华为云土耳其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



华为云计算技术有限公司

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



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 网络安全监管要求简介 1
1.3 名词定义 2
2 华为云安全合规 3
3 华为云责任共担模型 6
4 华为云全球基础设施 8
5 华为云如何遵从及协助客户满足BDDK《银行信息系统和电子银行服务条例》的要求 9
5.1 信息安全管理 9
5.2 系统开发和变更管理 21
5.3 信息系统的连续性和可访问性管理 24
5.4 外部服务采购 29
6 华为云如何遵从及协助客户满足BDDK《关于支付机构和电子货币机构信息系统管理和审计的公告》的要求 31
7 华为云如何遵从及协助客户满足SPK《管理程序和原则》的要求 42
8 华为云为客户提供的安全与隐私保护相关的云服务 64
9 结语 68
10 版本历史 69

1 概述

1.1 背景与发布目的

随着信息科技的迅猛发展，在金融科技的影响下，土耳其金融生态和资本市场都出现了新的变化，第三方支付、网络借贷、智能投顾、保险科技等新金融业态的出现改变了土耳其的金融生态。面对金融科技发展的挑战，土耳其金融纷纷加速数字化转型，在数字化转型监管体系、技术运用、开放银行建设、产品创新等方面，均走在时代的前列。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，如将业务部署在云环境中运行。为了规范金融行业对于信息科技的运用，金融监管机构针对金融机构如何进行科技风险管理、合规管理等方面提出了一系列监管要求和指引。

华为云作为云服务提供商，致力于协助客户满足这些监管要求，持续为客户提供遵从监管要求的云服务及业务运行环境。本文将针对客户在使用云服务时通常需遵循的土耳其网络安全监管要求，详细阐述华为云将如何协助其满足这些监管要求。

1.2 网络安全监管要求简介

土耳其银行监督管理局（Bankacılık Düzenleme ve Denetleme Kurumu，BDDK）是土耳其银行业和传统金融体系的最高监管机构。它主要负责向银行、信贷公司、租赁及保理公司颁发执照并实施日常监督，核心职责是维护银行体系的稳定、防范系统性金融风险并保护存款人利益。同时，BDDK 在规范金融数字化转型中扮演关键角色，对银行信息系统安全、电子银行服务以及反洗钱合规有着极高且严苛的本地化监管要求。

- **《银行信息系统和电子银行服务条例》**：本条例发布于 2020 年 3 月 15 日，规定银行在开展活动时使用的信息系统的管理要求，并作为提供电子银行服务的基础，和与之相关的风险管理所应采取的最低限度的程序和原则。
- **《关于支付机构和电子货币机构信息系统管理和审计的公告》**：专为金融科技（FinTech）企业、支付服务商及电子货币发行商量身定制，旨在规范非银金融机构的 IT 风险管理。公告要求这些机构必须建立与其业务规模相匹配的信息系统管理框架，涵盖严格的数据加密、访问控制、业务连续性计划以及灾难恢复机制。

土耳其资本市场委员会（Sermaye Piyasası Kurulu，SPK）是土耳其资本市场的最高证券监管机构。它专职负责监管股票、债券、衍生品等证券市场，对交易所、资产管理

版权所有 © 华为云计算技术有限公司

公司、投资银行、经纪商及上市公司进行全面合规审计。SPK 的核心宗旨是确保资本市场的公开、透明与公平交易，通过严厉打击内幕交易和市场操纵行为，切实维护广大投资者的合法权益。

- 《管理程序和原则》：是土耳其资本市场委员会（SPK）2025 年 3 月发布的确保相关机构、组织和合作伙伴的信息系统管理的方法和基础。旨在确保信息系统运行的正当性、准确性。内容包含信息系统管理控制措施、风险管理流程和程序、信息系统运行规则，开发与维护要求等。

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。

- **信息系统**

  收集、处理、储存、分配和利用信息的人力资源、业务活动和流程，以及与之互动的信息技术；

- **二级中心**

  一个结构，其中二级系统的安装方式是随时可以使用，在主要系统出现任何中断的情况下，人员可以工作，并且不存在与一级中心相同的风险。

- **主要系统**

  指用于存储法律法规中列出的信息的系统，包括用于执行活动的基础设施、硬件、软件和数据所构成的完整系统，这些信息应以安全的方式存储在系统中，并可随时提供访问。

- **次要系统**

  不直接承载核心使命，为主要系统提供支撑、备份或辅助功能的从属系统。

- **网络安全事件**

  侵犯信息系统或数据的保密性、完整性或可访问性的事件。

- **信息安全漏洞**

  任何破坏或企图破坏信息系统或此类系统处理的信息的机密性、完整性或可用性的行为。

- **信息资产**

  机构、组织和合伙企业在履行法律和相关法规规定的职责时所使用的数据，以及用于生成、处理、传输和存储这些数据的硬件和软件。

版权所有 © 华为云计算技术有限公司

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系的持续运行。
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，由国际标准化组织(ISO)和国际电工委员会(IEC)联合发布，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。
TL9000&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。 TL9000是一个建立在ISO 9001基础上的，由全球电信业优

版权所有 © 华为云计算技术有限公司

认证	描述
	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	BS 10012是BSI发布的个人信息数据管理体系标准，BS 10012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

 版权所有 © 华为云计算技术有限公司

认证	描述
	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。

 版权所有 © 华为云计算技术有限公司

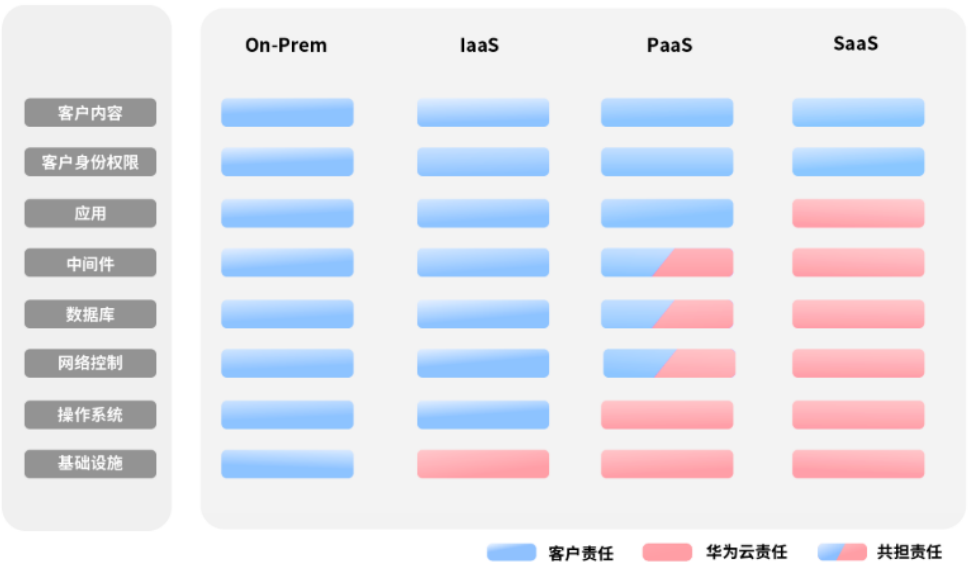
3 华为云责任共担模型

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

版权所有 © 华为云计算技术有限公司

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。

 版权所有 © 华为云计算技术有限公司

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。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 土耳其地理区域（Region）和可用区（AZ）示例



版权所有 © 华为云计算技术有限公司

5 华为云如何遵从及协助客户满足 BDDK《银行信息系统和电子银行服务条例》的要求

《银行信息系统和电子银行服务条例》的目的是规范银行在开展活动时使用的信息系统的管理，在开展电子银行服务和管理相关风险时应建立的最低程序和原则，以及应建立的信息系统控制。其该条例涵盖了系统风险管理和控制以及电子银行服务的安全要求。

由于华为云未在提供金融服务，因此对《银行业信息系统和电子银行服务管理规定》不承担任何直接义务。因此，下文将对《银行业信息系统与电子银行服务管理规定》中的管控要求进行总结，并详细介绍华为云作为云服务提供商如何帮助客户满足这些管控要求。

5.1 信息安全管理

编号	具体控制要求	客户关注点	华为云的应答
第8 条	（1）银行应制定信息安全管理体系，信息安全管理体系本质上要求以国家或国际标准或最佳实践为参考。并涵盖以下活动： a) 定期进行与信息资产相关的威胁和风险评估工作和活动； 和 b) 信息资产的分类、资产所有者的确定以及采取适合资产类别的安全措施； 和 c) 监测和报告违反信息安全的事件和事件； 和 d) 在银行提供的银行服务过程中，确保建立符合职责分离原则的有效身份验证和访问管理	1. 客户应建立网络安全政策与程序，可参考最佳实践和国际安全标准。此外，应在其网络安全要求中明确资产管理、网络安全评估、网络安全意识培训、合规性、漏洞管理以及业务连续性的安全要求。 2. 客户应根据计划的频率或外部监管的变化	华为云参照 ISO 27001 构建了完善的信息安全管理体系，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。全方位保护客户系统和数据的保密性、完整性和可用性。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。华为云至少每年审查一次网络安全管理策略和流程，并根据需要予以更 新，以反映业务目标或风险环境的变更情况。政策及流程的变更需要获得高级管理层的审批。同时华为云有专门的审计团队定期评估策略、规程及配套措施

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	e)… （3）信息安全管理体系在银行的总体应用方式由信息安全政策、程序和流程文件来确定和规范。 银行的信息安全政策由董事会批准，并确保向银行所有员工传达。 （4）信息安全政策由信息安全委员会以董事会名义制定并实施。 信息安全委员会由指定董事或总经理担任主席，并由信息安全主管协调。 （5）信息安全政策、程序和流程文件每年至少审核一次。 确保在重大安全事件、新的安全漏洞或技术基础设施发生重大变化后也对其进行单独审查。 （6）在银行组织内部，信息系统安全职能是独立于信息系统职能而组建和组织的，由负责信息系统的高层管理者和向其报告的单位组成。	定期对网络安全政策和程序进行审查和更新，并保留修订记录。 3. 客户方的董事会应以明确的方式支持网络安全目标。 4. 客户应定义和批准网络安全角色及通用职责，确保各职责间没有利益冲突。	和指标的符合性和有效性，向最高管理层报告调查的结果和建议。此外，华为云重点关注员工以及外包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。
第9条	(1) 银行应采取措施，确保在数据传输、传输、处理、存储和备份等各种环境中，用于开展银行业务的数据的保密性。无论数据存储介质是纸质还是电子形式，所采取的措施都必须与所保护数据的保密级别相适应，并在必要时建立额外的控制措施。如果包含数据的介质或设备被停用，则应根据其保密级别安全销毁其中包含的数据。 (2) 为确保数据隐私，加密技术应采用当前情况下可靠性依然良好且适用于现有技术的算法。加密密钥的长度应足以保证在相关算法的有效使用期间内无法破解，其有效期根据相关数据或操作的关键级别确定。一旦发现加密密钥已过期或可靠性下降，应立即停止使用。确保	客户对银行活动中使用的数据以及承载、传输、处理、保存和备份数据的所有介质都需要严格保密。同时确保不再使用的数据或设备根据其机密程度安全销毁。 客户应建立密钥管理机制，用于处理加密密钥的生成、保护、归档、恢复和销毁，使数据的机密性和完整性不会受到损害。	华为云为客户提供了**密码安全中心（Data Encryption Workshop，简称DEW）**,其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，助力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拥有主流国际安全认证，助力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。客户应制定安全措施保护通过组织网络传输的信息。客户可使用华为云提供的**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**

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	加密密钥在其整个生命周期内的安全性至关重要，包括安全地创建密钥、向客户和员工提供密钥以及安全地存储密钥。 (3) 在不同安全级别的环境之间传输敏感数据时，必须使用端到端安全通信，并将这些数据以加密形式存储。银行已确保对分配给员工的包含敏感或机密数据的台式机、笔记本电脑和移动设备的内容进行加密，并对服务器进行扫描，以确定连接到网络的服务器设备上是否存在明文形式的敏感数据。		**CC）**，实现不同区域之间业务的互联互通和数据传输安全。 华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流 程，要求存储介质及设备进出机房前需进行登记并得到授权。物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。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清零操作，使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，使其上的数据无法恢复。目前**虚拟专用网络（Virtual Private Network，简称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 **虚拟私有云（Virtual Private Cloud，简称 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（Direct Connect，简称 DC）**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。此外，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 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。 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。同时，华为云使用密钥管理服务（KMS）管理 RDS和 **对象存储服务（Object Storage Service，简称OBS）**用户的主密钥，RDS 和 OBS 通过调用 KMS 的内部接口请求使用主密钥用于加解密工作。 华为云在信息传输过程中使用安全加密信道（如 HTTPS），对存储的静态数据使用安全加密算法进行加密保护，确保不同状态下的数据的机密性。使用数字签名和

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性。 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如下方式提供： a.**虚拟专用网络（Virtual Private Network，简称VPN）**：用于在远端网络和 **虚拟私有云（Virtual Private Cloud，简称 VPC）** 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云。目前，华为云采用硬件实现的 IKE（密钥交换协议）和 IPSecVPN 结合的方法对数据传输通道进行加密。 b. 应用层 TLS 与证书管理：华为云服务提供 REST 和 Highway 方式进行数据传输。以上数据传输方式均支持使用传输。
第11条	(1)银行有义务确保对信息资产的访问采用合适的身份验证方法，并遵循根据职责分离原则确定的访问控制。 (2)银行应建立信息系统用户身份验证机制，并采取措施确保从会话开始到结束的身份验证数据的准确性。 (3)银行应采取身份验证数据加密存储、身份认证数据传输加密等措施确保身份认证数据的安全。 (4)身份认证机制应考虑以下功能： -记录并保存身份验证数据数据库的操作日志； -设置身份验证失败的阈值和警告，对多次尝试登录失败的账号进行锁定； -会话超时终止策略； -银行应禁止多个用户使用同一用户帐户或一个用户同时打开不同的会话，除非信息安全主管批准； -... (5)银行应依据职责分离的原则控制和限制访问权限的分配和使用，并每年审核一次。 (6)人员职务变动等人事变动	客户应建立身份和访问控制管理机制。客户应实施基于角色的访问控制和权限管理，并符合按需知晓最小权限原则。客户应通过日志监控异常活动，并定期审查和分析。 客户应根据计划的频率定期对身份与访问管理的网络安全要求进行审查和更新。确保在员工离职或业务变更后对其相关用户权限进行审查和回收。 此外，应定期审视账号权限范围，确保用户权限申请、变更或回收时，均可以按照身份和访问控制策略进行及时的管理。 客户应建立特权账号的管理机制，密切监督特权账号的使用。客户可通过华为云统一身份认	客户可使用华为云的**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。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。同时，客户应建立用户访问管理机制，基于最小权限原则进行访问系统权限限制 和监督。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。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。 华为云制定了公司账户账号权限管理的要求，规范华为云员工在申请、维护和注销权限时应遵循的流程。同时，华为云制定了运维账号的生命周期管理，包括帐号的开销户管理、帐号责任人/使用人管理、口令管理、开销户监控管理等，帐号一旦建立，立即纳入帐号管理员的日常维护管理工作。所有运维帐号，所有设备及应用的帐号均实现统一管理，并通过统一审计

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	后，及时办理相关用户账户的删除、暂停、撤销、变更用户授权等交易。 (7)银行应制定特权账号管理规范，管理特权访问权限的分配和使用。 (8)银行应针对临时授权账户应保存相关的账户操作记录。 (9)银行应监测各类用户账户的使用情况，实施适当的管理措施确保账户得到与账户权限的敏感性相称的保护。同时在平台中预设异常操作规则，在发现异常操作时做出报警。 (10)除业务强制性要求以及信息安全主管另有批准外，银行人员或外部服务提供商不得拥有本地管理员权限。 (11)银行应监测用户账户的使用情况，发现和阻止异常账户或不活跃账户。	证服务可以更有效地细化管理特权账户。	平台集中监控，并且进行自动审计。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。此外，针对华为云云平台账号，华为云制定了公有云账号权限管理要求及流程，明确了对账号的分类管理和访问控制策略。对云服务的访问通过统一身份认证服务（IAM）对用户进行访问控制和权限管理。 华为云制定了密码策略及账号口令安全相关管理规范，包括规定密码长度、复杂度、更改周期，密码中不允许包含用户ID，不可使用易被破解的常用口令以及最近 5 次使用过的密码等。对秘密鉴别信息的分配进行管理。新建系统中的账号密码在首次使用前由用户进行更改，当用户需要重置密码时对其身份进行验证。 华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求。华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，特权账号被严格纳管回收。特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。仅在员工职责所需时，对其授予特权或应急账号。所有特权或应急账号的申请需要经过多级的评审和批准。华为云仅会在得到客户授权后登陆租户的控制台或者资源实例协助客户进行维护。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。
第13条	（1）银行应建立与其信息系统和活动的规模和复杂程度相称的有效跟踪机制，用于跟踪其信息系统内发生的交易和事件。跟踪记录至少应包含以下信息，并应根据交易性质提供适当的细节和内容： a) 创建该记录的系统， b) 记录创建的日期、时间和时区信息， c) 指示所做更改类型的信息，以及创建该记录的交易或事件。 c) 指示与该记录关联的唯一用户或系统的信息。 （2）所建立的日志记录机制	客户应根据信息系统和活动的规模和复杂性制定日志记录机制，实施适当的管理措施保护日志信息和日志记录设施，防止未经授权的访问和修改。 客户应定期审查事件日志，并向责任人员报告可疑事件和检测到的异常情况，及时检测安全和事件。客户应建立监控平台对各个系统的安全日志进行持续监控和必要	华为云的**云审计服务（Cloud TraceService，简称CTS）**，可提供对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。客户可根据企业对日志保留期限的要求购买不同规格的**对象存储服务（Object Storage Service，简称OBS）**以实现日志的备份。华为云提供的**云日志服务（Log Tank Service，简称LTS）**提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务，客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该 IP地址的请求。华为云建立了安全日志管理规范，规范了华为云应用系

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	应当能够对信息安全事件进行后续调查，并获取有关这些事件的可靠证据。 （3）信息系统内发生的导致银行活动记录发生变化的交易记录，以及涉及访问、查询、查看、复制或修改敏感或机密数据的交易记录，以及与授予、修改或撤销对关键信息资产的访问权限相关的活动记录，以及对这些资产的未经授权的访问尝试记录，均在银行保存至少五年。 （4）银行通过网络服务、API或类似方法查询其他机构或组织所持有的数据的记录及其查询目的，由银行保存五年，并至少每月报告一次，以便调查是否存在未经授权或未经许可的查询，并满足调查结果的要求。 （5）跟踪记录在安全的环境中进行备份，并保存在银行，以便在需要时能够在合理的时间内从这些备份中进行恢复和检查。 （6）采用各种技术手段防止日志记录的完整性遭到破坏，并检测任何此类破坏行为。只有获得授权的人员才能根据“需要知道”原则访问日志记录，并且记录系统受到保护，免受任何未经授权的更改和干预。用户不得干扰与其自身活动相关的日志记录，并且采用各种技术手段防止日志记录系统被停止运行，或检测其是否已被停止运行。 （7）银行在预先设定并定期更新的跟踪系统情景框架内，建立流程，对异常情况和风险交易进行定期审查、监控和报告。银行确保生成异常情况和风险交易报告，并由银行审计部门对报告结果进行监控。	分析，及时检测和响应安全事态和事件。 客户应确保日志记录至少五年。	统、服务、网络设备安全日志的管理。同时，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，以确保支撑网络安全事件回溯，日志会保留合理的期限并实施保护措施避免未经授权的篡改、泄露等安全风险。 为确保日志数据安全，安全日志会进行统一备份或归档，并依照数据安全管理的要求，限制安全日志使用的申请及权限，仅允许授权人员因必要原因进行安全日志的查询，确保受控使用。 华为云遵从法律法规要求，具备集中、完整的日志审计系统，具备强大的数据保存及查询能力，确保所有日志内容保存时间超过 6 个月。内部人员运维操作均被日志平台采集并记录。 对于集中存储安全日志的日志分析平台，系统管理员会定期例行对采集状态、存储状态进行检查，保证安全日志的可用性。 华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理。异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	（8）银行应确保外部服务提供商保存的日志记录符合其标准，并且银行可以访问这些日志记录。		
第14条	(1) 银行应建立必要的网络安全控制体系，以应对来自自身企业网络和其他外部网络的威胁。 (2)银行将银行内部网络进行分段，通过将银行内部网络的具有不同安全敏感性的子网段分开来确保受控通道，维护不同网段之间数据流量的安全，确保只有经过授权的设备才可以连接到内部网络。 (3)银行确保关键系统部署在内部网络中，不能通过互联网直接访问。 (4)银行应定期评估与关键网络的连接，及时终止不必要的连接。 (5)除非经信息安全主管特别批准，银行人员和外部服务提供商未经主管人员批准不得从外部远程访问银行内部应用程序和系统。远程访问时，应采用多因素认证并保留访问日志。此外，应规定用户远程访问的时间和可用于连接的设备。 (6)银行应定期检查通过互联网或银行外网可访问的服务器和系统，对业务不再需要的服务器和系统应及时移动到银行内网。 (7)银行应限制从内网传输至外网的流量，记录会话并对超长会话发出警告。	客户需对其网络进行安全区域划分和隔离，针对不同安全域之间的访问进行严格的管控。 客户应明确对远程访问的安全管理要求，要求所有远程登录（用户和管理员）都通过安全通道进行，和采取适当的身份验证方法来控制远程用户的访问。 客户应记录远程访问的访问日志。	1. 华为云可帮助客户构建网络安全防护体系，保障客户云服务的安全。通过**虚拟私有云（Virtual Private Cloud，简称 VPC）**对关键网络分区进行划分和隔离 。部署**Web应用防火墙 （Web Application Firewall，简称WAF）**应对 Web攻击以保护部署在 DMZ 区、面向外网的 Web 应用服务和系统。客户可通过 Anti DDoS 流量清洗服务实现对网络层和应用层的 DDoS 攻击防护，Anti DDoS 为客户提供精细化的防护服务，客户可以根据业务的应用类型，配置流量阈值参数，并通过实时告警功能查 看攻击和防御状态。 2. 客户可使用华为云统一身份认证服务，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。修改密码、手机等敏感信息时，**统一身份认证服务（Identity and Access Management，简称IAM）**默认启用多因子认证，保用户账号安全。华为云的**云审计服务（Cloud TraceService，简称CTS）**为用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。华为云参考安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域、业务层面的划分和隔离。安全区域内部的节点具有相同的安全等级。华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，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。华为云数据中心主要分为以下五个，重要安全区域：DMZ 区、公共服务区（Public Service）、资源交付区（POD– Point

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			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。 3. 华为云对于生产及非生产环境使用物理和逻辑控制并用的隔离手段，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。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（Direct Connect，简称DC）**，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 的 ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。 4. 在每个云数据中心边界部署华为专业的Anti-DDoS 设备来完成对异常和超大流量攻击的检测及清 洗。华为云在网络边界部署了 IPS 设备， 包括但不限于外网边界、安全区域边界和租户空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS可以提供信息帮助定位 和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程 序和网络基础设施安全。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			5. 华为云所有接入华为内部网络包括有线办公网络和无线办公网络的计算机设备均必须安装公司安全软件，员工可通过公司安全软件从外部网络接入华为内部办公网络。此外，未经批准，在华为办公区域内，不允许接入非华为提供的无线网络，禁止在华为办公区域私自搭建无线网络或将测试无线网络接入公司办公网络，若有业务需 求，必须经过业务主管和 IT 管理部门评估和审核批准。此外，华为云根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。登录权限分为：核心网络、接入网络、安全设备、业务系统、数据库系 统、硬件维护、监控维护等。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，其他设备无权访问。
第16 条	(1)银行应建立漏洞和补丁管理的策略和流程。 (2)针对供应商无法再进行补丁更新且无法通过补偿控制保障合理水平安全性的系统、软件和设备，银行应停止使用。 (3)银行对联网系统和设备采用自动安全漏洞扫描工具。对于检测到的每个安全漏洞，优先列出最严重的安全漏洞的报告提交给银行信息安全主管和负责检测到漏洞的系统的系统管理员。 (4)银行有义务持续监控其台式机、笔记本电脑和服务器，并检测其中加载的恶意软件。	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。	客户可使用专门的自动化漏扫工具进行漏洞扫描工作。根据漏洞的重要程度，定义并分配时间范围，在定义的响应时间内完成漏洞修复。客户应将漏洞扫描的结果与相关部门报告，确定修复的建议方案。 华为云**镜像服务（Image Management Service，简称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。 华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，基于业界最佳实践 CVSS（Common Vulnerability Scoring System）对漏洞进行严重级别的评估，并结合漏洞在华为云中被利用的风险评估结果决定处理优先等 级，制定并落实漏洞修复方案或规避措施。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。华为云内外部的安全团队开展漏洞扫描活动需通过常规变更评审后才可进行漏洞扫描，并需要告知测试工具、目标系统、目的等，华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			华为产品安全事件响应团队（PSIRT – Product Security Incident Response Team）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尽快修复，降低对租户业务造成影响的风险。基于华为云责任共担模型，华为云承担研发并运维运营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层的多维立体安全防护体系，并保障其运维运营安全。 华为云建立安全补丁管理的流程，保证安全补丁在 IT 安全标准规定的期限内完成安装。同时，华为云制定了漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，不断优化云平台及云产品默认安全配置、及时在规定的期限内应用修补措施或补丁、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等。 华为云桌面终端标准镜像内默认提供防病毒软件，员工默认无法对防病毒软件进行禁用操作。在电子邮件保护方面，华为云的相关人员遵循华为公司针对 Email 系统、移动邮件使用、网络接入与使用的安全控制要求。
第17 条	（1）主要系统存放于数据中心、服务器机房和网络设备机房等安全区域，并设有适当的安全屏障和访问控制措施。只有获得授权的人员才能进入这些区域，且访问权限会定期审查和更新。 （2）银行在选择数据中心选址时会考虑自然风险和环境威胁。银行确保建筑物内没有任何标志或信息会泄露其内部设有计算设施。 （3）该银行使用系统和传感器来监测可能对数据中心运行产生负面影响的环境条件，例如停电、火灾、烟雾、温度、水、灰尘和湿度，并定期对其进行维护。 （4）除第一款授权人员外，	客户应对其主要系统所位于的数据中心、系统机房、网络机房等安全区域，制定并实施物理安全防护措施，客户应实施按职责授权个人的物理访问控制措施。应定期审查数据中心和敏感区域的访问记录，防止未经授权的访问，并确保及时删除不必要的访问权限。 客户应根据建筑物、ICT 系统和操作的重要性实施环	华为云已制定并实施完善的物理和环境安全防护策略、规程和措施。华为云信息安全环境采用分区管 理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。 华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了全天候保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	任何银行人员、访客、外部服务提供商或承包公司人员进入数据中心和主要系统均须经过审批机制，其在数据中心工作期间的活动受到严密监控，并始终有人陪同。对数据中心和服务器机房的访问请求和审批，以及在这些访问范围内进行的交易、出入情况均会被记录。这些区域均安装了无盲区的摄像头录像系统，录像至少保存一年。摄像头录像系统所记录的图像会备份到其他位置。	境安全保护措施。实施电力保障、温湿度控制、消防能力、例行监控、供水排水和防静电方面的要求。	理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，使非授权人员不可访问数据中心。 华为云对电气、消防安全执行严格管控。华为云数据中心采用多级保护方案保障业务 7*24 小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之 需。并配备了不间断电源(UPS)，提供短期备用电力供应。针对温度、水、灰尘和湿度通过精密空调、集中加湿器自动调节，华为云数据中心机房温湿度保持在设备运行所允许的范围内，使设备元器件处于良好运行状态。机柜冷热通道有合理的布置，利用架空地板下空间作为静压箱来给机柜送风，并设置了冷通道密闭，以防止局部热点。
第18条	(1) 银行应建立网络安全事件管理和网络安全事件响应流程，以应对和监控发生的网络安全事件，旨在最大限度地减少对银行业务的影响，并尽快恢复银行服务的正常运行。银行应设立一名具备足够技术和运营能力的首席安全官 (CSO)，并向监管机构提供该首席安全官的最新联系方式。银行应向监管机构和相关管理部门报告网络安全事件。 （2）公司安全运营经理负责在网络安全事件发生前对 IT 资产进行或安排例行渗透测试，定期监控日志管理系统界面的跟踪日志，检查跟踪日志之间可能产生有意义结果的关联性；并在网络安全事件发生期间，管理业务安全职能部门的响应，并协调业务安全职能部门的相关人员。 （3）为确保网络安全事件得到根据其严重程度进行处理，已制定网络安全事件严重程度分类标准，并制定相应的程序和干预计划，以便	1.客户应制定网络安全事件管理策略，建立安全事件上报和决策流程，并采取适当应对计划和沟通策略。客户应根据事件重要性对网络安全事件进行分级分类。 2.客户应遵循已制定的网络安全事件管理策略，对各个系统的安全日志进行持续监控和必要分析，在事故发生后开展取证、分析原因等活动，及时响应安全事态和事件。 3.客户应明确渗透测试的范围和频率，定期对进行渗透测试。 4.客户应定期进行培训以测试事件响应流程的有效性。 5.客户应制定通告机制，当发生危机事件时，客户应按	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，以确保支撑网络安全事件回溯。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。 华为云内部制定了安全事件管理机制，规范了华为云安全事件响应操作，根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。在事件解决后，会根据具体情况向客户提供事件报告。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。 华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案。同时，华为云每年会在组织内进行业务续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 华为云每半年都会组织内部以及外部具有一定资质的第三方进行对华为云平台范围内的所有的系统及应用进行渗透测试，并

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	在与根据这些标准确定的严重程度相对应的时限内处理和解决每起网络安全事件。针对已制定的干预计划中预见的各种情况，已建立快速、有效且常规的响应流程，以确保各项活动的可靠持续进行。干预计划的功能每年至少进行一次测试，并将测试结果报告给高级管理层。 （4）在干预计划的范围内，应处理快速查找与信息系统相关的事件源头、联系相关部门、确定事件的潜在范围、影响、损害和受影响的客户以及解决事件等流程。 （5）如网络安全事件升级为危机、导致数据泄露或披露，或需要启动信息系统连续性计划或备用中心，银行应立即通知行业安全运营中心（SOC）。如发生导致敏感或个人数据泄露或披露的网络安全事件，银行应在评估后通知客户。 （6）对于造成银行服务严重中断或故障的重大网络事件，银行有义务进行根本原因和影响分析，采取补救措施防止类似事件再次发生，并将所做工作报告给行业安全评估办公室。 （7）银行应至少每年进行一次渗透测试，由不参与银行通过其信息系统提供的服务的设计、开发、实施或执行的独立团队进行测试。 （8）银行有义务按照其确定的程序和原则，提供有关其在银行业中发现或了解到的新型网络威胁、恶意软件、网络事件或新型欺诈手段的信息，并指定一名可随时联系的联系人，以确保在打击欺诈方面尽早介入。	照本规定的要求向 SOME 报告。如果发生了个人数据泄露事件，应在评估时间后通知银行的客户。银行应指定一名 7*24 小时联系人响应监管当 局。	对渗透测试的结果进行跟进与整改，渗透测试报告及跟进情况会通过内部审计以及外部认证机构核查。

 版权所有 © 华为云计算技术有限公司

5.2 系统开发和变更管理

编号	具体控制要求	客户关注点	华为云的应答
第22条	(1) 银行应确保开发、测试和生产环境按照软件开发过程中的职责分离原则相互隔离。系统和应用程序的开发过程应按照职责分离原则进行，以防止源代码由同一人编写和编译并在开发、测试和生产环境之间传输。 （2）软件开发人员只有在确有必要且符合业务需要的情况下，并经过审批机制后，方可访问生产环境。即使在此类情况下，人员在生产环境中执行的操作也会被监控和记录。银行会记录访问生产环境的方法，并以书面形式保存，且必须获得高级管理层的批准。 （3）银行软件开发流程的各个阶段及其过渡条件、文档要求、编码标准，以及业务部门和其他利益相关者参与的阶段及其审批流程均以书面形式确定。确保遵守银行的软件开发生命周期、监管要求和内部政策，包括软件开发流程中的外部服务采购。 （4）为提高软件质量并最大限度地减少安全漏洞，信息安全在整个软件开发生命周期中都得到充分考虑。从软件开发或采购流程的开始，除了确定业务需求和软件预期功能需求外，还需确定安全相关需求，例如授权和访问、身份验证、数据完整性、日志记录和异常管理，并检查银行是否符合安全标准、政策和监管要求。 （5）银行内部开发的或从外部来源采购的可通过互联网访问的应用程序，在安装之前和对这些应用程序进行任何更新之后，都会定期进行	客户应确保其应用开发流程遵循安全系统开发生命周期的方法，在应用安全开发的生命周期中实施安全标准。客户应为每个需求定义适当的验收和测试标准，进行安全测试，确保每个需求都满足组织的信息安全要求。客户应该保证其开发、测试和生产环境相互隔离，并严格管控不同环境的使用。确保只有授权人员才能访问其权限内的环境，访问控制要求应获得银行高层经理的批准。测试环境在操作系统、数据库管理系统、集成应用和系统等方面能够代表生产环境。 客户应确保仅使用受信任的最新第三方组件，与外部软件服务提供商签订服务质量协议。在安装应用程序前应对其进行漏扫，并在后续使用和更新时，定期扫描。客户应执行基于版本控制和发布控制的完整性检查，代码在转移到生产环境时需要获得相关人员的批准。	1. **软件开发生产线（CodeArts）**是华为云面向开发者提供的一站式云端 DevOps 平台。 帮助客户在云端进行项目管理、代码托管、流水线、代码检查、编译构建、部署、测试、发布等，让开发者快速便捷地在云端进行开发。使用 CodeArts 开放的 API 和调用示例，客户可以对项目、工项、成员、代码仓库、流水线等进行管理。通过合理配置 CodeArts IDE Online，客户可以实现安全开发环境的建立和保护。华为云自主研发的一站式测试管理平台测试计划（CodeArts TestPlan）可以满足客户执行系统安全测 试及系统验收测试的需求。 软件开发生产线支持云上开发，提供可视化、可定制的自动交付流水线帮助实现云端可持续交付，同时覆盖软件交付的全生命周期，提供软件研发端到端支持，全面支撑 客户落地 DevOps。软件开发生产线增加多重安全防护功能，保证核心资产安全。客户 可以将自身的安全生命周期嵌入软件开发生产线，形成自动化的 DevSecOps 安全生命 周期管理流程，确保信息安全在开发生命周期中得到设计和实现。 2. 华为云已制定开发安全管理相关制度，对华为云服务在规划、设计、开发、部署、运维和用户支撑环境应遵循的安全编程规范及应用安全开发规范进行了定义。政策及流程的变更需要获得高级管理层的审批。 3. 华为云及相关云服务遵循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，并根据公司的测试用例库完成

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	安全漏洞扫描。 （6）考虑到软件的关键性、风险以及供应商倒闭的可能性，对于由外部公司开发且无法提供源代码的应用程序，需与第三方签订软件保留协议。产品更新和程序修复也包含在保留协议中。 （7）银行确保其软件开发人员接受针对其使用的软件开发环境的安全代码开发方面的培训。 （8）银行软件开发过程中新增的数据定义或对数据定义所做的更改，均需根据信息架构和数据字典进行评估，并进行必要的更新。 (9) 基于版本控制的完整性检查用于防止在软件代码于开发、测试和生产环境之间传输过程中，将未经授权或有害的代码片段插入其中。在传输到生产环境时，需获得相关用户或应用程序所有者的批准。 （10）确保测试环境在操作系统、数据库管理系统、集成应用和系统方面能够代表生产环境，确保测试数据在数量和质量方面能够代表生产环境中进行的操作，并且与客户的生产环境数据分开。		安全测试用例的设计，确保落地，最终保障产品、服务的安全。 4. 华为云严格遵从华为对内发布的安全编码规范。华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时，华为云引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（CI/CD–Continuous Integration，Continuous Deployment）工具链，通过质量门限进行控制，以评估云服务产品的质量。所有云产品、云服务在发布前，均需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。所有云服务发布前都经过了多轮安全测试，包括但不限于Alpha 阶段的认证、鉴权、会话安全等微服务级功能和接口安全测试，Beta 阶段通过对 API 和协议的 fuzzing 测试验证服务集成，Gamma 阶段的数据库安全等安全专项测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。同时，华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如 SecureCat 可以对业界主流的 OS 和 DB 的安全配置进行检查。华为云建立了正式的内部测试及验收措施，以确保仅适当且经过授权的变更被发布至生产环境。 5. 华为云建立了正式的环境隔离机制，对开发环境、测试环境及生产环境实现严格的逻辑隔离，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。并且严格控制未脱敏的数据流入测试环境，避免生产数据或未脱敏的生产数据用于测试，使用完成后需要进行数据清理。
第24条	(1) 银行应建立有效的变更管理流程，以最大限度地减少因变更而可能出现的错误和问题的数量和影响，确保变更得到有效、快速和可控的	客户应建立正式的变更管理程序，根据信息资产的重要性，对变更进行识别、分类和优先级	客户可通过**云审计服务（Cloud TraceService，简称CTS）**作为辅助，CTS 为客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。华为云制定了变更管理程序，管理应用变更和基础

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	实施，并确保变更期间进行的交易在变更后可审计。所有对信息系统要素（例如网络基础设施、硬件、操作系统和软件）以及系统、服务和应用程序配置和参数的变更，均应在变更管理流程框架内发起；变更请求应基于合理的业务需求；并应按照职责分离原则进行授权、测试、实施、记录和文档化。变更必须由已通过适当技术进行身份验证的授权用户执行；必须保留足够的变更日志记录；并且必须定期审查所保存的日志记录。 （2）银行保存信息系统软件组件主版本的记录，并按变更发生的顺序和变更日期记录对信息系统组件所做的变更。 （3）变更管理流程至少包括请求管理、风险评估、授权、变更实施、测试和验证等步骤。在此背景下； a) 变更请求会被记录，只有来自授权人员的变更请求才会被接受，对这些请求进行风险和影响分析，并且对收到的请求进行分类和优先级排序。 b) 为确保变更不会导致安全漏洞，开展了提供最高级别保证的审查活动，包括源代码审查。	排序。应测试已识别的变更，评估其信息安全风险，并在获得授权批准后才可以变更。客户应在变更管理要求中考虑紧急变更的流程，实施变更后退和回滚程序。客户应在变更管理要求中考虑紧急变更的流程。此外，应记录和保存与变更相关的日志。	设施变更，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。在提出变更申请生成后，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。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。 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。此外，华为云针对变更引起现网影响达到事件标准的，要求立刻上报应急小组，进行故障快速恢复。紧急变更均留有记录，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。
第25条	(1) 银行必须将其主要系统和次要系统保留在国内。 （2）无论主要系统的备份编号如何，所有主要系统的备份均视为次要系统，并受第一款规定的约束。 （3）不用于开展银行业务或履行法律法规所规定职责的内部通讯系统、市场监测平台及类似系统不属于主要系统。为使银行使用的任何系统或应用程序不被视为主要系统，不得通过该系统或应	组织采用外部服务提供商用于开展与其提供的服务相关的活动的信息系统及其备份也被视为主要系统和次要系统范围内的信息系统，应保存在国内。	1.客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，使客户内容数据存储在目标位置。当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，使客户只能访问到自己的数据。 2.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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	用程序开展任何业务流程，也不得处理、传输或存储敏感数据或可能被归类为机密的数据。 （4）除支付或信息系统等因交易性质需要与外国互动的银行交易外，银行必须能够通过境外建立的系统进行银行交易，而无需经过任何审批程序，并且即使与境外通信网络连接中断，也能通过其在境内建立的主要和次要系统继续在境内提供银行服务。 （5）如果为主要系统或次要系统范围内的活动而获取外部服务或云计算服务，则外部服务提供商用于开展与其提供的服务相关的活动的信息系统及其备份也被视为主要系统和次要系统范围内的信息系统，并保存在国内。		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。

5.3 信息系统的连续性和可访问性管理

编号	具体控制要求	客户关注点	华为云的应答
第26条	(1) 本行设有IT运营管理职能部门，负责IT基础设施的日常管理和维护，以确保银行服务按照既定的服务级别提供。这些服务的服务级别由各业务部门参与并经其批准后制定，并符合银行战略计划中的目标和业务需求。 （2）银行应建立服务台职能和问题管理系统，以便及时响应IT运行事件，为用户提供技术相关问题的支持，将问题转交给相关IT部门进行调查和解决，记录事件直至报告的问题得到纠正，并进行分析和跟进。 （3）本行实施性能监控流程，以确保对其信息系统的性能进行持续监控，并及时	客户应制定网络安全事件管理策略，建立安全事件上报和决策流程，并采取适当应对计划和沟通策略。客户应遵循已制定的网络安全事件管理策略，对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。 客户应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。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。 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。 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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	报告异常事件。该性能监控流程包含预警功能，以便在问题影响系统性能之前识别并纠正问题，提供符合既定业务目标的容量规划所需信息，并有助于编制工作量预测。 （4）银行应管理和规划其容量，以确保信息技术容量能够满足业务系统战略计划中规定的当前和未来业务需求，并符合既定的服务级别和工作负载预测。银行应确保持续维护和更新容量规划，并管理业务系统服务的性能，以达到或超过约定的服务级别下的性能目标，并对与容量相关的事件和问题进行诊断和解决。 （5）银行有义务采取措施，检测在客户频繁进行交易的日子（例如月底、节假日后、发薪日）是否会出现系统性能下降、容量不足、技术故障等问题，并找出这些问题的根本原因，确保这些问题得到解决。		的响应时限和解决时限。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 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。 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 目前，华为云已制定容量管理相关制度，对华为云容量统筹管理，以此提升华为云资源可用性服务水平和识别资源需求有效性的能力。并通过对华为云日常容量水平的统筹管理，以此指导资源扩减容方案制定。同时制定了管理透明、授权清晰、运作高效的原则，明确各层级组织在数据中心建设及容量管理决策上的授权规则。在容量管理方面，华为云基于容量监控平台实现对物理主机容量分配情况的系统监控。 容量监控小组在平台内配置告警策略，以确保在异常情况发生时，容量监控平台可以自动发送告警邮件至相关产品运维人员或容量经理处进行后续的跟进处理。华为云建立了周例会机制，责任部门在周例会中对本周内出现的资源需求进行评审，评审通过后会相应采取扩容措施。此外，华为云基础设施工程部每月会基于业务实际运营情况对服务的容量配置现状进行分析，对下一月的潜在容量需求进行分析预估，分析及预估结果会记录在月度分析报告内。华为云同时建立了正式的扩容审核流程，业务部门需通过统一资源管理平台提出申请并获取计划委员会的审批后才可以执行资源扩容。
第27条	(1) 为防止任何硬件或软件组件发生故障导致系统或大部分银行业务无法正常运行，银行有义务为关键硬件和系统建立冗余运行或备用方案。在确定哪些硬件和系统属于关键硬件和系统时，应	客户应制定备份与恢复的安全管理策略，定义组织对信息、软件和系统备份的要求。 客户需根据业务需求自行制定恢复测	华为云提供了多种有不同侧重的产品和服务。如果客户需要对业务数据、软件和系统镜像进行备份，华为云提供了多种有不同侧重的产品和服务。例如，客户可以使用华为云提供的**云备份 （Cloud Backup and Recovery，简称CBR）**服务对云内的云服务器、云硬盘、文件服务，云下文

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	考虑第28条规定的银行服务及其所连接的服务级别，以及第6条规定的信息资产的可访问性要求。 (2) 为确保数据的可访问性，银行有义务建立符合第6条所列各项数据可访问性要求的备份系统。为使系统能够从备份中恢复，备份程序中包含使系统正常运行的组件，例如操作系统、应用软件和数据。为确保备份正常工作，备份介质中的数据会定期通过执行恢复操作进行测试。备份传输时，会采用适当的加密技术和物理安全控制措施进行保护。 （3）如果由于网络和通信基础设施的原因而发生中断，银行有义务创建合适的替代通信渠道。 （4）银行有义务记录哪些系统、服务器和数据进行了备份，备份的频率、备份方法以及备份保存的环境和位置，并应反映当前情况。 (5) 银行有义务在收到司法机关（进行调查或起诉）或相关机构的数据请求后，立即制作数据副本并进行备份，或保留原始数据，直至请求得到满足。银行有义务将数据转换为请求机关易于查阅的已知格式，或向请求机关提供数据以及用于查阅数据的应用程序和工具。银行不得以法律规定的数据保留期限已过，或因本款所述数据请求处理延迟而导致数据无法访问为由进行辩解。银行应将根据本款要求提供的数据副本或额外备份至少保存两年。	试计划，对备份的有效性进行测试。客户在收到处理调查或起诉的机构或司法机关的数据请求后，需保留所有副本或附加备份至少两年。	件、 VMware 虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致数据不可用的场景前可将数据恢复到任意备份点。客户可使用**云硬盘（Elastic Volume Service，简称EVS）**中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。华为云还为客户提供了**镜像服务（Image Management Service，简称IMS）**，客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。**云服务器备份（Cloud Server Backup Service，简称CSBS）**服务可同时为云服务器下多个云硬盘创建一致性在线备份，保护数据安全可靠，降低数据被非法篡改的风险。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（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。 华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。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。所有数据中心都处于正常运营状态，无一闲置。同时，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，华为云要求本标准范围内的云服务均采用基于单地域多数据中心的冗余机制，以确保云服务的业务连续性。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（DCI – Data Center Interconnect），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。华为云能够在多个地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。 另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			冗余相连，进一步排除单点故障的风险。此外，用户可充分利用这些地域和可用区，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（包括自然灾害和系统故障）系统都能连续运行。 此外，像华为云提供的存储和数据库服务均具备高可靠保证，例如**云硬盘（Elastic Volume Service，简称EVS）**使用多副本的数据冗余保护机制，采用副本同步写、读修复等措施保证数据一致性，当检测到硬件故障能够通过后台自动修复，数据快速自动重建，使数据持久性可达99.999999999%。OBS通过支持对象数据的高可靠性，并通过业务节点的高可靠性网络和节点的多冗余设计，使系统设计可用性达 99.995%，完全满足对象存储服务高可用的需求。通过提供对象数据多份冗余和保证多份对象的数据一致性自动修复技术，来提供对象数据的高可靠性，使系统设计数据持久性高达99.999999999999%。RDS采用热备架构，故障系统 1 分钟自动切换。每天自动备份数据，上传到OBS桶，备份文件保留 732 天，支持一键式恢复。
第28条	(1) 为确保银行业务活动中所使用的银行服务（BS）的连续性，应制定银行服务连续性管理流程和经董事会批准的银行服务连续性计划，作为业务连续性管理及计划的一部分；同时，应任命银行服务连续性管理流程经理，并成立银行服务连续性委员会。 （2）业务连续性管理流程必须参考国家或国际标准或最佳实践。 （3）在计划编制过程中，评估所持有信息资产和数据的重要性级别，并在业务影响分析框架内，确定每项业务服务可接受的停机时间和可接受的数据丢失量。制定恢复程序，以确保服务能够在这些限制范围内恢复。银行还制定了灾后从备用中心恢复到主中心的程序。	客户应建立业务连续性管理机制，明确有关服务的恢复目标及最小恢复策略。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时间目标，为此类活动分配足够的资源，并按照业务影响分析制定业务连续性计划及灾难恢复计划，防范和减少突发事件导致的业务中断。客户应根据业务需求定期对信息资产进行备份。	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。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。此外，为满

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	（4）根据计划设立备用中心。备用中心可使用数据和系统备份。备用中心在地理位置上必须避免遭受与主中心相同的风险，例如地震、火灾、爆炸、洪水、山体滑坡、电力和通信线路中断等造成的损失。 （5）负责实施该计划的关键人员和在该计划范围内负有责任的人员每年都要接受BS连续性培训，培训内容和详细程度应与其职责相称，并且要了解其在该计划范围内的职责。 （6）即使在主要系统完全瘫痪的灾难情况下，银行也必须最迟在24小时内恢复运营。为确保计划的有效性和及时性，每年至少进行一次测试，模拟真实灾难场景，并通过备用中心维持运营。如有外部服务提供商，则需参与测试；测试结果将报告给高级管理层；并根据测试结果更新计划。主管机构有权制定有关本款实施的其他程序和原则。 （7）负责执行该计划的关键人员、计划下相关人员以及外部服务提供商的联系信息的有效性，以及这些人员的就绪状态和可用性，至少每年通过两次通信链测试进行检验。联系信息、计划以及相关救援或返回程序的最新副本应持续提供给需要知悉的人员，并且副本应保存在必要的位置。 （8）银行确保对主中心的系统、服务器、网络设备和其他IT组件进行的更新、补丁安装和配置更改应用到辅助中心的备份中，并执行完整性检查，以保证复制到辅助中心的数据和系统备份与主中心的数据和系统备份完全相同。		足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云向客户提供存储容灾服务（SDRS - Storage Disaster Recovery Service）为弹性云服务器、云硬盘和专属分布式存储（DSS – Dedicated Distributed Storage Service）等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。 华为云制定了业务连续性管理规定，以规范业务连续性相关管理框架、目的和范围、管理目标、角色和职责等内容。华为云已经通过 ISO 22301 业务连续性管理体系标准的认证，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。华为云每年会在组织内进行业务连续性的宣传和培训，针对危机管理岗位的员工开展专门培训以及定期做应急演练和测试，持续优化应急响应机制。 华为云为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面。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。华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案，定期做应急演练和测试，持续优化应急响应机制。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	（10）如果主数据中心或辅助数据中心采用外部服务，或者托管在与其他组织共享的数据中心，则主数据中心和辅助数据中心的工作环境以及外部服务提供商在数据中心所在地区或区域发生实际灾难时分配给银行的资源，必须能够保证银行的业务连续性。		

5.4 外部服务采购

编号	具体控制要求	客户关注点	华为云的应答
第29条	（1）银行高级管理层应建立适当的监督机制，使银行能够充分评估和管理拟采购的外部服务可能给银行带来的风险，并有效管理与外部服务提供商的关系。 （2）有关采购外部服务的条件、范围及其他定义，均应以书面合同形式订立。 （3）银行不能通过标准合同框架内执行的外部服务模式获取关键服务和无法强制执行第二款规定的合同义务的服务，也不能通过此类外部服务模式执行关键工作流程。 （4）银行应核实拟为其提供的银行服务投放广告的供应商（例如搜索引擎和社交媒体平台）是否已采取措施防止以银行名义发布虚假广告，并应拒绝接受未采取适当措施的供应商的广告服务。银行在与供应商（例如搜索引擎和社交媒体平台）签订的广告服务合同中，应包含相关条款，规定在发生虚假广告事件时，银行可以获取必要的事件信息以保护客户权益。本款规定同样适用于银行与已同意接受其广告服务的中介机构签订的合同。 （5）根据其安全政策中规定的原则，银行应进行必要的组织变革，以控制外包服务产生的风险，制定行政程序，并任命具有足够知识和经验的负责人来管理与外包服务提	1. 客户应在采用外包服务之前对该云提供商进行风险评估，客户应在与外包服务提供商签订的合同或协议中明确云服务提供商须遵守组织政策和程序、法律法规的要求。 2.在服务期间审查和监控第三方服务提供商是否遵守合同义务，合同内容应涵盖与服务水平相关的定义，退出策略条款等。	在服务协议终止时，客户可通过华为云提供的云数据迁移服务支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓 库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。 华为云作为云服务提供商，遵守客户提出的网络安全要求，确保各项云技术的安全开发、配置和部署以及所提供云服务的运维运营安全。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。在华为云内 部，华为云建立了正式的采购审核流程，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。合同与服务协议中明确了双方的责任和义务、服务内容及服务水平等要求，同时通过保密协议对违反保密性的条款进行了约束。 华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	供商的关系。 （6）对授予外部服务提供商的访问权限类型进行逐一评估。针对这些访问权限（包括物理访问权限和逻辑访问权限）开展风险评估，并根据风险评估结果制定额外的控制措施。进行风险评估时，应考虑所需的访问权限类型、所访问数据的价值、外部服务提供商采取的控制措施以及该访问权限对银行信息安全的影响。 （7）银行有义务采取必要措施，确保其自身及其用户在外部服务采购中机密信息的安全。授予外部服务提供商的系统访问权限、数据访问权限或数据查看权限仅限于完成工作所需的信息。银行有责任确保外部服务提供商采取措施保护本机构及其用户的机密信息。 （8）本条例规定的银行监管内部控制和内部审计活动不得外包，必须由银行自己的人员执行。 （9）银行的信息系统可以全部或部分外包； (10) 为确保主要系统和安全领域采购的产品和服务在土耳其生产，或其生产商的研发中心位于土耳其，我们将采取一切必要措施，并将此视为外包服务的一项重要标准。此类供应商和生产商必须在土耳其设立应急小组。本机构有权对银行使用的安全产品和其他IT要素提出额外要求。 （11）本行可将云计算服务作为外部服务使用。主要系统或次要系统的云服务可通过私有云服务模式获取，该模式下硬件和软件资源分配给单个银行。此外，通过社区云服务模式获取外部服务须经董事会批准。在该模式下，硬件和软件资源仅分配给受董事会监管的机构，物理上共享，但逻辑上为每家银行分配独立的资源。董事会有权在认为必要时变更可纳入社区云服务范围的机构。		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《银行信息系统和电子银行服务条例》所述的网络安全原则。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。在华为云内部，华为云在引入供应时会与其签署保密及服务水平协议，协议中包含对于供应商的安全和隐私数据处理的要求，管理其访问权限不应超过其服务所必须。供应商的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。

 版权所有 © 华为云计算技术有限公司

6 华为云如何遵从及协助客户满足 BDDK《关于支付机构和电子货币机构信息系统管理和审计的公告》的要求

《关于支付机构和电子货币机构信息系统管理和审计的公告》专为金融科技（FinTech）企业、支付服务商及电子货币发行商量身定制，旨在规范非银金融机构的 IT 风险管理。公告要求这些机构必须建立与其业务规模相匹配的信息系统管理框架，涵盖严格的数据加密、访问控制、业务连续性计划以及灾难恢复机制。

以下内容将总结《关于支付机构和电子货币机构信息系统管理和审计的公告》中与云服务供应商相关的控制要求，并详细阐述了华为云作为客户的云服务供应商时，会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	华为云的应答
第5条	（4）作为信息安全管理流程的一部分，高级管理层； a) 确保信息安全政策及所有责任至少每年审查、更新和批准一次； b) 根据信息系统及其处理、存储和传输的数据的安全敏感级别对其进行分类，并为每一类建立适当的安全控制级别。 c) 监控安全领域的最新发展、新的威胁和漏洞，并应用必要的软件更新和补丁； c) 监控并定期评估与信息安全漏洞相关的事件， d) 每年至少进行一次渗透测试，由不参与组织通过其信息系统提供的服务的设计、开发、实施或执行的独立团队进行测试；	客户应定建立信息安全政策并每年审查更新，并重点建设如下机制： a) 数据分级以及按级别的安全控制 b) 漏洞发现与管控； c) 渗透测试 d) 意识培训	为协助客户满足监管要求： **1.** 客户可以使用华为云提供的**数据安全中心（Data Security Center，简称DSC）**，这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。 **2.** 客户可通过华为云的**漏洞管理服务CodeArts Inspector** 实现 Web 漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测等功能，自动发现网站或服务器暴露在网络中的安全风险，以实现对其云上的业务进行多维度的安全检测。作为云服务提供商，华为

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	e) 开展活动，提高组织内部、用户和成员企业的信息安全意识		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。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。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. 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。
第6条	(1) 组织应建立安全事件管理和网络事件响应流程，用于处理和监控安全事件，包括与安全相关的用户投诉，并将该流程与信息安全管理流程相整合。在此流程中，应建立必要的管理架构，并按照组织确定的程序和原则，向组织和相关管理部门报告安全事件。	客户应建立安全事件管理和网络事件响应流程，用于处理和监控安全事件.	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。
第7条	(1) 组织应确保在所提供服务的设计、开发、测试和维护阶段，开发、测试和生产环境按照职责分离原则相互隔离。在此背景下，流程和系统的设计和运行方式应确保任何个人都无法进入、授权并完成关键操作。	客户应确保在所提供服务的设计、开发、测试和维护阶段，开发、测试和生产环境按照职责分离原则相互隔离。	1.华为云建立了正式的环境隔离机制，对开发环境、测试环境及生产环境实现严格的逻辑隔离，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。禁止未经授权打通测试环境和生产环境的网络链接，避免因测试环境被入侵而导致生产环境安全风险。同

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	(2) 系统、服务和数据的授权级别和访问权限遵循以下原则：尽可能为相关要素分配最低权限和最严格的访问权限。已分配的授权会定期审查和更新，以确保符合职责分离原则。 （3）当组织与自身企业网络之外的网络通信时，会建立网络控制安全系统，以防范来自这些外部网络的威胁。组织会使用一个或多个防火墙（根据需要进行配置并持续监控），以控制外部网络对其内部网络的访问，并通过将内部网络划分为具有不同安全敏感度的子区域来确保受控访问。 （4）在通过互联网提供的服务中，采用各种技术来验证用户进行交易的网站是否属于该组织。 （5）在不违反第十五条第一款规定的前提下，敏感支付数据必须以加密形式或安全组件存储。 （6）如果敏感支付数据和个人信息通过无线方式或互联网传输，则该传输应使用端到端安全通信进行。 (7) 所采用的加密技术基于当前文献中公认且可靠性未受损的算法。所使用的加密密钥长度足以确保在密钥有效且可用于相关算法的期间内无法破解。有效防止了无效、被盗或已损坏的加密密钥的滥用。 （9）该组织应根据当前技术建立控制措施，以确保在安全组件或支付工具丢失或被盗的情况下，托管其向用户提供的移动应用程序的移动设备上的敏感支付数据无法访问。 （10）本组织确保向用户提供的任何软件或移动应用程序的来源均可核实，确认其确实来自本组织。本组织负责确保这些软件程序不包含任何可能危		时，华为云遵循职责分离和权限制衡原则，对不相容职责进行分离，确保开发和运维人员职责分离。 2.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。所有访问都是基于最小权限概念遵循和授予的，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。 3.华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分区自我保护和容错恢复能力。华为云会维护最新的网络拓扑结构图。华为云数据中心主要分为以下五个重要安全区域：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。同时，在网络边界防护方面，华为云还可提供**Anti-DDoS流量清洗服务（简称Anti-DDoS）**和**DDoS 高防（Advanced Anti-DDoS，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。 4.当客户通过互联网提供Web网站业务

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	及用户安全的代码，并负责发布必要的补丁和更新以修复安全漏洞。		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。 5.华为云云硬盘、对象存储、镜像服务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。华为云服务端加密功能还集成了**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。客户可以使用IAM在DEW中对基于角色的授权模型进行权限管理，只授予用户执行任务所需的权限，在未授权的情况下，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。 6.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（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。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。 7.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（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。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。华为云使用的硬件安全模块（HSM）为客户创

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			建和管理密钥，拥有主流国际安全认证，助力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。 8.当客户移动应用的后台数据存储在华为云服务（如**云硬盘（Elastic Volume Service，简称EVS）**、**对象存储服务（Object Storage Service，简称OBS）**、云数据库RDS）时，客户可以启用服务端加密功能，使用KMS中管理的密钥对数据进行加密。即使设备丢失，存储在云端的支付数据也是密文，无法被直接读取。 9.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。同时，所有云服务发布前都经过了多轮安全测试，测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。此外，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。
第8条	（1）组织应建立有效的审计追踪记录系统，用于记录对用户信息的物理或逻辑访问、未经授权的访问尝试以及信息系统内所有与支付交易或电子货币相关的交易。审计追踪必须足够详细和清晰。 （2）采用各种技术手段防止审计跟踪的完整性受到损害，并检测任何此类损害。采取措施保护记录系统免受任何未经授权的更改和干预，并防止组织人员干扰与其自身活动相关的审计跟踪。采用各种技术手段防止审计跟踪记录系统停止运行，或检测其是否已停止运行。 （5）审计记录应至少保存 3 年，以备审计。 （6）通过在具有足够安全级	客户应建立有效的审计追踪记录系统，用于记录对用户信息的物理或逻辑访问、未经授权的访问尝试以及信息系统内所有与支付交易或电子货币相关的交易。	1.华为云提供的**云审计服务（Cloud TraceService，简称CTS）**可以为客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。可实时、系统地记录所有人员的操作，以便客户对各项变更执行事后审计。CTS若配置事件转储至OBS功能，则会定期将操作记录同步保存到用户定义的OBS桶中进行长期保存。满足客户审计记录保存3年的要求。 2.华为云提供了多粒度的数据备份归档服务（如OBS版本控制、云硬盘备份VBS、**云服务器备份（Cloud Server Backup Service，简称CSBS）**等），可对数据进行备份，保证在灾难发生时数据不丢失，这间接保障了审计跟踪的可访问性。 3.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。确保审计跟踪符合法律标准，并且组

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	别的环境中保护和备份审计跟踪，即使在可能发生的灾难之后也能确保可访问性。 （7）如果信息系统需要外部服务，组织应确保外部服务提供商保存的审计跟踪符合其自身标准，并且组织可以访问这些审计跟踪。		织可以访问这些审计跟踪。
第9条	（3）该组织应采取必要措施，确保其将要建立的系统和将要开发的应用程序中用户和人员身份验证信息的保密性和安全性。这些措施至少应包括：对数据库中的身份验证信息进行加密；在出于身份验证目的传输信息时对其进行加密；防止未经授权的访问或违反职责分离原则的不受控制的更改；为在这些数据库中进行的交易维护充分的审计跟踪；以及确保这些审计跟踪的安全。	客户应确保身份验证信息的保密性与安全性，数据库中的身份验证信息必须加密存储，传输过程须加密，防止未经授权的访问及违反职责分离的更改，并维护充分的审计跟踪且确保其安全。	客户可以使用华为云提供的**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，数据库中密码使用加盐的SHA512算法进行加密存储，密码通过TLS 1.2进行传输中加密，所有华为云IAM的API调用都支持 HTTPS 来对传输中的数据进行加密。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。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（Cloud TraceService，简称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。
	(4) 在提供敏感支付数据访问权限的情况下，在必须进行身份验证的交易中，应使用至少包含两个独立组件的身份验证机制来启动这些交易。这两个组件选自个人“知道”、“拥有”或“具有生物特征”的两类不同要素。组件的独立性意味着一个组件的泄露不会危及另一个组件的安全。这些组件必须能够保护身份验证信息的机密性，并且是用户特定的；除使用生物特征组件的情况外，至少一个组件必须是一次性的；并且必须确定该一次性组件所需的最短有效期。	在敏感支付交易中，客户须使用至少两个独立组件的多因素认证，组件独立性确保一个泄露不危及另一个，除生物特征外至少一个组件须为一次性且明确最短有效期。	华为云IAM支持多因素认证（MFA），满足“至少包含两个独立组件”的要求，认证组件包括用户名和密码、虚拟MFA设备（如华为云App、Google Authenticator等，产生6位数字动态验证码）、安全密钥（基于FIDO协议的硬件设备，如Yubikey）、访问密钥（AK/SK）、Windows Hello支持指纹、人脸识别等生物特征验证。 虚拟MFA基于时间的一次性密码（TOTP）标准，安全密钥基于物理硬件设备，这些组件与密码相互独立，一个组件的泄露不会危及另一个组件的安全。虚拟MFA设备产生的6位数字动态验证码具有时效性（通常30秒），满足“至少一个组件必须是一次性的”要求。临时访问密钥也具备时效性，可对有效期进行设置，到期后无法重复使用。
	（5）除首次用户登录外，对用于向用户提供支付工具和身份验证工具的电话号码和地址	除首次登录外，客户对电话号码、地址等敏感信息修改及安全	华为云**统一身份认证服务（Identity and Access Management，简称IAM）**支持对敏感操作和关键信息修改启用操作保

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	等信息的修改、用户定义的安全接收者列表以及可以使用单因素身份验证执行的交易列表，均按照第四款的规定使用双因素身份验证进行。	接收者列表变更，均须使用双因素认证。	护，要求进行二次身份验证。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。如果用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，并访问用户的华为云资源。
	（8）制定符合当前技术且安全的密码策略，用于管理应用于用户身份验证的密码。	客户应制定安全的密码策略（如复杂度、有效期、历史密码禁用等）。	华为云**统一身份认证服务（Identity and Access Management，简称IAM）**提供完整的密码策略管理功能，IAM支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。
	（9）从生产阶段到交付给用户的整个过程中，用于用户身份验证机制的组件（如密码、可变密码、一次性密码设备、加密密钥、智能卡和交易验证码）的安全性都得到了保证。	从生产到交付全过程，密码、一次性密码设备、加密密钥等身份验证组件的安全性须得到保障。	华为云**统一身份认证服务（Identity and Access Management，简称IAM）**确保身份验证组件从生产到交付全过程的安全性： 1) 密码：加密存储，支持重置机制 2) 访问密钥（AK/SK）：只能在首次创建时获取，如遗失只能重新创建，防止泄露 3) 临时访问密钥：具备时效性，到期后无法重复使用 4) 虚拟MFA设备：基于标准TOTP算法，与用户账号绑定
	（10）认证机制； a) 系统应在用户首次登录时告知其身份验证尝试失败的情况，如果失败尝试次数超过一定次数，则应阻止用户访问支付服务。 （b）在身份验证尝试失败后，用户不应向尝试进行身份验证的人员提供有关错误输入的用户名或密码的不必要信息，例如系统中不存在的用户名或输入错误的密码。 c) 对于没有发生任何活动的非活动会话，或者如果由于用户未安全注销而退出移动应用程序导致应用程序在后台继续运行，则会话将在一段时间后终止。 c) 除授权多个用户使用同一支付账户或同时登录不同会话的	客户应具备如下认证机制： 1）首次登录应告知用户失败尝试情况，超过一定次数则阻止访问； 2）失败后不应透露“用户名不存在”或“密码错误”等具体信息； 3）非活动会话及后台运行的移动应用会话应在超时后终止； 4）除授权场景外，系统不应允许同一用户同时登录多个会话并发出警告。	华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**产品设置了完善的认证机制。只有管理员和委托身份可以设置登录验证策略，普通IAM用户只有查看权限，不能对其进行设置，如需修改，需联系管理员操作或添加权限。 1) 系统会对华为账号登录进行安全认证，如果更换终端，初次登录将进行安全认证(安全手机二次验证)。 2) 会话超时策略：如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。管理员和委托身份可以设置会话超时的时长，会话超时时长默认为1个小时，可以在15分钟~24小时之间进行设置。 3) 账号锁定策略：如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间。锁定时，账号不能为自己或IAM用户解锁，锁定时间

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	情况外，系统不应允许同一用户同时尝试登录多个会话，并应向该用户发出警告。		结束后，才能重新登录。 4) 账号停用策略：如果IAM用户在设置的有效期内没有通过界面控制台或者API访问华为云，再次登录时将会被停用。账号停用策略默认关闭，管理员和委托身份可以选择开启，并在1~240天之间进行设置。该策略仅对账号下的IAM用户生效，对账号本身不生效。IAM用户被停用后，可以联系管理员重新启用。 5) 最近登录提示：如果开启最近登录提示，用户登录成功后，将在“登录验证”页面中看到上次登录成功时间，最近登录提示可以帮助用户查看是否存在异常登录信息，如果存在不是本人的登录信息，建议立即修改密码。
第10条	（1）组织应制定信息系统连续性计划，以确保支持其运营和关键业务功能的信息系统服务的连续性。该计划须经最高管理层批准。 （2）在计划编制过程中，评估信息系统资产和所持有数据的重要性级别，确定每项服务的可接受停机时间，并制定恢复程序，以确保在这些时间内能够再次访问服务。 （3）根据该计划，设立一个备用中心。数据和系统备份保存在备用中心，随时可用。 （4）在任何影响组织信息系统连续性的事件或变化发生后，该计划都会进行审查和更新。 （5）为确保计划的有效性和及时性，每年至少通过二级中心进行一次测试，如有外部服务提供商，则将其纳入测试，测试结果报告给高级管理层，并根据这些结果更新计划。	客户应制定信息系统连续性计划，以确保支持其运营和关键业务功能的信息系统服务的连续性。	华为云根据内部业务连续性管理体系的要求，制定了完善的恢复策略，以支撑云服务持续运营的关键业务。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。
第11条	(1) 组织的高级管理层应建立适当的监督机制，以便评估和管理信息系统服务外包可能给组织带来的风险，并有效开展与外部服务提供商的关系。在	客户的高级管理层应建立适当的监督机制，以便评估和管理信息系统服务外包可能给组织带来的风	1. 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和监督。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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	此背景下，组织的高级管理层至少应监督外包服务的可访问性、性能和质量，以及服务范围内发生的安全漏洞事件，并监督外部服务提供商的安全控制措施、财务状况和合同履行情况。	险，并有效开展与外部服务提供商的关系。	服、自助服务、热线电话等联络到华为云的支持团队。 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、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. 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。
	（2）外部服务采购合同至少应包括以下内容： a) 与服务水平相关的定义。 b) 服务终止条件。 c) 外部服务提供商和组织在信息系统连续性计划范围内的义务。 c) 确保外包范围内的所有系统和流程均符合组织自身的风险管理、安全和隐私政策的规	外部服务采购合同至少应包括服务水平定义与服务范围、服务期限与终止条件、价格与支付方式、双方权利义务与保密、质量验收与售后服务、违约责任、知识产权归属、不可抗力与争议解决。	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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	定。 d) 与本协议所涵盖的产品和服务的产权和知识产权相关的规定。 e) 确保合同中构成外部服务提供商义务的条款，也是与分包商签订的合同中具有约束力的条款。 f) 与管理因外包服务意外终止或中断而产生的风险相关的规定。 g) 确保组织所受法律规定的条款也适用于所接受服务的外部服务提供商。 （g）规定，在组织内部开展外包活动的情况下，应按照预期进行同样的独立审计，且不得缩小审计范围。 h) 规定外部服务提供商有义务及时、准确地提供主管机关要求的有关其活动的所有信息和文件，并妥善保管与这些活动相关的所有电子、磁性及类似记录，以及访问和读取这些记录所需的所有系统和密码，以便随时查阅。 i) 规定组织及其独立审计师有权向外部服务提供商索取与外包服务主题相关的任何信息和文件。 i) 确保外部服务提供商按照董事会或机构的指示，在规定的时间内实施对组织信息系统的变更，作为所接受服务的一部分。		
	（5）组织可以使用云计算服务作为外部服务来处理、存储和传输所有类型的数据。但是，只有在通过私有云服务模式获取外部服务的情况下，才能使用云计算服务来处理、存储和传输敏感的支付数据、个人信息或任何可以与用户关联并识别用户身份的信息。私有云服务模式下，外部服务仅通过分配给组织的硬件和软件资	客户使用外部云计算服务来处理、存储和传输所有类型的数据时，需选择私有云服务模式。	如果客户需要私有云服务模式，华为混合云通过持续创新，提供Huawei Cloud Foundation(HCF) 、 Huawei Cloud Stack(HCS)、Huawei Cloud Stack专属云多种方案，帮助政企客户在本地数据中心构建安全、可靠、高效的云基础设施，助力客户从业务上云迈向深度用云，加速数智化转型。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	源提供。		
	（6）本组织有义务采取必要措施，确保在采购外部服务时，属于本组织及其用户的机密信息的安全。授予外部服务提供商的系统访问权限、数据访问权限或数据查看权限仅限于完成工作所需的信息。本组织有责任确保外部服务提供商采取措施保护属于本组织及其用户的机密信息。	客户有义务采取必要措施，确保在采购外部服务时，保护本组织及其用户的机密信息的安全。	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。
第16条	（1）组织必须将其主要系统和次要系统保留在境内。 （2）所有用于执行同一机构用户之间或不同机构用户之间支付交易的信息系统及其备份必须位于国内。在此背景下，如果使用外部服务，外部服务提供商用于开展与该服务相关的活动的信息系统及其备份也必须位于国内。	客户必须将其主要系统和次要系统保留在境内。	1.华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据。客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，使客户内容数据存储在目标位置。华为云在土耳其伊斯坦布尔有3个可用区，在多个相邻国家例如爱尔兰也设有可用区。当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，使客户只能访问到自己的数据。 2.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。 3.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。

 版权所有 © 华为云计算技术有限公司

7 华为云如何遵从及协助客户满足 SPK《管理程序和原则》的要求

《管理程序和原则》是土耳其资本市场委员会（SPK）2025 年 3 月发布的确保相关机构、组织和合作伙伴的信息系统管理的方法和基础。旨在确保信息系统运行的正当性、准确性。内容包含信息系统管理控制措施、风险管理流程和程序、信息系统运行规则，开发与维护要求等。

以下内容将总结《管理程序和原则》中与云服务供应商相关的控制要求，并详细阐述了华为云作为客户的云服务供应商时，会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	华为云的应答
第12条	(1)为保护数据中心或主要系统所在的安全区域免受未经授权的物理访问、环境条件变化、基础设施服务中断和灾害的影响，至少应采取下列控制措施： a)所有人员的出入均有正当理由、获得授权、记录在案并受到监控。已实施门禁控制机制。访问权限定期审查。 b)将建立机制，实时监控未经授权的访问尝试。 c)采用不间断电源供电。 c)空调控制确保合适的工作条件。 d)针对火灾、洪水、地震、爆炸和其他自然灾害或人为灾害造成的损害，设计并实施了物理防护措施。 e)配套基础设施服务（空调、不间断电源、发电机、灭火系统等）应至少每年进行一次定期	客户应建立并保证数据中心或主要系统的物理和环境安全。	1.华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了全天候保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，使非授权人员不可访问数据中心。 2.华为云数据中心采用多级保护方案保障业务7*24小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源(UPS)，提供短期备用

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	维护。 f)非机构、组织和合作机构雇员但将从事安装、维护和维修服务的个人，须在开始工作前签署保密协议。这些人员在机构、组织和合作机构工作期间将全程有人陪同。 g)配套基础设施服务应具备在运行条件偏离预期范围时发出警报并通知相关方的功能。		电力供应。在机房供电线路上的配置了稳压器和过压防护设备。在供电设备及线路上还设置冗余或并行的电力电缆线路为计算机系统供电。
第13条	（1）已建立并有效管理各项控制措施，以保护企业网络免受内部和外部威胁，并确保使用该网络的系统、数据库和应用程序的安全。采用分层安全方法来确保企业网络及其上的信息系统的安全。在这种方法中，网络基础设施、操作系统和应用程序防御等多层保护措施被设计并作为一个整体加以实施。 （2）公司网络的物理和逻辑拓扑结构，包括所有子网、安全设备、接入点和连接路径，均有文档记录，并保持更新，且安全存储。 （3）通信基础设施受到保护，免受窃听和物理损坏。 （4）采取并实施安全措施，以应对移动设备访问企业网络所带来的风险。 （5）防止未经授权访问网络基础设施，并建立监控流程。 （6）通过内部资源提供或从外部来源接收的所有网络服务的安全标准、服务级别和管理要求均在服务协议中定义和包含。 （7）远程访问服务采用多因素身份验证。远程访问授权需经信息安全官批准。远程访问仅允许使用安装了最新应用程序和操作系统的设备进行。远程访问会保留审计日志。 （8）远程访问连接采用当前稳定可靠的通信协议。通过互联网进行访问时，使用端到端安	客户应建立并有效管理各项控制措施，以保护企业网络免受内部和外部威胁，并确保使用该网络的系统、数据库和应用程序的安全。	1.为配合客户满足监管要求： a)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（Virtual Private Cloud，简称 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。 b)华为云**Web应用防火墙（Web Application Firewall，简称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、webshell、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。 2.华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分区自我保护和容错恢复能力。华为云会维护最新的网络拓扑结构图。华为云数据中心主要分为以下五个重要安全区域：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–

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	全通信技术。如果在规定的时间内未进行任何操作，远程访问会话将自动终止；需要恢复访问时，需重新进行身份验证。 (9)在企业网络与外部网络通信过程中，防火墙持续监控来自外部网络的威胁，并采用符合当前技术水平的解决方案来检测和阻止网络中的异常活动和攻击企图。防止通过互联网直接访问包含敏感数据的信息系统。 （10）通过互联网提供的服务受到保护，免受拒绝服务攻击。 （11）在内部网络端口实施网络访问控制，只有经过批准连接的设备才能加入网络。 (12)为确保受控访问，已建立相应的控制措施，将内部网络中具有不同安全要求的子网络进行隔离。在此背景下，至少应为客户端、服务器和管理进程创建独立的子网络。有线网络和无线网络也应彼此隔离。 （13）分析传入和传出的网络流量，当检测到有害或异常流量时，隔离相关的网络段。 （14）通过适当手段阻止访问不符合信息安全要求和法律要求的网站。 （15）使用白名单或黑名单结构限制网络访问，并阻止不受信任的连接。 （16）无线网络采用强加密协议。无线网络实施身份验证和访问控制。身份验证过程采用可靠且最新的协议。访客网络与企业网络隔离，访客网络用户仅被授予临时且受限的访问权限。		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。 3.除了通过IAM管理远程接入人员的身份和权限外，华为云还提供**虚拟专用网络（Virtual Private Network，简称VPN）**、HTTPS等加密传输方式供客户选择。此外，华为云只能通过华为云统一管理接入网关和SVN权限远程访问其内部系统。此外，接入网关支持强日志审计，确保运维人员能够在目标主机上的行为可以定位到个人。
第14条	（1）各机构、组织和伙伴关系应建立必要的控制措施，以确保按预期水平持续提供所需的信息系统服务。本条款范围内各项服务的水平应与业务部门	客户应建立必要的控制措施，以确保按预期水平持续提供所需的信息系统服务。	1.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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	协商确定，并符合业务需求。应建立相关机制，记录用户在使用信息系统时遇到的问题和提出的请求，并予以回应，同时解决问题的根本原因。 （2）主要系统受到持续监控，以确保其按预期服务水平运行。每个系统都设定了阈值，当超出这些阈值时，系统会自动向相关人员发送通知。如果未达到预期性能值，则会调查根本原因并采取必要的纠正措施。 （3）进行容量规划是为了确保信息系统能够以预期的性能水平运行，同时考虑到机构、组织和伙伴关系的活动可能增长、用户数量增加以及类似情况。 （4）定期监控信息系统中的安全漏洞，以防止其影响业务流程。对已发布的安全漏洞补丁的应用情况进行评估。决定应用的补丁首先进行测试。对于未应用的补丁，将建立额外的控制措施来应对风险，或停用相关组件。补丁应用在变更管理框架内进行。定期向信息安全官报告决定不应用的补丁。 （5）对配置设置进行监控，以确保信息系统组件在其整个生命周期内始终以预期的性能、质量和安全水平运行。信息系统组件中所有不必要的功能均被禁用。针对每种组件类型定义并应用基本配置设置。当出现新的安全漏洞或现有组件升级到新版本时，将审查配置设置的适用性和充分性。监控一个组件中配置设置更改对其他组件的影响。任何配置设置的更改及其理由均会被记录和跟踪。所有组件的配置设置均已备份。任何配置设置的更改均在变更管理框架内进行处理。 （7）针对影响机构、组织和合作伙伴信息系统的恶意软件，		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。 2.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。 3.华为云针对弹性云服务器（Elastic Cloud Server，简称ECS）配套提供了镜像服务，租户可自行选择华为云官网提供的标准镜像或者私有化镜像，通过控制台（Console）的管理，可以方便地进行版本管理和发布管理。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。 4.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。当出现新的安全漏洞或现有组件升级到新版本时，将审查配置设置的适用性和充分性。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	已采取必要措施。为此，已使用恶意软件检测和清除软件，并确保这些软件保持最新状态。已将台式机、笔记本电脑和服务器系统配置为在连接便携式媒体或外部设备时不自动播放内容，并已设置恶意软件拦截工具，以便在连接此类设备时自动扫描。		
第15条	(1)对于通过信息系统进行的交易，应确定并实施与信息资产安全等级相适应的身份验证方法。 （2）该认证方法涵盖用户从登录信息系统到完成交易并离开系统的整个过程。采取必要措施，确保认证信息在会话开始到结束始终准确无误。 （3）采取必要措施，确保存储认证数据的环境以及用于此目的的工具的安全。这些措施至少包括：使用强加密算法或以不可逆的方式加密存储认证数据；建立能够检测数据任何更改的系统；维护充分的审计跟踪并确保其安全。采取措施确保认证数据在传输过程中的机密性。 （4）所指定的认证方法至少应具备以下功能： a)如果身份验证尝试失败，则进行尝试的人员将无法获得有关系统或用户的任何信息。 b)如果连续多次身份验证尝试失败，则相关用户的访问权限将被阻止，并且该用户将收到通知。 c)未激活的会话在指定的超时时间后将被终止或锁定，在这种情况下，必须重新进行身份验证才能重新打开会话。 c)未经信息安全官批准，不允许同一用户进行多次登录。 （5）用户密码管理至少应采取下列措施： a)强制用户在首次登录时更改其在首次注册系统时设置的密	客户应在信息系统的获取、开发、修改或外包过程中建立控制措施，并以书面形式明确功能、技术与安全需求。系统结构应与组织规模、活动性质和产品相适应。对于无法提供源代码的外部开发应用程序，应签订软件存储协议。大规模开发或修改项目应在项目管理框架内进行，经高级管理层批准并定期提交进度报告。应建立覆盖软件开发生命周期所有阶段的安全软件开发程序，并规划、测试、实施系统更新或变更，避免业务流程中断或信息安全风险。参与开发的人员应接受安全软件开发培训。开发、测试和实际环境应相互隔离，测试环境中不包含客户信息。系统在投入实际环境前须按	1.华为云的**统一身份认证服务（Identity and Access Management，简称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（Cloud TraceService，简称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。 2.IAM通过加密算法对用户个人敏感数据加密后进行存储。用户名、AK：不属于敏感数据，明文存储。密码使用加盐的SHA512算法进行加密存储。邮箱、手机号、SK使用安全AES算法进行加密存储。 用户个人敏感数据（包括密码）将通过TLS 1.2进行传输中加密，所有华为云IAM的API调用都支持 HTTPS 来对传输中的数据进行加密。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。 3.华为云的IAM产品设置了完善的认证机制。只有管理员和委托身份可以设置登录验证策略，普通IAM用户只有查看权限，不能对其进行设置，如需修改，需联系管理员操作或添加权限。系统会对华为账号登录进行安全认证，如果更换终端，初次登录将进行安全认证(安全手机二次验证)。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	码。 （b）密码的复杂性和长度应该使其难以猜测和破解。 c)强制定期更改密码。 c)禁止追溯使用一定数量的旧密码。 d)更改新安装的系统和设备上的默认密码。 e)密码在屏幕上以遮罩方式显示。 （6）在关键系统和应用中，采用独立的多因素身份验证机制。各因素的独立性意味着，即使其中一个因素遭到破坏，其他因素的安全性也不会受到影响。至关重要的是，用户拥有的身份验证因素必须是用户独有的，并且无法被模仿。 （7）特权用户帐户采用多因素身份验证机制。 （8）对于关键系统和应用程序中身份验证过程中的成功和失败的交易，都会保留审计跟踪。 （9）采用自动生成用户账户报告的方法，包括锁定账户、禁用账户、密码过期账户和密码永不过期账户，并将这些报告转发给相关方，以便他们采取必要的措施。	验收标准进行功能、技术和安全测试，关键应用须完成安全测试并处理问题。修改或新开发的系统须与原系统并行运行至成熟方可投入实际环境，若无法并行则须保持原系统可用且不丢失数据。除非经信息安全官批准并在有限时间内，否则应用程序开发人员不得访问真实环境，所有交易须保留审计跟踪记录。版本控制工具应用于开发过程，源代码变更须反映在版本控制工具中并附有理由。	会话超时策略：如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。管理员和委托身份可以设置会话超时的时长，会话超时时长默认为1个小时，可以在15分钟~24小时之间进行设置。 账号锁定策略：如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间。锁定时，账号不能为自己或IAM用户解锁，锁定时间结束后，才能重新登录。 账号停用策略：如果IAM用户在设置的有效期内没有通过界面控制台或者API访问华为云，再次登录时将会被停用。账号停用策略默认关闭，管理员和委托身份可以选择开启，并在1~240天之间进行设置。该策略仅对账号下的IAM用户生效，对账号本身不生效。IAM用户被停用后，可以联系管理员重新启用。 最近登录提示：如果开启最近登录提示，用户登录成功后，将在“登录验证”页面中看到上次登录成功时间，最近登录提示可以帮助用户查看是否存在异常登录信息，如果存在不是本人的登录信息，建议立即修改密码。 4.华为云IAM提供完整的密码策略管理功能，IAM支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。 5.华为云IAM支持多因素认证（MFA），满足“至少包含两个独立组件”的要求，认证组件包括用户名和密码、虚拟MFA设备（如华为云App、Google Authenticator等，产生6位数字动态验证码）、安全密钥（基于FIDO协议的硬件设备，如Yubikey）、访问密钥（AK/SK）、Windows Hello支持指纹、人脸识别等生物特征验证。 虚拟MFA基于时间的一次性密码（TOTP）标准，安全密钥基于物理硬件设备，这些组件与密码相互独立，一个组件的泄露不会危及另一个组件的安全。虚拟MFA设备产生的6位数字动态验证码具有时效性（通常30秒），满足“至少一个组件必须是一次性的”要求。临时访问密钥也具备时效性，可对有效

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			期进行设置，到期后无法重复使用。
第16条	（1）机构、组织和伙伴关系应建立适当的访问控制措施，以控制对信息系统的访问和应用程序的使用。在确定授予用户的权限级别时，应遵循授予最低必要权限和最严格访问权限的原则，并考虑用户的职责。权限和职责应符合职责分离原则。在访问管理中应用基于角色的访问控制至关重要。 （2）所有授权至少每年由相关信息资产的负责人审核一次。非必要业务需求的授权将被撤销。 （3）账户创建、授权及其他与用户访问权限相关的流程均须遵循职责分离原则，并经过审批程序。所有与访问权限相关的流程均会保留审计记录，并定期进行审查。 （4）如遇工作职责变更或雇佣关系终止，应将拟采取的措施以书面形式记录，并对该范围内采取的措施作出记录。在此情况下，应审查现有授权，并立即取消任何不必要的授权。 （5）除强制要求外，禁止在信息系统中使用通用账户或默认账户；如有必要使用这些账户，则应建立控制措施，明确使用这些账户的人员的责任，并保留这些账户所进行交易的审计跟踪。 （6）除非必要，否则不得向信息系统用户授予本地管理员权限。如工作需要，此类权限的授予须经信息安全官批准。 （7）信息系统中需要特权访问的任务和交易会开设单独的账户。这些账户执行的交易都会保留审计跟踪记录。 （8）建立了检测和预警异常或意外访问尝试（包括使用特权	客户应建立适当的访问控制措施，以控制对信息系统的访问和应用程序的使用。	1.为配合客户满足监管要求： a)每一位华为云客户在华为云都拥有唯一可辨识的用户ID，并提供多种用户身份验证机制，包括账号密码、多因素认证等。**统一身份认证服务（Identity and Access Management，简称IAM）**支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，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。如果用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，并访问用户的华为云资源。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。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。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（Cloud TraceService，简称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。 2.金融机构可通过华为云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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	用户帐户进行的访问）的机制。 （9）紧急授权是临时授予的，并保留审计跟踪，以便监控授权期间开展的操作。		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。
第17条	（1）各机构、组织和伙伴关系应采取必要措施，确保通过信息系统进行的交易、记录和数据的完整性。确保完整性的措施应涵盖数据传输、处理和存储的所有阶段。对于与提供信息系统相关外部服务的组织进行的交易，也应采取同样的做法。 （2）采用各种技术来检测关键流程、记录和数据中可能发生的腐败行为，并及时发出必要的通知。	客户应采取必要措施，确保通过信息系统进行的交易、记录和数据的完整性。确保完整性的措施应涵盖数据传输、处理和存储的所有阶段。	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。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。 2.为保障客户安全的处理云上数据，华为云对数据生命周期各阶段进行层层防护： a)数据创建：华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据。客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，使客户内容数据存储在目标位置。当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，使客户只能访问到自己的数据。 b)目前，**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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			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。 c)数据使用：华为云从数据访问控制、安全防护、审计等方面为客户提供了相关服务，协助客户对数据的使用和流转做到更加细粒度的管控。 d)数据传输：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。 e)数据归档：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**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。通过与密码安全中心集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。 f)数据销毁：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。
第18条	（1）各机构、组织和伙伴关系应采取措施，确保信息系统活动范围内进行的交易以及在这些交易范围内传输、处理和存储的数据的保密性。为确保保密性而开展的工作至少应包括以下内容： a)数据必须按照其安全等级进行保护。 （b）在个人职责框架内界定数据访问权限，记录访问情况，	客户应采取措施，确保信息系统活动范围内进行的交易以及在这些交易范围内传输、处理和存储的数据的保密性。	1.为配合客户遵从监管要求，华为云参照各类法规要求、监管要求、国际或行业标准建立了一套完善的信息安全和隐私保护管理体系，并持续改进。华为云践行管理体系的要求，保障客户的业务和数据安全。 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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	并保护这些记录免受未经授权的访问和干扰。 c)在所有环境中对敏感数据进行加密、存储、传输和备份。 c)当使用加密技术来确保数据隐私时，应使用可靠、稳健的算法；应防止使用过时、被盗或破解的加密密钥；应根据数据和操作的重要性确定密钥更换的频率；并且应安全地存储密钥。 （2）机构、组织和伙伴关系应根据其安全等级采取措施，防止在机构、组织和伙伴关系之外的信息系统活动范围内进行的交易所产生的、传输的、处理和存储的数据被故意或意外泄露。 （3）机构、组织和伙伴关系应建立控制措施，以确保通过信息系统获取或存储的个人数据的保密性，并采取必要措施来做到这一点。 （4）保存期限已过的数据应从其所在的所有介质中安全且不可逆转地删除，并且所采取的措施应予以记录。 （5）机构、组织和合伙企业应当采取必要措施保护和处理个人数据。本条未涵盖的情况，应当适用《个人数据保护法》（第6698号）及其他相关法律的规定。		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.华为云云硬盘、对象存储、镜像服务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。华为云服务端加密功能还集成了**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。客户可以使用IAM在DEW中对基于角色的授权模型进行权限管理，只授予用户执行任务所需的权限，在未授权的情况下，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。 4.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。 5.关于隐私保护的相关信息，具体可参考‘华为云土耳其意思遵从性指南’。
第19条	（1）各机构、组织和伙伴关系的最高管理层应建立监督机制，以便对信息系统范围内从外部供应商采购服务所产生的风险进行充分评估和管理，并确保与外部供应商的关系有效开展。所建立的监督机制至少应包括以下几点： a)外包信息系统服务范围内的所有系统和流程必须遵守机构、组织和合作伙伴自身的风险管理、信息安全和客户隐私原则。 （b）在必须将机构、组织和伙	客户应建立监督机制，以便对信息系统范围内从外部供应商采购服务所产生的风险进行充分评估和管理，并确保与外部供应商的关系有效开展。	1.华为云具备： a)财务状况：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IDC发布的《2019年Q1中国公有云服务市场跟踪报告》显示，从IaaS+PaaS整体市场份额来看华为云营收增长超过300%，华为云PaaS市场份额增速接近700%，在Top5厂商增速排名第一，位居中国公有云服务商第一阵营。 b)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、

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	伴关系的数据传输给外部服务提供商的情况下，该组织的信息安全原则和实践必须至少与机构、组织和伙伴关系所采用的原则和实践处于同一水平。 c)应规范与外包信息系统服务相关的事项，并采取必要的预防措施，同时考虑到机构、组织和合作伙伴关系的业务连续性。 c)在外包信息系统服务中，测量、评估、报告、安全和授权等流程的最终责任和决策权应归机构、组织和合作伙伴所有。 d)外包服务的性质不得妨碍机构、组织和合伙企业履行其法律义务和接受有效监督。 e)在决定选择外部服务提供商之前，应进行评估，以确定本组织是否具备必要的技术设备和基础设施、财务实力、经验、知识和人力资源，能够以所需的质量提供服务。该评估还应考虑对外部服务提供商的关注程度、服务退出策略以及服务的可替代性。最终的技术能力报告应提交给高级管理层审批。 f)对于从外部供应商处获得的服务；服务的范围、服务提供商的联系信息、服务的有效期、服务的级别及其重要性状态必须以书面形式记录。 （2）各机构、组织和合作伙伴的高级管理层应指定具备足够知识和经验的负责人，密切监督从外部获取的关键服务的可及性、性能和质量，监督这些服务范围内发生的安全漏洞，以及通过外包提供服务的组织的安全控制、财务状况和合同履行情况。这些负责人应至少每年编写一份评估报告，内容涵盖本条所列事项，并提交高级管理层。 （3）外包服务的条件、范围及		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。 c)管理能力：华为云继承了华为公司的风险管理能力，建立了完善的风险管理体系，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。 d) 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。 e)运营能力：华为云遵循ISO 27001、ISO 20000、ISO 22301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。 f)与认可机构的企业文化和未来发展策略的匹配程度：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。 g)对银行业的熟悉程度：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。同时，华为云已委托第三方开展独立评估，将华为云的内部管控现状与香港金管局发布的监管指引和公告要求对比，进行差距分析，并确保任何差距项均得到整改。 h)紧贴市场创新步伐的能力：自上线以

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	其他相关定义应载入合同，并由提供外包服务的机构签署。服务合同至少应包含以下内容： a)与服务水平相关的定义。 b)服务终止的条件，以及在服务终止的情况下，将属于机构、组织和合作伙伴关系的所有数据交付给机构、组织和合作伙伴关系，并在服务提供商组织内安全且不可逆转地销毁这些数据的义务。 c)服务意外终止或中断时应采取的制裁措施。 c)关于机构、组织和合作伙伴关系信息安全政策中重要事项的要求，以及服务提供商在服务期间和之后对所获取的有关机构、组织和合作伙伴关系的信息保密的义务。 d)如果合同中涉及产品的制造，则应规定产品的所有权，并考虑知识产权和工业产权。 e)确保约束外部服务提供商的条款在与分包商的合同中也具有约束力的规定。 f)服务提供商有义务在资本市场法律规定的范围内，按要求的时间和质量，向机构、组织和合伙企业、董事会或董事会认为合适的其他组织提供所要求的信息；董事会和董事会认为合适的其他组织有权查阅服务提供商内部与合同项下提供的服务相关的任何信息、文件和记录。 g)确保服务提供商组织内部发生的安全漏洞或数据泄露等事件立即报告给主管机构、组织和合作伙伴的规定。 g)合同范围内机构、组织和伙伴关系对外部服务提供商的活动进行监测和评估的原则。 h)在相关法律对机构、组织和合伙企业就外包活动施加义务的情况下，应制定条款确保提供外包服务的组织也履行这些		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。 2.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。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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	义务。 （4）对于无法在服务合同第一、二、三款中规定的事项中列明的非关键服务，可以通过标准合同获得，但应当以书面形式说明理由。 （5）授予外部服务提供商的访问权限将逐一进行评估。这些访问权限可能涉及物理或逻辑访问，并会进行风险评估，必要时会建立额外的控制措施。进行风险评估时，会考虑所需的访问类型、待访问数据的敏感性以及访问对信息安全的影响。访问权限包括完成工作所需的最低权限，必要时会设定为与时间相关的权限。如果所接受的服务终止，所有相关的访问权限都将被取消。 （6）机构、组织和合伙企业可将云服务用于其全部或部分活动。云服务的获取、使用和管理均视为外包。 （7）从分销商、供应商或制造商处获得承诺，即外部采购的软件、硬件、操作系统或包含一个或多个此类组件的设备/系统不包含专门设计和/或故意包含的漏洞或缺陷，以绕过现有的安全措施提供访问权限。		
第22条	（1）各机构、组织和合作组织应建立有效的审计追踪记录机制，记录信息系统的使用情况，并应考虑信息系统面临的风险、系统或活动的复杂性和范围。在此范围内，至少应记录以下交易的审计追踪：导致与主要系统和机构、组织及合作组织活动相关的记录发生变更的交易；访问、查询、查看、复制和修改敏感数据的交易；授予、修改和撤销关键信息资产访问权限的功能；以及对这些资产的未经授权的访问尝试。如此，即可确保与信息系统内发生的、导致机构、组织及合作组织活动相关记录发	客户应建立有效的审计追踪记录机制，记录信息系统的使用情况。	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。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。云审计服务记录了租户

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	生变更和删除的交易相关的审计追踪得到充分详细和清晰的记录。应采取措施保护记录机制，防止未经授权的系统和用户访问。 （2）采取必要措施防止审计追踪的完整性受到损害，并检测任何此类损害。定期审查审计追踪的完整性，并将异常情况报告给高级管理层。 （3）审计跟踪中至少应保留以下信息： a)所执行操作的类型和性质。 b)执行该操作的应用程序。 c)执行交易的人的身份。 c)采取行动的时机。 d)操作结果。 e)所访问的系统、接口或文件的名称。 （4）审计跟踪记录至少保留5年。通过在具有足够安全级别的环境中保护审计跟踪记录并进行备份，即使在可能发生的负面事件之后，也能确保在预期期限内可访问这些记录。此外，用于获取和存储审计跟踪记录的工具或方法也受到监控。如果审计跟踪机制出现故障，相关人员将自动收到警报。 （5）用户被告知，他们在信息系统上的活动将被记录。 （6）保留审计跟踪记录不会改变机构、组织和合伙企业根据其所受法律或其他相关法律规定应承担的文件保存义务。 （7）审计追踪记录受到持续监控。针对异常情况，系统建立了自动警报机制，并向相关方发送通知。每条通知都会经过审查，并将结果记录在案。 （8）对于从外部获得的服务，本条款范围内保留审计跟踪记录，并向机构、组织和合作伙伴提供访问权限。 （9）审计跟踪通过中央记录管理系统进行监控和分析。定义		对云服务资源新建、修改、删除等操作的详细信息，记录的事件信息会在云审计中保存7天。如果需要将操作记录保存7天以上，则需要配置事件转储至OBS功能，云审计服务会定期将操作记录同步保存到用户定义的OBS桶中进行长期保存。此功能可实现审计记录永久储存。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	了关联规则并创建了预警机制，以便及早发现可能的安全事件。 （10）负责管理关键活动的信息系统的管理人员和负责管理与这些系统相关的审计跟踪的人员是分开的。		
第23条	（1）机构、组织和伙伴关系的信息系统中使用的时间信息应根据单一参考源进行同步。	客户的信息系统中使用的时间信息应根据单一参考源进行同步。	华为云使用标准NTP4.2.8协议对系统内的时间进行集中式的时钟同步，使得通信设备与通信网的时钟同步，确保系统内各网元时间的一致性。
第24条	（1）各机构、组织和合作组织应建立管控措施，以管理其信息系统中发生的任何信息安全漏洞或已发现的安全隐患。在此方面，所有人员均应了解其职责。漏洞或已发现的安全隐患应尽快记录在案，并采取必要措施。 （2）制定了信息安全漏洞事件或风险评估标准。这些标准至少包括：关键运营和服务可能中断的时间、数据泄露中被盗记录或受影响账户的数量、受影响用户的数量、中断期间及之后的总收入损失，以及违反服务级别协议的百分比。此过程以书面形式记录。 （3）信息安全漏洞事件应对计划已制定并经高级管理层批准。该计划至少应包括： a)事件响应团队的角色、职责和联系方式， b)谁可以报告事件、漏洞或威胁，以及如何报告。 c)内部和外部沟通原则， c)针对每一项当前威胁和潜在网络事件；事件评估、通知相关方、事件响应、恢复、报告、学习和改进等阶段； 它位于那里。 （4）如果确定该事件有可能扰乱关键运营或导致数据泄露，则应立即通知董事会、客户和其他相关机构。 （5）事件发生后，应编制网络安全事件响应报告，记录针对	客户应建立信息安全漏洞事件或风险评估标准。这些标准至少包括：关键运营和服务可能中断的时间、数据泄露中被盗记录或受影响账户的数量、受影响用户的数量、中断期间及之后的总收入损失，以及违反服务级别协议的百分比。	1.作为云服务提供商： a)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。 b)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。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。 2.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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	该事件做出的决策、受事件影响的信息系统和业务流程、所有应对措施、事件的根本原因、相关人员、耗时、成本和人工成本，并提交给高级管理层。如果关键系统或敏感数据受到事件影响，则应立即将编制好的报告提交董事会。 （6）通过培训计划提高参与事件响应过程的人员的能力、经验和知识。 （7）制定了控制措施，以确保收集和完整保存证据，用于法律诉讼。 （8）每年至少进行一次测试，以确保事件响应计划的有效性和时效性，并将测试结果报告给高级管理层。		间内将事件的相关信息通知客户。
第25条	（1）各机构、组织和合伙企业应在信息系统的获取、开发和维护过程中建立必要的控制措施。这些控制措施应涵盖各机构、组织和合伙企业自行开发、修改或通过外包方式获取的所有类型的信息系统。 （2）拟开发、修改或通过外包采购的信息系统的功能需求，以及设计、开发和测试各阶段的技术和安全需求，均应以书面形式明确。在确定应用程序的安全性和可访问性需求时，应考虑机构、组织和合作伙伴确定的数据安全分类和风险。 （3）要开发、修改或从外部来源获取的信息系统结构必须与机构、组织和伙伴关系的规模、其活动的性质和复杂性以及所提供的产品相适应。 （4）考虑到供应商倒闭的风险和重要性，对于由外部公司开发且无法提供源代码的应用程序，在第三方参与下签订软件存储协议。 （5）信息系统中的大规模开发、修改或购置流程均在项目管理框架内进行。拟实施的项目须经机构、组织和合作伙伴	客户应在信息系统的获取、开发和维护过程中建立必要的控制措施。这些控制措施应涵盖组织自行开发、修改或通过外包方式获取的所有类型的信息系统。	华为云提供了一系列用于安全开发的工具和服务，覆盖软件开发全生命周期。 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)。华为云通过CodeArts软件开发生产线提供覆盖软件全生命周期的安全开发能力。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CodeArts提供需求管理服务（Req），支持将功能需求、设计、开发和测试各阶段的技术与安全需求以书面形式明确记录。该服务能够帮助团队结构化地定义和追踪需求，确保在确定应用程序的安全性和可访问性需求时，充分考虑数据安全分类和风险。 3.华为云提供Flexus云服务系列，支持弹性伸缩和按需配置，能够根据机构、组织的规模、活动性质和复杂性灵活调整系统结构。同时，通过项目管理服务实现项目规模的动态适配。 4.华为云所有云服务发布前都经过了多轮安全测试，测试内容包括但不限于接口安全测试，代码扫描，漏洞扫描，渗

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	的高级管理层批准。项目进度报告须定期提交给高级管理层。 （6）建立安全软件开发程序，以涵盖软件开发生命周期的所有阶段。 （7）详细讨论信息系统更新或变更的规划、测试和实施步骤，以便重大更新或变更不会扰乱业务流程，也不会造成信息安全风险。 （8）参与软件开发过程的人员接受安全软件开发方面的培训。 （9）开发环境、测试环境和实际环境相互隔离，以防止未经授权的访问和修改风险。测试环境中的数据不包含客户信息，并且与实际环境中的操作保持一致。 （10）信息系统在实际环境中投入使用前，需确定验收标准，并根据预先制定的计划进行功能、技术和安全需求测试，且其部署到实际环境的审批流程也需跟进。关键应用在投入实际环境前需进行安全测试，并处理发现的任何问题。 （11）如有必要，修改后或新开发的系统应与原系统并行运行，直至达到一定成熟度后方可投入实际环境使用。若无法并行运行，则应保持原系统随时可用，确保数据不丢失，直至修改后或新开发的系统达到一定成熟度。 (12)除非绝对必要，否则应用程序开发人员不得访问真实环境。如有必要，经信息安全官批准，可在有限时间内访问真实环境，但必须保留所有交易的审计跟踪记录。 （13）版本控制工具用于应用程序开发过程中，对源代码所做的更改会反映在版本控制工具中，并附有理由。		透测试。针对外部公司开发且无法提供源代码的应用程序，华为云建议结合第三方软件存储协议（源代码托管）机制进行风险管理。CodeArts的代码托管服务（Repo） 提供了基于Git的高可用代码托管能力，可作为第三方代码托管的基础设施。 5.华为云提供持续集成/持续交付（CI/CD），用于规划、测试和实施系统更新或变更。CodeArts平台的构建服务支持多语言并行构建和可视化交付流水线，能够确保重大更新或变更不会扰乱业务流程，也不会造成信息安全风险。 6.华为云基于经验和实践开发了各种运维，并开设相关的赋能培训课程，帮助参与软件开发过程的人员接受安全软件开发方面的培训，提升开发人员的安全意识和技能。 7.华为云CodeArts平台支持环境隔离机制，开发环境、测试环境和实际环境相互隔离。 8.华为云提供漏洞管理服务和安全测试服务，支持在实际环境中投入使用前，根据预先制定的计划进行功能、技术和安全需求测试。关键应用在投入实际环境前需进行安全测试，并处理发现的任何问题。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
第26条	（1）机构、组织和伙伴关系应制定控制措施，以确保应用程序的安全运行。这些控制措施包括输入输出控制、错误处理、更新、访问控制、移动应用程序和API操作特定问题，并且至少在关键应用程序中应予以考虑。 (2)在应用程序中，数据录入必须完整、准确、有效，以确保数据操作产生准确结果，防止数据丢失、流程丢失、未经授权的修改和滥用。为此，系统建立了输入验证和过滤机制。输入内容经过验证，以防止有害内容的出现。同时，系统确保输入内容符合预定的长度和格式要求。 （3）保证应用程序输出结果的完整性。 （4）应用程序生成的错误消息的结构不会危及系统安全，也不会造成数据泄露的风险。 （5）系统会记录并监控可能对应用程序的保密性、完整性和可访问性产生负面影响的错误。在此情况下，如果检测到错误发生频率高于正常水平，系统会自动向相关人员发送通知。 （6）身份验证数据、个人和财务数据以及类似的敏感数据不会被存储在cookie中。 （7）为确保数据安全，Cookie的保存期限最短，持久性Cookie的保存期限根据安全要求而定。会话Cookie会在会话关闭时自动删除。 （8）每次会话中生成的Cookie都是唯一的。Cookie值对每个用户都是唯一的，并在登录时重新生成。 （9）应用程序的临时用户或访客用户访问权限仅在特定期限内提供，期限到期后将被禁用。 (10)API访问采用安全协议进行	客户应制定控制措施，以确保应用程序的安全运行。这些控制措施包括输入输出控制、错误处理、更新、访问控制、移动应用程序和API操作特定问题。	1.华为云为客户提供基础设施，将基础设施安全视为构筑多维全栈的云安全防护体系的核心组成部分，在物理环境、网络、平台、应用程序接口、数据等主要方面提供了多层次的安全防护。 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CSP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.华为云制定了会话超时策略、账号登陆和锁定策略。其中明确系统支持根据账号、角色、IP等多种特征组合来确定是否允许通过认证建立认证后的会话，同时必须使用会话Token对敏感和关键的操作进行校验以确保会话的真实性。此外管理员在进行系统维护时，查看或检测到非法用户会话时，可通过管理界面强制该用户下线，并清除用户的会话信息。同时设置会话超时机制，在一段时间未收到消息后，可进行会话锁定或返回登录页面，目前超时页面会话为30分钟。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	身份验证和授权。访问请求通过令牌进行验证，用户凭据受到保护。除非绝对必要，否则不会通过API传输敏感数据。 （11）实施流量管理是为了防止API访问过载和滥用行为。为此，采用了需求限制和减速机制。 （12）应用程序的会话超时时间根据应用程序的重要性而定。如果超过此时间，会话将自动终止，用户将被强制重新登录。 （13）应用程序的源代码受到保护，免受恶意使用和干扰。 （14）在应用程序中，建立了控制措施来检测和防止用户提交的所有输入中的恶意内容，并为此目的使用了保护解决方案。 (15)为确保上传至应用程序的文件安全，系统会对文件类型、大小和内容进行检查。系统会根据最新的恶意软件特征码和威胁数据库扫描文件，以防范潜在威胁。任何检测到的可疑文件都会被自动隔离或阻止上传。只有授权人员才能访问已上传的文件，其安全性得到保障。系统会保留访问日志。 （16）除移动应用程序的首次安装、激活或不可用状态外，通过安装激活移动应用程序的客户不会收到用于验证登录或登录期间所执行交易的短信一次性密码，并且此方法不会用作身份验证因素。		
第27条	（1）各机构、组织和合伙企业必须将其主要系统和次要系统设在境内。次要系统的选址应确保其在发生自然灾害和环境灾害时不会面临与主要系统相同的风险。 （2）确定参与信息系统连续性计划制定和实施的人员及其角色和职责，并为其提供相关培训。将决定计划实施的人员和	客户必须将其主要系统和次要系统设在境内。	1.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，华为云在土耳其伊斯坦布尔有3个可用区，在多个相邻国家例如爱尔兰也设有可用区。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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	情况以书面形式记录下来。信息系统连续性计划需经高级管理层批准。确保只有相关人员才能访问该计划，并在必要时保留最新的纸质副本。 （3）在计划范围内建立了一套备用系统。该备用系统用于保存机构、组织和合作伙伴关系的关键数据和系统备份，以备随时使用。 (4)该计划至少应涵盖支持关键业务流程的信息系统及其所在位置，并应考虑与业务部门开展的业务影响分析结果以及业务连续性计划中确定的目标。对于计划中包含的每个流程，都应确定可接受的停机时间和最大可接受的数据丢失值。在此背景下，应建立备用恢复流程和程序，以确保服务能够恢复运行并采取必要的措施。 （5）确定信息系统连续性计划实施时所需的容量，并采取措施提供该容量。 （6）采取必要措施，防止信息系统可能出现的中断，以及可能降低处理性能或扰乱业务连续性的情况。 （7）为了确保信息系统的连续性，开展风险评估、风险降低和风险监控活动。 （8）该计划至少每年审查和更新一次，或在任何可能影响业务流程或信息系统的变更发生后进行更新。为确保计划的有效性和及时性，需进行测试；如有外部服务提供商，则需将其纳入测试；测试结果需报告给高级管理层。测试每年重复进行。 （9）如果主要系统完全瘫痪，机构、组织和伙伴关系必须能够在二十四小时内恢复其活动。 （10）如果主要系统完全瘫痪，应立即通知董事会。 （11）制定从二级系统返回主		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。 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。 当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，使客户只能访问到自己的数据。 2.华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	要系统的程序。 （12）信息系统备份按照业务连续性计划中的优先级进行，并且从备份中恢复的必要流程已纳入信息系统连续性计划和测试中。为此，制定了备份计划，并经高级管理层批准，且确保其保持最新状态。至少一份备份副本存储在不同的地理位置。已采取必要的措施保障备份的安全。 （13）每年至少对关键系统进行一次备份恢复测试，并记录参与人员信息、日期、测试详情和结果。确保所做备份在法定保存期限内可恢复。 （14）机构、组织和伙伴关系应在其信息系统中建立必要的基础设施，以确保其能够在业务连续性计划中确定的可接受停机时间和最大数据丢失值范围内继续开展活动。 （15）机构、组织和伙伴关系应在其信息系统中建立冗余运行或备用安排，以防止其关键活动无法运行。 （16）机构、组织和合作伙伴应在安全的环境中保存其信息安全政策、信息系统连续性计划、信息资产清单以及其他对业务连续性和安全性至关重要的文件和与信息系统管理相关的密码的最新版本。		
第28条	（1）机构、组织和伙伴关系应制定控制措施，以管理对其信息系统的所有软件、硬件和基础设施组件、文档和信息所做的变更。这些控制措施至少包括以下内容： a)对于任何需要进行的变更，都将创建记录，描述变更的原因、范围、影响、涉及的风险、预期收益、变更执行人员、成本以及必要的测试和培训活动。 b)在实施计划变更之前，会进行详细的测试过程，以验证这	客户应制定控制措施，以管理并记录对其信息系统的所有软件、硬件和基础设施组件、文档和信息所做的变更。	华为云作为云服务供应商，负责其提供的基础设施和IaaS、PaaS和SaaS各类各项云服务的变更管理。华为云制定了完善的变更管理流程并定期对其评审和更新。按照变更可能对业务造成影响的程度定义了变更类别和变更窗口，以及变更通告机制。该流程要求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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
	些变更的可靠性和功能性，并确保变更后系统和应用程序的配置设置和版本设置正确。 c)计划变更必须经过审批程序才能进行；但是，对于紧急变更将制定特殊程序，以确保尽快完成此类变更的文档和记录。 c)计划变更、调试日期、测试和培训活动将提前通知所有相关方。 d)如果在实施变更过程中出现错误或不可预见的情况，则应事先确定要应用的回滚程序和相关责任，并在可能的情况下测试这些程序。 e)对已实施的变更的结果进行审查。 f)所有已作出的变更、已取消的变更或已拒绝的变更都会被记录并存储，同时记录变更的原因。		以及所有可能的影响。 华为云提供在线版本的**《华为云云服务等级协议》**，明确了提供的服务的内容和级别，以及华为云的职责。华为云将派专人积极配合客户的尽职调查。客户在华为云的审计和监督权将根据情况在与客户签署的协议中承诺。

 版权所有 © 华为云计算技术有限公司

8 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。	资产管理 漏洞管理 入侵检测

版权所有 © 华为云计算技术有限公司

	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。	
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
DDoS防护 Anti-DDoS Service (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	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

版权所有 © 华为云计算技术有限公司

- **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	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、	安全审计

版权所有 © 华为云计算技术有限公司

Service (LTS)	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。	
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

版权所有 © 华为云计算技术有限公司

9 结语

华为云致力于为土耳其云用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监管重点领域下的安全实践，有助于土耳其云用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、构建和部署符合土耳其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监管要求的遵从性。

 版权所有 © 华为云计算技术有限公司

10 版本历史

日期	版本	描述
2026年7月	1.0	首次发布

版权所有 © 华为云计算技术有限公司