Service， 简称 HSS）对主机进行基线检查，包括检测系统弱口令、风险账号，以及常用系统与中间件的配置，以识别不安全项目，预防安全风险。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 该实体已实施补丁管理程序，以确保及时将补丁应用于软件和固件。	客户应建立有效的补丁和漏洞管理机制，对所有技术资产进行漏洞识别和风险评估，对关键补丁进行测试，制定补丁更新周期以及补丁修复的工作流程。	作为云服务提供商： （1）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。 （2）华为云安全运营中心（SOC）已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，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，降低对用户业务造成影响的风险。同时，华为 PSIRT 和华为云 SOC 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，使基础设施、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用户业务的风险。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用户业务造成影响。 （3）此外，华为云会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为云相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。
4.1 保护关键网络安全资产，检测威胁和漏洞	-通过实施补充工具（例如防火墙、Web 应用程序防火墙(WAF)、入侵防御系统（IPS）、数据丢失防护系统（DLP）、服务拒绝系统、电子邮件过滤、防病毒和防恶意软件），充分保护计算机网络免受来自 Internet 或其他外部网络的攻击。	客户应实施实时监控程序和工具，以检测威胁，异常表现或可能表明潜在网络风险的事件。	客户应采取网络安全监控措施以侦测恶意活动，并对计算机和网络系统的访问和操作记录进行保存和审计。为配合客户满足监管要求： （1）华为云建立了稳固、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离； Anti-DDoS 快速发现和防护 DDoS 攻击；WAF 实时检测和防御 Web 攻击；IDS/IPS 实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。针对公有云攻击的手段多样、流量巨大的特点，华为云使用分析系统，关联各种安全设备的告警日志，安全云脑（SecMaster）并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威

			胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，包括最常见的云攻击威胁：暴力破解、端口扫描、肉鸡（被黑客远程控制的机器）、Web 攻击、Web 未授权访问、APT 攻击等。并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。 （2）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，以助力支撑网络安全事件回溯。该日志分析系统有强大的数据保存及查询能力。华为云有专门的内审部门，定期对运维流程各项活动进行审计。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。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 对计算机网络进行分段，以实施差异化控制，考虑到用户组、加密数据流量、服务类型和信息系统等方面，以保护通信和关键网络安全资产，并隔离网络攻击可能对技术基础设施造成的不利影响的蔓延。 - 网络分段涵盖了实体提供的不同环境，包括开发、测试和生产环境。 - 现有的控制措施有助于保护、检测和遏制通过使用恶意代码对 IT 基础设施的攻击。 - 现有的控制措施有助于降低与内部或外部员工使用移动设备和远程工作以及物联网（IoT）设备相关的风险。	低：客户应使用网络外围防御工具，对高风险网络端口进行持续监控，通过无线网络进行身份验证和数据传输需要强加密（如适用），在互联网接入点以及 DMZ 区与内网之间部署防火墙，建立防火墙规则变更和定期审计的机制，部署入侵检测/防御系统，实施技术控制防止未经授权的网络连接。 中：除上述控制外，客户应将企业网络分区，采用纵深防御策	1.客户应制定适当的网络隔离措施来部署网络基础设施，以保护关键系统及客户数据免受网络攻击。为配合客户满足监管要求： （1）客户应对网络进行区段划分，对不同区域的数据或系统连接进行访问控制。客户可以使用华为云提供的虚拟私有云（VPC）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）华为云 Web 应用防火墙服务（WAF）是结合了华为多年攻防经验和一系列针对性优化算法的高级 Web 应用防火墙。采用正则规则和语义分析的双引擎架构对 SQL 注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意 bot、web shell、CC 等攻击实现实时的高性能防护。华为云 WAF 给用户提供简便的管理界面，用户可根据自身业务需要进行相关防护设置，亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。

		略。为远程访问管理控制台实施安全控制。对无线网络部署外围防火墙，使用高强度加密密钥。将访客无线网络与内网进行物理隔离。采用反欺骗措施来检测和阻止伪造的源 IP 地址进入网络。 高：除上述控制，客户应部署工具和/或制定流程阻止不安全的员工自有设备或未经授权的设备的访问，限制和监控受信任和不受信任区域之间的流量，并定期或按需评估和审查环境变化，已识别差距并采取补救计划。	（3）华为云建立了合理、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；Anti-DDoS 快速发现和防护 DDoS 攻击；WAF 实时检测和防御 Web 攻击；IDS/IPS 实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。 2.华为云制定了移动设备管理规定，以实施对移动计算设备的统一管理。对移动设备使用的原则、职责、权限要求、设备管理安全要求、网络接入要求及违规处罚等均做出规定。 3.华为云每年会对建立的移动办公终端相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。 4.员工离职或转岗等，必须对办公计算机硬盘进行格式化处理，若涉及机密、绝密信息，应确保删除的数据无法恢复，同时主动及时的卸载 BYOD 上公司应用清楚公司数据。若设备丢失或被盗，员工须向业务主管和信息安全部门报告，并远程擦除公司数据，并取消设备绑定。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 身份和物理和逻辑访问管理包括充分的控制，以保护受限访问区域、授予系统用户的权限、网络服务、操作系统和数据库、业务应用程序等的访问权限。 - 该实体提供的客户和用户与之互动的电子渠道具有适当的访问控制机制，以减轻第三方冒充或滥用提供给他们的产品和服务的风险。	客户应建立适当的访问控制政策，采用可靠的认证方式，如多因素认证。另外，客户还应定期审查和更新密码策略，保障密码的安全性。 客户应根据不同的功能或传输的数据类型，将网络在逻辑上或物理上隔离成不同的域和子网络。	1. 金融机构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。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。 2.华为云制定并记录正式的逻辑安全的政策和程序。及时批准、添加、修改或禁用，并定期审查华为员工和承包商的用户帐户。 华为建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循和授予的。堡垒主机提供基于密码和邮箱验证码的双因素身份验证功能，以验证用户的身份。用户通过互联网访问华为云办公子网，需要根据注册设备及其账号和密码进行双因素认证。华为云员工可以在 Cloud Scope 中进行逻辑访问管理，Cloud Scope 涵盖 Cloud Mnet System、CBC 帐户中心、堡垒机、FUXI 和 SVN 等多种支

			撑工具。支持工具涵盖本报告范围内所有产品的操作系统，包括但不限于虚拟服务器和基础设施设备的支持工具。在所有相关层的支持工具中的访问授权基于最小权限强制实施。高于最低权限的访问需要获得指定人的批准。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 该实体已建立规则和程序，确定需要通过加密技术以及允许或授权的密码算法来保护信息的传输和存储，以保护信息的机密性和完整性。	1. 客户应建立密码管理政策，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，并使用专门的证书颁发机构的证书对密钥的存储和传输进行管理。 2. 客户应实施适当和相关的加密技术以保护敏感数据的保密性和完整性。	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。 华为云建立了保护技术设备上的数据的加密策略与密钥管理机制，对人员的权限与职责分配、加密级别、加密方法进行了规定。针对于加密，华为云自身使用行业广泛使用的 AES 强效加密法对平台内的数据进行加密，对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过虚拟专用网络（VPN）和应用层 TLS 与证书管理，华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道。 华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。 针对于静态数据，华为云为保护租户数据的存储安全采取了一系列的保护机制。首先，华为云提供了数据加密服务（Data Encryption Workshop，简称 DEW）。它帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM－Hardware Security Module），为租户创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。与华为云服务对接 KMS 的服务有 OBS、云硬盘等。其次，专属加密满足租户更高合规性要求的加密场景，采用通过国家密码局认证或 FIPS140-2 第 3 级验证的硬件加密机，对租户业务进行专属加密，默认双机架构以提高可靠性。最后，华为云多款存储产品如 EVS、VBS 等均提供存储加密的机制。 针对于传输中的数据，华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过虚拟专用网络（VPN）和应用层 TLS 与证书管理，华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。控制台和 API 两种访问

			方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 该机构根据内部政策和现行法律规定，为信息的保存、传输和删除采取了适当的保护措施	客户应制定数据安全政策及对应安全策略，以对信息的保存、传输和删除进行保护。	华为云制定了数据安全策略及数据安全保护管理规定，对数据资产的分级分类标准进行了定义，同时明确了数据匿名化及标签化处理标准，对数据在整个生命周期中须遵循的安全措施进行了规范。华为云每年会对建立的数据安全管理相关规范和策略流程进行审计。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 该实体提供了持续监控工具，使其能够主动识别、收集和分析可能影响其网络安全资产的新威胁和漏洞的内部和外部信息。 - 该实体拥有自己的安全响应中心（SOC）或通过外部服务，该服务每天 24 小时运行，配备设施、技术工具、流程和经过培训的专职人员，以预防、检测、评估和响应网络安全威胁和事件。	客户应建立有效的补丁和漏洞管理机制，对所有技术资产进行漏洞识别和风险评估，对关键补丁进行测试，制定补丁更新周期以及补丁修复的工作流程。	作为云服务提供商： （1）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。 （2）华为云安全运营中心（SOC）已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，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，降低对用户业务造成影响的风险。同时，华为 PSIRT 和华为云 SOC 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，使基础设施、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用户业务的风险。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用户业务造成影响。 （3）此外，华为云会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为云相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。
4.1 保护关键网络安全资	- 实体有一个备份管理流程，使其能够在发生事故或灾难时确保其信息和处理设施的完整性和可用性，该流程必须与业务连续性管理的风险分析相一	客户应建立备份管理机制，定期对重要数据和文件进行备份，并采用适当的备份恢复方案，以便	作为云服务提供商： （1）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、云备份（CBR）、云硬盘备份（VBS）、云服务器备份（CSBS）等功能，将云上的文档、硬盘、

产，检测威胁和漏洞	致。信息备份应在无恶意代码的环境中生成、维护和使用，并得到适当控制。反过来，该实体至少每年对其备份执行一次恢复测试，以验证在原始数据丢失或损坏的情况下，关键信息可以恢复。	成功回滚重大系统变更。	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。 （2）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，系统在遵从相关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。
4.1 保护关键网络安全资产，检测威胁和漏洞	- 该实体定期识别和评估其技术基础设施可能暴露的攻击媒介，如通信篡改或拦截、网络钓鱼、恶意软件、权限提升、代码注入、拒绝服务、社会工程等；明确区分可能影响物理基础设施、逻辑基础设施或最终用户设备（终端）的攻击媒介。 - 该实体定期对其技术基础设施进行足够的范围和深度的安全测试，以检测可能存在的威胁和漏洞，例如笔试和/或道德黑客。结果由各自领域根据其职责进行管理，并至少每半年向董事会通报一次。会议纪要显示了对应采取的行动所采取的分析和协议。	客户应定期测试其网络安全框架的所有组成部分，以决定其整体成效。客户可使用一个或多个最新的方法和实践，例如安全漏洞评价、情景为本的测试及渗透测试。	作为云服务提供商： （1）华为云的云监控服务（CES）为客户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。可协助用户快速获取对云资源的告警，并采取相应的应对措施。同时华为云还可提供 Anti-DDoS 流量清洗服务、DDoS 高防（AAD）、Web 应用防火墙服务（WAF）、数据库安全服务（DBSS）、云审计服务（CTS）可帮助用户精准有效地实现对流量型攻击和应用层、数据层攻击的全面防护，以及事后对安全事件进行追溯和审计的功能。 （2）针对公有云攻击的手段多样、流量巨大的特点，华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速识别已经发生的攻击，并预判尚未发生的威胁。 （3）华为云定期会开展内部网络安全实战演练（如红蓝对抗）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。 （4）华为云安全运营中心（SOC）已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，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，降低对用户业务造成影响的风险。同时，华为 PSIRT 和华为云 SOC 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，使基础设施、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用户业务的风险。

			（5）华为云目前已获得多项国际上权威的安全与合规认证。华为云每年会聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计。
4.2 事件响应和恢复	- 实体至少每年测试一次，测试必要的计划，以充分处理可能影响网络安全的场景，以及对可能发生的网络事件做出响应的设备。每当发生变更或威胁网络安全的事件发生时，这些计划都会更新。 - 实体有明确的行动计划，根据网络安全事件的严重程度，允许将情况上报给高级管理层进行决策。 - 该实体针对高影响网络安全事件制定了由高级管理层主导的沟通计划，该计划将所有内部和外部利益相关者联系在一起，以使他们及时了解情况。	客户应制定事件响应计划，包括员工的角色和责任、事件检测和评估、报告和升级以及响应策略、与外部利益相关者（包括客户）的沟通计划。	作为云服务提供商，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。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响应时限和解决时限。 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。并根据事件的实时状态进行事件升级和通报。 华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。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。 在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知内容包括事件的描述、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。 华为云作为金融机构的服务提供方，会积极配合金融客户主动发起的沟通。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、热线电话等联络到华为云的支持团队。 同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。

9 华为云为客户提供的安全与隐私保护相关的云服务

客户负责客户数据安全，为保障客户内容安全，客户可以根据客户内容适合的安全级别，采取额外的安全措施，额外的安全措施可以来源华为云，也可来源第三方。

华为云理解客户的安全与隐私保护需求，并结合自身丰富安全与隐私保护实践及技术能力，提供了相关的安全与隐私保护相关云服务供客户选择。云服务涵盖网络、数据库、安全、管理与部署工具等产品，相关产品的数据保护、数据删除、网络隔离、权限管理、容灾备份、安全审计等功能可帮助客户加强安全保障。

- **安全合规**

产品名称	产品介绍	核心功能
Web 应用防火墙 Web Application Firewall (WAF)	WAF 可对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，阻挡诸如 SQL 注入或跨站脚本等常见攻击。 客户可使用 WAF 保护其网站或服务器免受外部攻击，避免这些攻击影响 Web 应用程序的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险。	安全防护
云防火墙 Cloud Firewall (CFW)	CFW 是新一代的云原生防火墙，提供云上互联网边界和 VPC 边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI 提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，让用户快速灵活应对威胁。 云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	资产保护 访问控制 在线防御
企业主机安全 Host Security	HSS 能提供资产管理、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	资产管理

Service (HSS)	主机安全风险，实时发现并阻止黑客入侵行为，以及满足等保合规的要求。 客户可通过 HSS 更方便地管理主机、容器的安全风险，实时发现勒索、挖矿、渗透、逃逸等入侵行为，以满足等保合规的要求。	漏洞管理 基线检查 入侵检测
数据库安全服务 Database Security Service (DBSS)	DBSS 是一款智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL 注入攻击检测，风险操作识别等功能。 客户可通过 DBSS 检测潜在风险，保障云上数据库的安全。	安全审计
数据加密服务 Data Encryption Workshop (DEW)	DEW 是一款综合的云上数据加密服务，提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块保护，并与华为云其他服务集成。客户也可以借此服务开发自己的加密应用。 客户可采用 DEW 进行密钥全生命周期集中管理，保障数据存储过程中的完整性。	数据加密
DDoS 高防 (AAD)	AAD 是一款保护互联网服务器免受大流量 DDoS 攻而击导致不可用的增值服务。 客户可以通过 AAD 产品配置高防 IP，将攻击流量引流到高防 IP 清洗，确保源站业务稳定可靠。	安全防护
数据安全中心 Data Security Center (DSC)	DSC 是新一代的云原生数据安全平台，提供数据分类分级，数据安全风险识别，数据水印溯源，数据脱敏等基础数据安全能力。 客户可通过 DSC 整合数据安全生命周期各阶段状态，构建云服务全景图，保护数据采集、存储/传输、使用、交换/销毁的安全。	数据分级分类 数据脱敏 数据水印
云堡垒机 Cloud Bastion Host (CBH)	CBH 是华为云的一款 4A 统一安全管控平台，为企业提供集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体的运维管理服务。 客户可通过 CBH 对云主机进行远程运维，提高客户的访问控制安全能力，保护资源运维和系统管理的安全性，降低系统和运维资源被非法入侵的风险。	权限管理
云证书管理服务 Cloud Certificate Manager (CCM)	CMM 是一个为云上海量证书颁发和全生命周期管理的服务，提供 SSL 证书管理和私有证书管理服务。 客户可通过 CCM 提高对 SSL 证书和私有证书的保密性和安全性，提升访问和传输通道的安全，降低数据在传输和访问过程中被非法入	证书管理

	侵、访问或盗取的风险。	
安全云脑 SecMaster	安全云脑基于云原生安全，提供全面的日志采集、安全治理、智能分析、态势感知、编排响应等快速闭环的安全信息和事件管理能力，实现自动化安全运营，助客户守护云上安全。	态势感知 安全运营

- **存储**

产品名称	产品介绍	核心功能
云备份 Cloud Backup and Recovery (CBR)	CBR 为云上的弹性云服务器、裸金属服务器、云硬盘、云下 VMware 虚拟化环境和本地文件目录，提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。	数据备份
云硬盘备份 Volume Backup Service (VBS)	VBS 为云硬盘创建在线永久增量备份，并对加密盘发备份数据自动加密，并可将数据恢复到任意备份点，增强数据可用性。 VBS 可降低病毒入侵、人为误删除、软硬件故障等事件的发生的可能性，保护数据安全可靠，降低数据被非法篡改的风险。	数据备份
云服务器备份 Cloud Server Backup Service (CSBS)	CSBS 可同时为云服务器下多个云硬盘创建一致性在线备份。 CSBS 可降低病毒入侵、人为误删除、软硬件故障等事件的发生的可能性，保护数据安全可靠，降低数据被非法篡改的风险。	数据备份

- **管理与监管**

产品名称	产品介绍	核心功能
统一身份认证服务 Identity and Access Management (IAM)	提供身份认证和权限管理功能，可以管理用户（比如员工、系统或应用程序）帐号，并且可以控制这些用户对其名下资源的操作权限。 客户可通过 IAM 采取适合的用户管理、身份认证和细粒度的云上资源访问控制等措施，防止对内容数据进行的未授权修改。	权限管理
云审计服务 Cloud Trace Service (CTS)	为客户提供云帐户下资源的操作记录，实现安全分析、合规审计、问题定位等场景。 客户可以通过配置 CTS 对象存储服务，将操作记录实时同步保存至 CTS，以便保存更	安全审计

产品名称	产品介绍	核心功能
	长时间的操作记录，保障数据主体的知情权、实现快速查找。	
云监控服务 Cloud Eye Service (CES)	为客户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。 客户可通过 CES 全面了解华为云上的资源使用情况、业务的运行状况，并及时收到异常报警做出反应，保证业务顺畅运行。	安全审计
云日志服务 Log Tank Service (LTS)	提供日志收集、实时查询、存储等功能，无需开发即可利用日志做实时决策分析，提升日志处理效率，帮助用户轻松应对日志实时采集、查询分析等日常运营、运维场景。 客户可通过 LTS 保留对个人信息的操作记录，保障数据主体的知情权。	安全审计
配置审计 Config	配置审计（Config）服务提供全局资源配置的检索，配置历史追溯，以及基于资源配置的持续的审计评估能力。 客户可通过 Config 查看资源详情、资源之间的关系、资源历史，并可以通过配置合规规则来对资源进行合规性检查，确保云上资源配置变更符合预期。	安全审计

- **网络**

产品名称	产品介绍	核心功能
虚拟专用网络 Virtual Private Network (VPN)	VPN 用于搭建客户本地数据中心与华为云 VPC 之间便捷、灵活，即开即用的 IPsec 加密连接通道。 客户可通过 VPN 实现灵活一体，可伸缩的混合云计算环境，并且由于 VPN 的加密特性，提高了客户的安全防护能力。	安全传输
虚拟私有云 Virtual Private Cloud (VPC)	VPC 是客户在华为云上的隔离的、私密的虚拟网络环境。客户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性 IP 搭建业务系统。 VPC 是客户的云上私有网络，各客户之间 100%隔离，增强云上数据的安全性。	网络隔离

10 结语

华为云致力于为金融行业客户提供符合监管要求的安全的云环境，并持续运营华为云安全保障体系。本文描述了华为云在金融监管重点领域下的安全实践，有助于金融行业客户详细了解华为云对于金融行业监管要求方面的遵从性，让客户安全、放心地使用华为云。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合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，不具备任何法律效力或构成任何形式的法律建议。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金融行业监管要求的遵从性。

11 版本历史

日期	版本	描述
2025 年 5 月	1.0	首次发布

