

华为云哥伦比亚

金融行业监管要求遵从性指南

文档版本 1.0
发布日期 2026-07-13



版权所有 © 华为云计算技术有限公司 2026。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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
1.1 背景与发布目的	1
1.2 适用的哥伦比亚金融监管要求简介	1
1.3 名词定义	2
2 华为云安全合规	4
3 华为云责任共担模型	7
4 华为云全球基础设施	9
5 华为云如何遵从及协助客户满足《基础法律通函 C.E. 006/2025》的要求	10
5.1 P1-T1-C4 云计算服务使用规则	10
5.2 P1-T1-C8 金融创新活动受控测试空间	21
5.3 P1-T1-C9 开放金融相关规则	23
5.4 P1-T2-C1 金融服务提供中信息处理渠道媒介安全与质量	26
5.5 P1-T4-C5 信息安全和网络安全管理的最低要求	32
6 华为云为客户提供的安全与隐私保护相关的云服务	39
7 结语	43
8 版本历史	44

1 概述

1.1 背景与发布目的

近年来，哥伦比亚金融监管体系持续演进。2025 年，哥伦比亚金融监管局（SFC）发布了《基础法律通函 C.E. 006/2025》，该文件全面整合并替代了旧版法规，成为金融机构合规管理的核心依据。新通函系统性地纳入了云计算服务使用规则、开放金融框架、信息安全管理及网络安全风险防控等关键章节，为金融机构在数字化转型中的合规运营提供了明确指引。与此同时，财政与公共信贷部（MHCP）通过第 1297/2022 号法令等文件，持续完善开放银行、数字支付及数据共享的监管标准。

华为云作为云服务提供商，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监管要求的云服务及业务运行环境。本文将针对哥伦比亚金融机构在使用云服务时通常需遵循的监管要求，并阐述华为云将如何协助其满足这些监管要求。

1.2 适用的哥伦比亚金融监管要求简介

哥伦比亚财政与公共信贷部（MHCP）是哥伦比亚的中央财政主管部门，负责国家的财政政策、公共信贷及国库管理，主要职能包括制定财政与税收政策、管理公共债务、编制政府预算，并代表政府进行国际金融合作。

- 第 2555/2010 号法令（Decreto 2555 de 2020）**：该政策文件是对哥伦比亚金融法令的集合版，资产管理、云外包原则及最新的开放金融条款，明确了第 2555/2010 号法律的执行细则。
- 第 1234/2020 号法令（Decreto 1234 de 2020）**：该政策文件规定了金融科技创新监管沙盒（Sandbox）的设立范围与运行机制，以及哥伦比亚政府对金融机构在受控环境下测试创新产品、服务和业务模式的要求和期望。具体内容在本白皮书 5.2 中分析。
- 第 1297/2022 号法令（Decreto 1297 de 2022）**：该法令由财政部发布，旨在修改和补充哥伦比亚金融体系中关于开放银行业（Open Banking）、数字支付及支付系统治理的规定。主要内容涵盖了金融机构间数据共享的安全性标准、低价值支付系统的互操作性要求，以及关于电子钱包和数字入职的运营细则。具体内容在本白皮书 5.3 中分析。

哥伦比亚金融监管局（SFC），是哥伦比亚主要的金融监管机构，其核心职能是制定并执行金融领域的规则，监督金融机构和加密服务提供商的关键信息基础设施安全与数据保护。

- **基础法律通函 C.E. 006/2025（Circular Básica Jurídica）**：该政策文件是对哥伦比亚金融机构法律合规要求的全面更新与集成，2025 年发布的版本彻底整合并替代了旧版（29/14），详细规定了金融机构在公司治理、消费者保护及合规经营方面的具体义务。包含与云计算服务使用有关的规则，开放金融相关规则等章节。
 - **P1-T1-C4 <云计算服务使用规则>**：该政策文件规范了金融机构与云计算服务使用有关的规则。包含对服务商的尽职调查、建立完整的信息安全管理体系，合同必备条款以及确保监管机构审计权的合规义务。该章节内容整合了**外部通函 C.E. 005/2019（Circular Externa 005 de 2019）**的内容。
 - **P1-T4-C5 <信息安全和网络安全管理的最低要求>**：该政策文件通过修订金融审计管理体系（SARO），细化了业务连续性管理与网络安全风险的最低要求，规定了机构在面对信息安全威胁时必须建立的预防、检测及响应机制。该章节内容整合了**外部通函 C.E. 007/2018（Circular Externa 007 de 2018）**的内容。
 - **P1-T1-C8 <金融创新活动受控测试空间>**：该通函由 SFC 发布，正式确立了监管沙盒（Sandbox）的运行机制。主要内容包括受控测试空间的申请流程、入选标准及退出机制，允许金融实体和技术公司在受限且受监控的环境中，对创新的金融产品或业务模式进行为期最长两年的实测。该章节内容整合了**外部通函 C.E. 016/2021（Circular Externa 016 de 2021）**的内容。
 - **P1-T1-C9 <开放金融相关规则>**：该政策文件依据 2010 年第 2555 号法令，SFC 制定了发展开放金融所需的技术、安全和其他标准。该文件规定在获得金融消费者授权的情况下，以标准化的方式与其他受监管实体或第三方共享金融消费者信息，从而使这些实体能够向所述客户提供服务。该章节内容整合了**外部通函 C.E. 004/2024（Circular Externa 004 de 2024）**的内容。
 - **P1-T2-C1 <金融服务提供中信息处理渠道 媒介 安全与质量>**：由 SFC 发布，重点修订了《基础法律通函》中关于业务安全与质量的最低要求。该通函规定了金融实体在提供银行服务（特别是通过数字渠道和代理商）时必须遵守的技术标准，涉及身份验证、交易监控及防范电子欺诈的风险防控措施。该章节内容整合了**外部通函 C.E. 008/2018（Circular Externa 008 de 2018）**的内容。
- **基础金融通函 C.E.004/2026（Circular Básica Financiera）**：由哥伦比亚金融监管局于 2026 年 4 月 14 日正式发布，并自 2026 年 6 月 1 日起生效。该通函按照风险管理、法定控制与审慎监管事项、财务信息与报告框架以及其他规定四大部分重新组织金融监管要求，涵盖综合风险管理、资本充足率与偿付能力、压力测试、大额风险暴露管理、金融信息披露、会计处理及监管报送等内容，成为哥伦比亚受监管金融机构遵循的核心审慎监管和财务监管汇编文件。法规中合规相关条款基础法律通函 C.E. 006/2025 的分析中已覆盖，详情请参考本白皮书 5.1-5.5。

1.3 名词定义

- 华为云

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。

- **分包商或合作伙伴**

是指由云服务提供商雇佣或与其相关的第三方，此类第三方活动涉及开发受监管实体所使用的云服务中的大部分内容且为可能访问受监管的信息和数据的非辅助性和支持性活动。

- **网络攻击**

一个或多个代理人利用网络空间服务或应用程序进行有组织或预谋的犯罪行为，或者成为此类犯罪行为的目标，或者网络空间是犯罪的来源或工具。

- **网络安全**

是指发展企业防御和预测网络威胁的能力，以保护和保障网络空间中对企业运营至关重要的数据、系统和应用程序。

- **开放金融**

根据哥伦比亚 1297/2022 号法令，开放金融被确立为一种基于客户授权的、标准化的金融数据交换模式，旨在促进竞争和支付系统的互操作性。

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
ISO 27001	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的持续运行。
ISO 27017	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 27018	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 42001	ISO/IEC 42001是全球首个人工智能管理体系标准，该标准提供了一个可认证的人工智能管理体系（AIMS）框架，为组织建立、实施、维护和持续改进人工智能管理体系提供要求和指南，旨在帮助组织和社会负责任地开发、提供和使用AI系统，并从人工智能中受益。
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ISO 9001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

认证	描述
	套通用的质量管理体系要求。它包括了ISO 9001的所有要求，ISO 9001将来的任何改动也会导致TL9000的改动。 华为云取得了ISO 9001 / 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。
ISO 20000	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 22301	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。
CSA STAR	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。
ISO 27701	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ISO 27701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	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信息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 and 内部控制情况出具的独立审计报告。

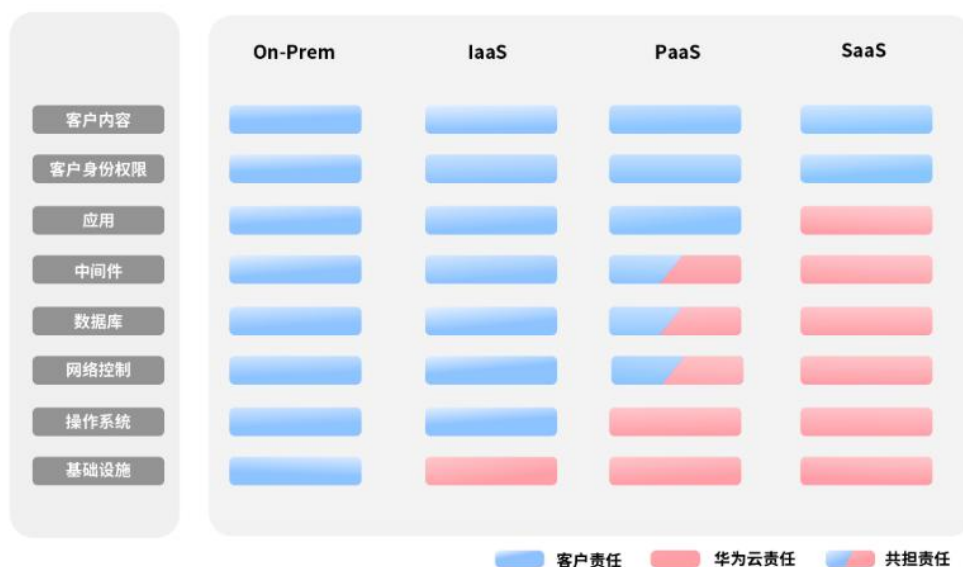
3 华为云责任共担模型

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。

在监管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。华为云在哥伦比亚工业和商业监管局（SIC）认可的数据保护充分性水平国家（墨西哥、巴西、秘鲁、阿根廷、爱尔兰等）部署了地理区域（Region）和可用区（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 地理区域（Region）和可用区（AZ）示例



5 华为云如何遵从及协助客户满足《基础法律通函 C.E. 006/2025》的要求

哥伦比亚金融监管局（Superintendencia Financiera de Colombia，简称 SFC）于 2025 年 6 月 26 日更新了 C.E.006/2025 号基本法律通告（通告 Básica Jurídica）。本政策文件全面更新和整合了哥伦比亚金融机构的法律合规要求。2025 年发布的版本完全整合并取代了之前的版本（2014 年第 029 号通知），详细说明了金融机构在公司治理、消费者保护和合规运营方面的具体义务。它包括与云计算服务使用和开放金融法规相关的规则等章节。

当金融机构遵守《基本法律通告》的要求时，华为云作为云服务提供商（CSP）可能会参与这些要求所涵盖的一些活动。以下部分将总结《基本法律通告》中与云服务提供商相关的控制要求，并详细说明华为云作为 CSP 如何帮助金融机构满足这些控制要求。

5.1 P1-T1-C4 云计算服务使用规则

P1-T1-C4 <云计算服务使用规则>章节规范了金融机构与云计算服务使用有关的规则。包含对服务商的尽职调查、建立完整的信息安全管理体系，合同必备条款以及确保监管机构审计权的合规义务。该章节内容整合了外部通函 C.E. 005/2019（Circular Externa 005 de 2019）的内容。

金融机构在遵循<云计算服务使用规则>的要求时，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<云计算服务使用规则>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。

编号	具体控制要求	客户关注点	华为云的应答
3.1.	金融机构应从订购的云服务类型、处理地点、所订购的服务、待处理的信息类型、虚拟化环境中的数据保护安全控制措施、企业应用程序的保护措施等多方面有效管理使用云计算服务而产生的运营风险。	客户应有效管理因使用云计算服务而产生的风险，包括订购的云服务类型、处理地点、所订购的服务、待处理的信息类型、虚拟化环境中的数据保护安全控制措施。	为配合客户满足监管要求，华为与在安全机制、责任分工、可提供的数据处理位置、覆盖数据生命周期的安全管控等方面做充分的努力： 1. 华为云参照ISO 27001、ISO 20000、CSA STAR等众多国际及行业标准，构建并实施了一套完善的云计算风险管理体系，涵盖了IT治理

编号	具体控制要求	客户关注点	华为云的应答
			/管理、信息系统开发和获取、IT运营、通信网络、信息安全等各个领域，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。 2. 为配合客户满足合规要求，华为作为云技术的研发者和云服务运营者的双重角色，华为云负责其作为云服务提供商的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全保障。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。此外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。 3. 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

编号	具体控制要求	客户关注点	华为云的应答
			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。 4. 为保障客户安全的处理云上数据华为云对数据从数据创建、数据存储、数据使用、数据共享、数据归档到数据销毁全生命周期的各阶段进行层层防护，并通过友好的操作界面和接口，方便客户使用与集成，满足不同行业客户对数据安全的个性化需求。为了满足合规要求，华为云还在认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理破坏等方面，通过优秀的技术、实践和流程，为客户提供一系列遵循先进行业标准的数据安全生命周期管理服务。它还确保租户隐私、所有权和对其数据的控制不受侵犯，为用户提供最有效的数据保护。
3.3.	金融机构应验证云服务提供商是否拥有并保持至少 ISO 27001 认证，并符合 ISO 27017 和 27018 等标准或最佳实践。提供商可能通过替代、替换或修改先前标准或最佳实践的认证，并且必须提供服务组织控制报告（SOC1、SOC2 和 SOC3）。	客户应验证云服务提供商的资质。	华为云已通过 ISO 27001、ISO 27017、ISO 27018、SOC 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，向客户提供服务组织控制报告（SOC1、SOC2 和 SOC3）。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”。
3.4.	金融机构应确认服务提供商在 IaaS 和 PaaS 模式下提供的云服务可用性至少为 99.95%。对于 SaaS 模式下的云计算服务提供商，可用性必须至少为 99.5%。	客户应确认服务提供商在 IaaS 和 PaaS 模式下提供的云服务可用性。	华为云遵循适用的法律法规要求，为客户提供满足可用性要求的服务。如华为云弹性云服务器服务（ECS）通过商业和技术上的合理努力，单实例维度（单区域单可用维度）每服务周期服务可用率不低于99.975%；单区域多可用区维度每服务周期服务可用率不低于99.995%。

编号	具体控制要求	客户关注点	华为云的应答
3.5.	金融机构应管理云服务提供商提供的 API 或 Web 服务所涉及的风险。	客户应管理云服务提供商提供的 API 或 Web 服务的风险。	1. 华为云在信息传输过程中使用安全的加密通道（如 HTTPS），对存储的静态数据使用安全的加密算法，确保不同状态下的数据机密性。通过数字签名、时间戳等控制机制，防止数据传输过程中的篡改，保证信息的完整性，以及防止重放攻击。记录应用服务中的操作日志，以此来支持审计。对接口进行身份认证、传输和边界保护，确保 API 应用的安全。 2. 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。
3.7.	金融机构应建立机制，允许对云端处理的信息进行备份，以便在需要时实体能够访问这些信息。	客户应建立机制，允许对云端处理的信息进行备份。	1. 作为云服务提供商，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（Object Storage Service，简称 OBS）的版本控制、云硬盘备份（Volume Backup Service，简称VBS）、云服务器备份（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，也可以通过华为云云备份（Cloud Backup and Recovery，简称CBR）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

编号	具体控制要求	客户关注点	华为云的应答
			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。
3.8.	金融机构应确保信息和备份与其他在云端处理信息的实体的信息相互独立。这种独立性可以在逻辑层面或物理层面实现。	客户应确保信息和备份与其他在云端处理信息的实体的信息相互独立。	1. 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。 2. 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。
3.9.	无论是在传输过程中还是在存储状态下，都应使用国际公认的最新强加密标准和算法，对被归类为机密的信息进行加密。	客户应使用国际公认的最新强加密标准和算法，对被归类为机密的信息进行加密。	1. 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（Elastic Volume Service, 简称EVS）、对象存储服务（Object

编号	具体控制要求	客户关注点	华为云的应答
			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，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密码安全中心（Data Encryption Workshop, 简称 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。钥泄露，保护密钥安全。DEW 还支持金融机构导入自有密钥作为金融机构主密钥进行统一管理，方便与金融机构已有业务的无缝集成、对接。同时华为云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. 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。针对客户业务混合云部署和全球化布局的场景，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数据传输安全。

编号	具体控制要求	客户关注点	华为云的应答
3.10.	根据合同约定的服务模式，对用户和访问权限进行管理，以访问所提供的服务以及在云端运行的平台、应用程序和数据库。	客户应对用户和访问权限进行管理。	1. 华为云提供了线上的《华为云用户协议》以及《华为云云服务等级协议》，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。 2. 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。华为云的云审计服务（Cloud TraceService，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。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。
3.11.	监控承包服务，以发现不必要的操作或变更，并在需要时采取预防或纠正措施。	客户应监控外包服务，以发现不必要的操作或变更。	1. 客户可以使用华为云的云审计服务（Cloud TraceService，简称CTS）进行操作监控，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

编号	具体控制要求	客户关注点	华为云的应答
			常见应用场景。 2. 华为云建立了集中、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，持续的监控和实时分析保证对安全事件的及时发现，以确保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，确保所有日志保存时间超过 180 天，90 天内可以实时查询。华为云有专门的内审部门，定期对运维流程各项活动进行审计。
3.12.	金融机构应建立程序，以核实是否遵守与云服务提供商及其分包商或合作伙伴签订的协议和服务级别协议（如果由他们提供服务），并与第三方设定服务分包的条件。	客户应建立程序，以核实服务提供商及其分包商或合作伙伴是否遵守协议。	1. 华为云提供了线上的《华为云用户协议》以及《华为云云服务等级协议》，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。 2. 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ISO 27001、ISO 27017、ISO 27018、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。
3.13.	与云服务提供商建立端到端加密的通信通道，并尽可能使用不同的路由。	客户应建立端到端加密的通信通道。	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（Virtual Private Network，简称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，

编号	具体控制要求	客户关注点	华为云的应答
			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。
3.16.	确定云服务提供商仅使用共享信息来运行合同服务，并明确表示数据归受监管实体所有。	客户应确定云服务提供商仅使用共享信息来运行合同服务，并明确表示数据归受监管实体所有。	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，并遵守各国《个人数据保护法》所述的数据保护原则。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。
3.17.	金融机构应通过报告和认证，验证云服务提供商在合同服务中的质量、性能和有效性。	客户通过报告和认证应验证云服务提供商在合同服务中的质量、性能和有效性。	1. 华为云已通过ISO 27001、ISO 27017、ISO 27018、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。 2. 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”。
3.18.	建立数据删除机制，以便在存储介质被更换、合同终止或受监管实体要求时，加快安全删除存储介质上的现有数据。	客户应建立机制，以便在存储介质被更换、合同终止或受监管实体要求时，加快安全删除存储介质上的现有数据。	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。在客户终止使用华为云服务，需要对内容数据进行销毁时，华为云会对指定的数据及其所有副本进行全面的清除。当客户确认删除操作后，华为云

编号	具体控制要求	客户关注点	华为云的应答
			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。
3.19.	考虑及时有效地纠正已发现的计算机漏洞。	客户应及时有效地纠正已发现的计算机漏洞。	为配合客户满足监管要求： 1. 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。华为云已与合作伙伴联合推出了主机入侵检测、Web应用防火墙、主机漏洞检测、网页防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力。 2. 华为安全运营中心（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。 3. 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

编号	具体控制要求	客户关注点	华为云的应答
			计。
3.20.	对管理控制台的访问采用多因素身份验证技术。	客户应对管理控制台的访问采用多因素身份验证技术。	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。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。IAM 支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信验证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。
3.21.	在业务连续性计划中考虑云计算服务。	客户应在业务连续性计划中考虑云计算服务。	1. 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ISO 22301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。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。 2. 客户可以依赖华为云数据中心集群的区域和可用区架构，实现业务系统的容灾和

编号	具体控制要求	客户关注点	华为云的应答
			备份。按规则在全球部署数据中心。客户通过两个地方拥有灾难数据备份中心。如果发生故障，系统会自动从受影响区域传输客户应用程序和数据，在满足合规策略的前提下，确保业务连续性。华为云还部署了全球服务器负载均衡中心。客户应用可以在数据中心实现N+1部署。即使一个数据中心发生故障，它也可以将流量负载均衡到其他中心。
3.23	与供应商建立沟通渠道，以便了解任何可能对服务提供产生重大影响的事件或情况。	客户应与供应商建立沟通渠道，以便了解任何可能对服务提供产生重大影响的事件或情况。	华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。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。

5.2 P1-T1-C8 金融创新活动受控测试空间

哥伦比亚财政与公共信贷部于 2020 年 9 月 14 日发布了《2020 年第 1234 号法令》。该文件规定了金融科技创新监管沙盒（Sandbox）的设立范围与运行机制，以及哥伦比亚政府对金融机构在受控环境下测试创新产品、服务和业务模式的要求和期望。具体内容在基础法律通函 C.E. 006/2025 的 P1-T1-C8 <金融创新活动受控测试空间>章节呈现。

P1-T1-C8 <金融创新活动受控测试空间>由 SFC 发布，正式确立了监管沙盒（Sandbox）的运行机制。主要内容包括受控测试空间的申请流程、入选标准及退出机制，允许金融实体和技术公司在受限且受监控的环境中，对创新的金融产品或业务模式进行为期最长两年的实测。该章节内容整合了外部通函 C.E. 016/2021 (Circular Externa 016 de 2021) 的内容。金融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 P1-T1-C8 <金融创新活动受控测试空间>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。

编号	具体控制要求	客户关注点	华为云的应答
2.35.7. 2.3	参与的受监管实体必须向哥伦比亚金融监管局提交临时运营证书申请，申请内容必须包括： 1. 将创新技术开发与其执行的金融、股市或保险活动分开，旨在促进计时赛的运作拆解，避免参与金融消费者之间	客户的创新技术开发应与其他执行分开，在单独本地化环境开展业务。	作为云服务供应商，华为云在上述要求可提供的支持的如下： 1. 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力、业界标准等作为检

编号	具体控制要求	客户关注点	华为云的应答
	的混淆。		查项，开发配套的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。 2. 华为云对云端数据的隔离是通过虚拟私有云（Virtual Private Cloud，简称VPC）实施的，VPC采用网络隔离技术，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：一方面，结合虚拟专用网络（Virtual Private Network，简称VPN）或云专线，将VPC与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用VPC构建私有网络环境，通过子网规划、路由策略配置等进行网络区域划分，将存储放置在内部子网，并通过配置网络 ACL 和安全组规则对进出子网以及和虚拟机的网络流量进行严格的管控。 3. 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

编号	具体控制要求	客户关注点	华为云的应答
			均将客户数据隔离作为重要特性。
2. 35. 7. 2. 5 2. 35. 7. 4. 1	临时作证书包含测试进行的条件而有效期，临时运营证书自签发日起最长可达两年。 一旦临时运营证书规定的期限届满, 必须根据哥伦比亚财政监督局为此目的发布的一般指令启动撤销计划。在此程序执行过程中需要完全停止与受控测试领域开发的金融服务或产品的运营。	客户应注意申请的测试空间运营证书期限最长使用时间为2年。终止时需要完全停止与受控测试领域开发的金融服务或产品的运营。	作为云服务供应商，华为云在上述要求可提供的支持的如下： 1. 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。为了避免重要数据销毁后不可恢复，或因误操作丢失，建议客户在销毁数据之前慎重考虑，对拟销毁的数据做好备份或迁离。 2. 在客户确认删除数据后，会对指定的数据及其所有副本进行全面的清除，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 P1-T1-C9 开放金融相关规则

P1-T1-C9 <开放金融相关规则>章节是依据第 1297/2022 号法令 (Decreto 1297 de 2022)法令， 制定发展开放金融所需的技术、安全和其他标准。该文件规定在获得金融消费者授权的情况下，以标准化的方式与其他受监管实体或第三方共享金融消费者信息，从而使这些实体能够向所述客户提供服务。该章节内容整合了外部通函 C.E. 004/2024（Circular Externa 004 de 2024）的内容。

金融机构在遵循 <开放金融相关规则> 的要求时，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 <开放金融相关规则> 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。

编号	具体控制要求	客户关注点	华为云的应答
3.1	参与开放金融的受监管实体必须制定政策、程序，并配备技术和人力资源，以确保金融消费者的个人数据得到安全处理。为此，受监管实体必须遵守以下规定： a) 内部网络中，开放金融相关系统的维护与其他网络逻辑隔离。 b) 监控在开放金融框架内流通的信息是否符合受监管实体与第三方数据接收方之间制定的规范。 c) 避免公开用于开发开放金融的信息库。 d) 对每次开放金融开发过程中提出的数据请求进行日志记录，日志保存五年。这些日志至少应包含以下信息：请求来源、信息使用时间、请求发起者、流通的信息以及处理状态。在所有情况下，根据信息的敏感程度，必须对信息进行脱敏或加密处理。 e) 为确保信息系统随时可用且易于访问，并建立冗余、负载均衡和容错机制，以保证其持续可用性。	客户应制定相应的政策、程序，并配备相应的技术和人力资源，以确保金融消费者的个人数据得到安全处理。	1. 华为云从最初的网络架构设计、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）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，对进出子网以及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，并遵守各国《个人数据保护法》所述的数据保护原则。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

编号	具体控制要求	客户关注点	华为云的应答
			重要特性。 3. 华为云有集中、完整的日志大数据分析系统。该系统统一收集数据库的管理行为日志和各安全产品及租价的维系检测告警日志，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天内可实时查询。 4. 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。
3.2 3.2.3	受监管实体必须实施自动信息交换协议，以处理第三方数据接收方在发展开放金融过程中提交的个人数据访问请求。如果第 3.2 条中规定的任何格式、参考框架、标准或协议被其制定或支持机构宣布过时，则受监管实体必须采用对其进行修改、替代或补充的版本。	客户应参考框架、标准或协议保障数据安全性。	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。针对客户业务混合云部署和全球化布局的场景，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数据传输安全。

5.4 P1-T2-C1 金融服务提供中信息处理渠道媒介安全与质量

P1-T2-C1 <金融服务提供中信息处理渠道媒介安全与质量>章节主要关于业务安全与质量的要求。该通函规定了金融实体在提供银行服务（特别是通过数字渠道和代理商）时必须遵守的技术标准，涉及身份验证、交易监控及防范电子欺诈的风险防控措施。该章节内容整合了外部通函 C.E. 008/2018 (Circular Externa 008 de 2018) 的内容。

金融机构在遵循<金融服务提供中信息处理渠道媒介安全与质量>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<金融服务提供中信息处理渠道媒介安全与质量>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。

编号	具体控制要求	客户关注点	华为云的应答
1.2.2.1.2.4	根据本章第 2.3.4.1.5 款的规定，使用强加密机制将有关通过技术媒介进行的操作的信息传输到受监管实体的技术平台。	金融机构应使用强加密机制将有关通过技术媒介进行的操作的信息传输到受监管实体的技术平台。	华为云为金融服务机构提供端到端的数据传输安全保护，支持使用符合国际标准的 TLS 1.2 及以上版本的协议。客户可以通过华为云提供的虚拟私有云（VPC）和 VPN 连接实现安全的加密数据传输。
1.2.2.1.2.1.1	详细记录你的通讯员通过技术手段开展的所有活动（成功和失败）。	金融机构应详细记录通讯员通过技术手段开展的所有活动（成功和失败）。	华为云的 云审计服务（Cloud Trace Service, 简称CTS） 为用户提供云账户资源操作的记录，CTS 收集、存储并审计由华为云管理控制台、SDK、API 或其他方式发起的资源操作请求及其结果。
2.3.1.	关于信息安全 2.3.1.1. 保密性：指保护未经授权不得披露的信息。 2.3.1.2. 完整性：信息从创建到销毁必须准确、一致和完整。 2.3.1.3. 可用性：信息必须在现在和将来以所需的格式和时间可用，并且必须具备使用该信息所需的资源。	金融机构应确保信息的保密性，完整性，可用性	为保障客户安全的处理云上数据，华为云对数据从数据创建、数据存储、数据使用、数据共享、数据归档到数据销毁全生命周期的各阶段进行层层防护，并通过友好的操作界面和接口，方便客户使用与集成，满足不同行业客户对数据安全的个性化需求。为了满足合规要求，华为云还在认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理破坏等方面，通过优秀的技术、实践和流程，为客户提供一系列遵循先进行业标准的数据安全生命周期管理服务。它还确保租户隐私、所有权和对其数据的控制不受侵犯，为用户提供最有效的数据保护。

编号	具体控制要求	客户关注点	华为云的应答
2.3.3.1.1.	拥有硬件、软件和电信设备，以及必要的程序和控制措施，以便在安全和质量条件下提供服务和处理信息。	金融机构应保证硬件、软件和电信设备控制在安全和质量条件下提供服务和处理信息。	华为云通过完善的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，确保信息安全在信息系统开发生命周期中得到设计和实现。华为云参照ISO 27001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。
2.3.3.1.2.	管理信息安全，他们可以使用 ISO 27000 标准或其替代标准作为参考。	金融机构应保证管理信息安全。	华为云参照ISO 27001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。
2.3.3.1.4.	确保实体设备和网络上处理的机密客户信息的安全。	金融机构应确保实体设备和网络上处理的机密客户信息的安全。	华为云作为云服务提供商，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先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为用户提供最切实有效的数据保护能力，保证租户对其数据的隐私权、所有权和控制权不受侵犯。华为云使用多种隐私保护平台工具，帮助华为云更快速、系统、高效地处理与隐私保护相关的各项工作。

编号	具体控制要求	客户关注点	华为云的应答
2.3.3.1.5.	确保发送给客户的信息不含恶意软件。	金融机构应确保发送给客户的信息不含恶意软件。	客户可通过使用华为云的 企业主机安全（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、恶意程序检测等功能，能够帮助企业更方便地管理主机安全风险，助力实时发现并阻止黑客入侵行为。
2.3.3.1.6.	保护信息系统的访问密钥。为履行此项义务，各实体必须避免使用共享密钥、通用密钥或群组密钥。实体设备和计算机系统上的身份识别和认证必须是唯一且个性化的。	金融机构应保护信息系统的访问密钥。	客户可以适用华为云提供的 密码安全中心（Data Encryption Workshop, 简称 DEW） 进行密钥管理，DEW 是一款综合的云数据加密服务，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。
2.3.3.1.16.	同步实体所有参与分销渠道的信息系统时钟。应以负责提供法定时间的机构根据适用法规提供的官方时间作为参考。	金融机构应同步实体所有参与分销渠道的信息系统时钟。	华为云所有的物理服务器和虚拟机均通过网络时间协议（NTP）与华为云授时中心同步。华为云授时中心本身与高精度的原子钟同步，确保系统时间的准确性。
2.3.3.1.18	具有报告通道状态的控制和报警功能，并允许及时发现和纠正故障。	金融机构软件应具有报告通道状态的控制和报警功能，并允许及时发现和纠正故障。	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、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。
2.3.3.1.23.	受监管实体必须向证监会（SFC）报告任何严重影响客户服务渠道支持系统中所处理信息的保密性、完整性或可用性的事件。	金融机构应向证监会（SFC）报告任何严重影响客户服务渠道支持系统中所处理信息的保密性、完整性或可用性的事件。	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。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。

编号	具体控制要求	客户关注点	华为云的应答
2.3.4.8.	客户端远程访问系统 (RAS) 远程访问是指受监管实体通过定制应用程序（通常使用专用链路）向其客户提供的用于开展业务的访问权限。 提供远程访问服务以开展货币业务的实体必须为其系统配备硬件安全模块，该模块至少应符合 FIPS-140-2（联邦信息处理标准）安全标准。该模块必须是专用设备，且与任何其他信息处理、计算机安全、数据传输和/或接收、通信、交换、路由、网关、远程访问服务器 (RAS) 和/或集中器设备或组件完全分离和独立。	金融机构提供远程访问服务以开展货币业务的，必须为其系统配备硬件安全模块。	客户可以使用华为云提供的密码安全中心（Data Encryption Workshop，简称DEW）服务来保障远程访问的安全，DEW的密钥管理功能提供满足哥伦比亚监管要求的信息处理、计算机安全、数据传输和/或接收等条款。
2.3.4.9.2.	每年至少对用于通过此渠道进行货币交易的设备、装置和通信渠道进行两次漏洞和渗透测试。但是，如果平台发生任何影响渠道安全性的变更，则必须进行额外的测试。	客户应建立并实施漏洞分析与渗透测试。	为配合客户满足监管要求： 1. 华为云的云监控服务（Cloud Eye Service，简称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 防护（Anti-DDoS Service，简称AAD）、Web 应用防火墙（Web Application Firewall，简称WAF）、数据库安全服务（Database Security Service，简称DBSS）、云审计服务（Cloud TraceService，简称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，

编号	具体控制要求	客户关注点	华为云的应答
			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。华为云已与合作伙伴联合推出了主机入侵检测、Web 应用防火墙、主机漏洞检测、网页防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力。 4. 华为云产品安全事件响应团队（CSIRT）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 CSIRT 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，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。
2.3.5.1	维护三个独立的环境：一个用于软件开发，一个用于测试，第三个用于生产系统。在任何情况下，一个环境的性能和安全性都不能影响其他环境。	金融机构应建立环境隔离 (开发/测试/生产)。	华为云目前将生产及非生产环境划分为多个安全区域，包括：DMZ区、公共服务区（Public Service）、资源交付区（POD - Point of Delivery）、数据存储区（OBS - Object - Based Storage）、运维管理区（OM - Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根

编号	具体控制要求	客户关注点	华为云的应答
			据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。
2.3.6	外包 根据外包或第三方模式，与自然人或法人签订合同，委托其部分或全部处理不同渠道或渠道中使用的设备，或者在其活动过程中接触到实体或其客户的机密信息的实体 2.3.6.1.在与第三方签订的合同中，至少包括以下方面： 2.3.6.1.1.信息所有权。 2.3.6.1.2.对所用软件的限制。 2.3.6.1.3.将应用计算机和物理安全标准。 2.3.6.1.4.发现设备或信息被更改或操纵的证据时应遵循的程序。 2.3.6.1.5.服务结束后，第三方对所处理信息的交付及其销毁的程序和控制。实体必须有必要的程序来验证是否遵守了本小节中规定的义务，这些程序必须提前报告给内部审计或履行其职能的任何人。 2.3.6.2.要求签约的第三方有适当记录的应急和连续性计划。实体必须验证与商定服务相关的计划是否在商定的条件下运行。 2.3.6.3.制定程序，明确合同第三方官员的身份。 2.3.6.4.为与签约第三方发送和接收机密信息实施强大的加密机制。	金融机构应建立外包管理与合规证明验证体系。	华为云提供了线上的《华为云用户协议》以及《华为云云服务等级协议》，其中规定了所提供服务和水平，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。 华为云定期接受第三方机构的审核，以验证其安全控制措施的有效性。相关的合规证明（如 PCI DSS、SOC 1/2/3 报告）可根据客户要求提供，以证明其符合金融行业标准。

5.5 P1-T4-C5 信息安全和网络安全管理的最低要求

P1-T4-C5 <信息安全和网络安全管理的最低要求>章节通过修订金融审计管理体系（SARO），细化了业务连续性管理与网络安全风险的最低要求，规定了机构在面对信息安全威胁时必须建立的预防、检测及响应机制。该章节内容整合了外部通函 C.E. 007/2018（Circular Externa 007 de 2018）的内容。

金融机构在遵循<信息安全和网络安全管理的最低要求>的要求时，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 <信息安全和网络安全管理的最低要求> 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。

编号	具体控制要求	客户关注点	华为云的应答
3.4	实施控制措施，以减轻可能影响机密信息（无论是在存储状态还是传输过程中）安全的风险。	客户应实施控制措施，以减轻可能影响机密信息（无论是在存储状态还是传输过程中）安全的风险。	1. 客户可以使用华为云提供的云硬盘（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）等多个服务来实现机密信息存储安全，这些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密码安全中心（Data Encryption Workshop, 简称DEW）的密钥管理功能，由DEW进行密钥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，助力客户云上数据的安全。 2. 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。针对客户业务混合云部署和全球化布局的场景，可以

编号	具体控制要求	客户关注点	华为云的应答
			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数据传输安全。
3.5	采用适当的身份验证机制，并明确划分具有管理员权限或提供远程支持的用户的角色和职责。这样做是为了降低信息安全风险。	客户应采用适当的身份验证机制，并明确划分具有管理员权限或提供远程支持的用户的角色和职责。	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还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。IAM同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM默认启用多因子认证，保证用户账号安全。
3.6	制定信息保留和最终销毁程序。	客户应制定信息保留和最终销毁程序。	1. 为保障客户安全的处理云上数据，华为云对数据从数据创建、数据存储、数据使用、数据共享、数据归档到数据销毁全生命周期的各阶段进行层层防护，并通过友好的操作界面和接口，方便客户使用与集成，满足不同行业客户对数据安全的个性化需求。 2. 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

编号	具体控制要求	客户关注点	华为云的应答
			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。针对于数据安全删除，华为云在客户确认删除数据后，会对指定的数据及其所有副本进行全面的清除，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。
3.8	在软件开发生命周期中，包括处理实体或金融消费者机密信息的 Web 服务和应用程序（从需求收集等初始阶段到相关的安全测试和生产），考虑与信息安全的方面，以减轻所述风险。	客户应在软件开发生命周期中，考虑与信息安全的方面，以减轻所述风险。	1. 华为云追求新的DevOps流程，具有快速持续迭代能力，集成了华为安全开发生命周期(SDL)。此外，逐步形成高度自动化的新安全生命周期管理方法和流程，称为DevSecOps，与云安全工程能力和工具链一起确保DevSecOps的顺利灵活实施。华为云对开发环境进行分层管理，并实施物理隔离、逻辑隔离、访问控制、数据传输通道审批和审计等保护措施。 2. 华为云通过完善的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，确保信息安全在信息系统安全生命周期中得到设计和实

编号	具体控制要求	客户关注点	华为云的应答
			现。 3. 客户可以使用华为云提供的代码检查（CodeArts Check）是基于云端实现代码质量管理的 服务，软件开发者可在编码完 成后执行多语言的代码静态检 查和安全检查，获取全面的质 量报告，并提供缺陷的改进建 议和趋势分析，有效管控代码 质量，帮助产品成功。客 户还可以使用华为云提供代码托管（CodeArts Repo），这 是面向软件开发者的基于Git 的在线代码托管服务，是具备安全管控、成员/权限管理、分支保护/合并、在线编辑、统计服务等功能的云端代码仓库，CodeArts Repo支持版本管理和标签管理，标签（tag）是Git提供的帮助团队进行版本管理的工具，用户可以使用Git标签标记提交，从而将项目中的重要版本管理起来，以便日后精确检索历史版本。
3.9	在与关键第三方签订的合同中，应包含有关信息安全和网络安全风险管理政策的采纳和遵守的相关措施和义务。	客户应在与关键第三方签订的合同中，包含有关信息安全和网络安全风险管理政策的采纳和遵守的相关措施和义务。	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。
3.10	定期核查根据本章第 3.9 款确定的义务和措施的遵守情况，为此，他们可以实施适当的机制。	客户定期核查根据本章第 3.9 款确定的义务和措施的遵守情况。	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。

编号	具体控制要求	客户关注点	华为云的应答
4.1.1	建立、维护和记录访问控制（逻辑、物理和程序）和身份管理，前提是人们只能在必要时拥有其工作所需的资源。	客户应建立、维护和记录访问控制和身份管理，员工只能在必要时拥有其工作所需的资源。	客户可以使用华为云的 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。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。IAM可以避免与其他用户共享账号密钥，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、访问控制列表来助力用户账户的安全。
4.1.3	管理和记录技术平台的安全。	客户应管理和记录技术平台的安全。	华为云的 云审计服务（Cloud TraceService，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。
4.1.4	识别并尽可能衡量可能影响实体的新兴网络风险，并建立控制措施以减轻这些风险。	客户应识别并尽可能衡量可能影响实体的新兴网络风险，并建立控制措施以减轻这些风险。	为配合客户满足监管要求：华为云的 云监控服务（Cloud Eye Service，简称CES） 为客户提供一个针对弹性云服务、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DDoS防护 Anti-DDoS流量清洗服务、DDoS防护（Anti-DDoS Service，简称AAD）、Web应用防火墙（Web Application Firewall，简称WAF）、数据库安全服务（Database Security Service，简称DBSS）、云审计服务（Cloud TraceService，简称
4.1.7	拥有能够关联事件并发出安全事件警报的工具或服务，例如 SIEM。	客户应拥有能够关联事件并发出安全事件警报的工具或服务。	
4.2.2	管理支持关键信息资产且暴露在网络空间中的平台的漏洞。	客户应管理支持关键信息资产且暴露在网络空间中的平台的漏洞。	

编号	具体控制要求	客户关注点	华为云的应答
4.2.3	对您的技术平台进行持续监控，以便识别可能表明实体遭受网络攻击的异常行为。	客户应对技术平台进行持续监控，以便识别可能表明实体遭受网络攻击的异常行为。	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。华为云的安全云脑（SecMaster）实现中央安全日志管理和监控，基于云原生安全，为客户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。安全云脑支持一键接入 WAF、HSS、CFW 等多种云产品的日志数据。接入后，可以统一管理日志信息，以及检索并分析所有收集到的日志，对告警进行集中分析。同时依靠云原生能力，安全云脑整合了 HSS、云防火墙、WAF、安全组等各类产品的处置与封禁能力，可以为企业客户提供集中处置、一键处置、自动处置，极大的提升威胁响应效率。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。华为产品安全事件响应团队（PSIRT）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 和华为云安全运营中心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

编号	具体控制要求	客户关注点	华为云的应答
			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。

6 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 Service (HSS)	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主机安全风险，实时发现并阻止黑客入侵行为。 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。	资产管理 漏洞管理 入侵检测

产品名称	产品介绍	核心功能
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
密码安全中心 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
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、存储或传输、使用、交换或销毁的安全。	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
云证书与管理服务 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侵、访问或盗取的风险。	证书管理
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

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	VBS 为云硬盘创建在线永久增量备份，并对加	数据备份

Volume Backup Service (VBS)	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。	
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

● 管理与监督

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）账号，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)	为客户提供云账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，以便保存更长时间的操作记录，保障数据主体的知情权、实现快速查找。	安全审计
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	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

7 结语

本文描述了华为云为客户提供的云服务如何遵从哥伦比亚金融行业监管要求，并表明华为云遵守哥伦比亚金融监管局（SFC）发布的重点监管要求，有助于客户详细了解华为云对哥伦比亚金融行业监管要求方面的遵从性，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、构建和部署遵从哥伦比亚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。

本白皮书仅供一般性参考，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，并负责确保在使用华为云时对相关哥伦比亚金融行业监管要求的遵从性。

8 版本历史

日期	版本	描述
2026 年 7 月	1.0	首次发布