华为云意大利
网络安全监管要求遵从性指南

文档版本 1.0

发布日期 2026-05-18

华为云计算技术有限公司

商标声明

和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为云计算技术有限公司

地址: 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址: **https://www.huaweicloud.com/**

目 录

1 概述

1.1 背景与发布目的

随着数字化转型的持续推进，意大利公共行政机构不断加快信息系统上云、基础设施整合以及数字服务重构进程。与此同时，云计算、数据迁移、数字基础设施外包以及关键信息技术产品采购等活动，也使公共部门在数据安全、业务连续性、供应链安全和国家网络安全方面面临更高要求。为规范公共部门对数字基础设施和云服务的使用，并加强涉及国家战略利益和国家安全场景下的信息技术采购安全，意大利主管机构陆续发布了一系列监管规则，对公共行政机构数字基础设施、云服务、迁移安排、服务资质以及网络安全采购要求做出了较为系统的规定。

华为云作为云服务提供商，致力于协助客户满足当地监管要求，持续为客户提供符合意大利网络安全与云治理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意大利监管要求，详细阐述华为云将如何协助其满足相关合规要求。

1.2 适用的网络安全监管要求简介

意大利国家网络安全局（Agenzia per la Cybersicurezza Nazionale, ACN）是意大利网络安全治理的重要主管机构，负责国家网络安全体系建设、公共行政云安全规则制定、云服务资格管理以及相关技术标准和程序要求的落地执行。在公共行政数字化与云迁移领域，ACN 与意大利总理府数字化转型主管部门共同推动公共部门数据、数字服务和基础设施向符合国家要求的云环境迁移，并通过分类分级、最低安全要求、迁移计划和资质审查等机制，强化公共行政领域的云安全治理。

- **《用于保护国家战略利益和国家安全背景下的信息技术产品和服务合同规则》（Regulations on the Management of Procurement Contracts for Information Technology Products and Services Involving National Strategic Interests and National Security）：**意大利 2025 年 4 月 30 日发布了《用于保护国家战略利益和国家安全背景下的信息技术产品和服务合同规则》，该规则提出在国家战略利益和国家安全保护背景下使用的信息技术产品和服务采购活动（含云服务），服务提供商限定为公共机构或者按照 ACN n.21007 的要求获取公共行政部门云服务资格认证的私营主体，产品和服务需要满足网络安全核心要素。
- **《公共行政数字基础设施和云服务条例》（ACN n.21007）：**该条例围绕公共行政数字基础设施、云服务、数据和数字服务分类、迁移安排以及云服务资格认定程

序建立了系统规则，明确了公共行政机构在最低安全水平、云服务质量与安全特性、迁移期限与方式以及云服务适配和资质审查方面应遵循的具体要求。

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。

- **云服务**

  是指云服务提供商根据用户请求，通过互联网以云计算模式提供的 IT 服务和计算资源，根据计算模式可将云服务分成基础设施即服务（Infrastructure-as-a-Service，IaaS）、平台即服务（Platform-as-a-Service，PaaS）、软件即服务（Software-as-a-Service，SaaS）三类。

- **云服务提供者**

  指向公共行政部门提供云服务的公私主体，其亦可通过分销商、经销商或增值服务提供者提供服务，但前述中介在不决定服务交付方式和手段的情况下，不被视为云服务提供者。

- **公共行政云服务**

  指支持公共行政机构用于向公众提供数字服务的云服务。

- **数字服务**

  指通过行政机关的网络和信息系统，或通过代表行政机关的第三方网络和信息系统，向第三方、行政机关内部或为支持行政机关的服务而提供的信息技术服务，但不包括基础信息通信技术服务。行政部门数据和数字服务，根据其特征分为以下三类：

  战略类——指其受损可能对国家安全造成不利影响的公共行政数据或数字服务。

  关键类——指其受损可能对社会相关功能维持、公共健康、公共安全以及国家经济和社会福祉造成不利影响的公共行政数据或数字服务。

  普通类——指其受损不会造成“关键”或“战略”等级所对应不利影响的公共行政数据或数字服务。

- **公共行政机构数字基础设施**

  指用于提供公共行政机构数字服务的数字基础设施，涵盖：数据处理中心（含计算、网络及存储资源）、第三方提供的云组件（含托管）以及第三方提供的旨在优化服务交付性能的边缘本地设施（如边缘数据中心服务器）。

- **公共行政机构云服务基础设施**

  由数字基础设施运营者提供并用于向公共行政部门交付云服务的数字基础设施。

2 华为云安全合规

华为云继承了华为公司完备的管理体系以及 IT 系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多全球性、区域性和行业特定的安全合规的权威认证，全力保障客户部署业务的安全。

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

华为云部分标准类认证/鉴证示例：

认证	描述
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，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。
ENS	ENS（西班牙语：Esquema Nacional de Seguridad，ENS）是西班牙国家安全认证计划，其通用框架分为基本原则、控制要求和安全措施三个部分。ENS适用于所有西班牙公共部门以及与西班牙政府合作的供应商。认证的目的是确保组织管理的数据、信息和服务在机密性、完整性、可追溯性、真实性和可用性五个维度中得到充分保护。

认证	描述
C5	C5全称Cloud Computing Compliance Criteria Catalogue（云计算合规标准目录），是由德国联邦信息安全办公室（BSI）针对云服务商制定的安全标准，旨在基于标准化的检查和报告来说明云服务提供商的信息安全性。C5目前已经广泛地被欧洲乃至全世界的企业使用，是云服务领域受到充分认可的高级别安全标准。C5:2020基于《欧洲网络安全法》对云服务产品的信息安全标准进行了延伸（e.g. 标准化云服务提供商处理政府机构查询的行为），提升了服务提供商行为的规范和严谨性。
EU Cloud CoC	《欧盟云行为准则（EU Cloud CoC）》是欧洲数据保护委员会（EDPB）签署的跨国运营合规行为准则，旨在为云服务商提供明确的指导，帮助其遵守《通用数据保护条例（GDPR）第28条-数据处理者》规定的义务。 获得《欧盟云行为准则》认证可作为云服务商面向欧盟监管机构和云用户的合规证明。 该合规性工具适用于提供不同云服务模式的各种规模的企业。
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TL 9000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。

认证	描述
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息的保密性、完整性、可审计性和可用性的指导。 华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。
ISO 27034	ISO/IEC 27034是国际标准化组织ISO通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得ISO/IEC 27034认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。
SOC 审计报告	SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控 制情况出具的独立审计报告。

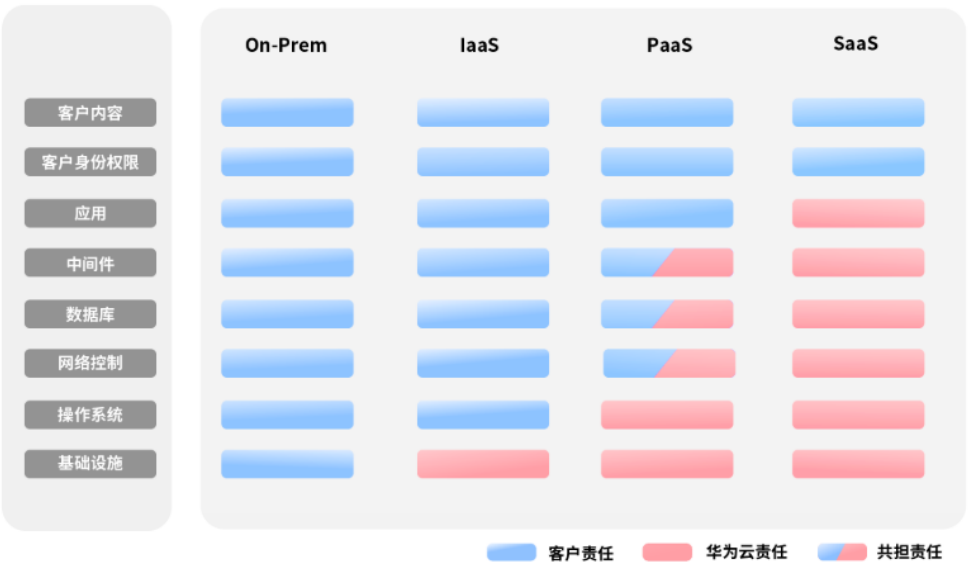
3 华为云责任共担模型

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

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

在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。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**”。

5 华为云如何遵从及协助客户满足《用于保护国家战略利益和国家安全背景下的信息技术产品和服务合同规则》的要求

意大利 2025 年 4 月 30 日发布了《用于保护国家战略利益和国家安全背景下的信息技术产品和服务合同规则》，该规则提出在国家战略利益和国家安全保护背景下使用的信息技术产品和服务采购活动（含云服务），服务提供商限定为公共机构或者按照 ACN n.21007 的要求获取公共行政部门云服务资格认证的私营主体，产品和服务需要满足网络安全核心要素。

客户在遵循上述规则要求时，华为云作为云服务提供商，可能会参与到相关信息技术服务供应、云环境支撑及网络安全能力保障等活动中。以下内容将总结该规则中与云服务提供商相关的控制要求，并阐述华为云作为云服务提供商，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
第一部分：产品及服务属性要求	1）信息技术产品和服务的设计、开发、生产和供应确保基于风险管控原则实现适当网络安全水平。	客户采购的信息技术产品和服务时，应关注信息技术产品和服务是否在设计、开发、生产和供应全生命周期中基于风险管控原则实现适当网络安全水平。	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现。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

编号	具体控制要求	客户关注点	华为云的应答
			控制、数据传输通道审批和审计等保护措施。
	2）基于网络安全风险评估，信息技术产品和服务应当 a) 交付时不存在已知可被利用的安全漏洞；	客户采购的信息技术产品和服务交付时应不存在已知可被利用的漏洞。	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，确保提供时不存在已知可被利用的漏洞。
	b) 提供预设安全配置选项，并支持恢复至原始状态功能；	客户采购时应关注，信息技术产品和服务以默认安全配置提供，并允许将相关信息技术产品或服务恢复至原始状态。	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。
	c) 通过安全更新（含自动更新）及时处理漏洞，默认启用自动更新功能，提供清晰、便捷的更新暂停机制，并向用户推送可用更新通知；	客户采购时应关注，信息技术产品和服务应确保可通过安全更新处理漏洞，并默认启用自动安全更新功能，同时提供更新通知和暂停更新的功能。	作为云服务提供商，华为安全运营中心（SOC）已经建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，使基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在SLA时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响用户业务的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对用户业务造成影响。 客户也可以使用华为云的**企业主机安全（Host Security Service，简称HSS）**中提供的漏洞管理功能，其可以检测Windows/Linux操作系统与SSH、OpenSSL、Apache、Mysql等软件存在的漏洞，并给出修复建议，Linux软件漏洞和Windows系统漏洞还支持控制台一键漏洞修复。
	d)采用身份认证、访问管理等机制防止未授权访问，实时监测并报告未授权访问行为;	客户采购时应关注，信息技术产品和服务应通过适当控制机制防止未经授权的访问。	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。以此确保

编号	具体控制要求	客户关注点	华为云的应答
			用户隐私和数据不受未授权访问。此外，华为云通过**云审计服务（Cloud TraceService，简称CTS）**为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用，租户可在CTS查看IAM的关键操作，并设置关键操作通知，以实时监测并报告未授权行为。
	e)对存储、传输及处理的个人和非个人数据，采取加密等先进技术保护；	客户采购时应关注，信息技术产品和服务应通过采用最先进技术，保护所存储、传输或以其他方式处理的数据的保密性，包括对静态或传输中的相关数据进行加密的系统。	针对于加密，华为云自身使用行业广泛使用的国际通用的AES强效加密法对平台内的数据进行加密。**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。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。对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过虚拟专用网络（VPN和应用层 TLS 与证书管理，华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。
	f)防止用户未授权的数据、指令、程序及配置篡改，并具备异常篡改告警功能;	客户采购的信息技术产品和服务时，信息技术产品和服务应保护所存储、传输或以其他方式处理的数据、命令、程序和配置的完整性，防止用户实施任何未经授权的篡改或修改，并对	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。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

编号	具体控制要求	客户关注点	华为云的应答
		数据损坏进行报告。	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，以此来实现防止未授权的篡改。 华为云通过**企业主机安全（Host Security Service，简称 HSS）**实现对未授权篡改行为的检测与告警。企业主机安全是华为云提供的核心主机防护产品，其入侵检测功能能够实时监控主机内部的风险异变，并对多种未授权篡改行为进行告警。
	g) 仅处理与预定目的相符的必要数据（数据最小化）；	客户采购的信息技术产品和服务时，信息技术产品和服务应仅处理与预定目的相适应、相关且限于必要范围内的数据。	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。协助客户满足仅处理与预定目的相适应、相关且限于必要范围内的数据要求。
	h)确保核心功能在遭受攻击（如拒绝服务攻击）后仍可持续运行； i)最小化对其他设备或网络服务可用性的影响；	客户采购的信息技术产品和服务时，信息技术产品和服务在发生事件之后，也应保护基本和关键功能的可用性，包括通过针对拒绝服务攻击的韧性和缓解措施。	华为云作为CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS各类各项云服务的重大事件管理。华为云拥有集中、完整的日志审计系统。并利用大数据安全分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。华为云拥有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重大事件。并根据事件的实时状态进行事件升级和通报。 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韧性和可用性，数据中心按规则部署在全球各地，客户可通过两地互为冗余，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，保证业务的持续运行。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。

编号	具体控制要求	客户关注点	华为云的应答
	l) 在设计、开发、生产及供应环节，采取限制攻击面的措施，包括外部接口；	客户采购的信息技术产品和服务时，信息技术产品和服务应尽量减少其对其他设备或网络所提供服务可用性的负面影响。	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现。 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。
	m) 在设计、开发、生产和供应时，应通过适当的缓解机制和技术降低安全事件影响；	客户采购的信息技术产品和服务时，信息技术产品和服务在设计、开发、生产和提供时，应限制攻击面，包括外部接口，通过适当的缓解机制和技术降低事件影响。	华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套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。此外，华为云云平台版本、重要云服务上线前，需要通过华为公司安全管理部门和首席法务官的严格审查，针对所服务区域的安全隐私要求的遵从性进行分析、判断，确保为华为云以及华为开发的云服务满足各区域法律法规和客户安全需求。华为云严格遵从

编号	具体控制要求	客户关注点	华为云的应答
			多种编程语言的安全编码规范。使用静态代码扫描工具例行检查，其结果数据进入云服务工具链，以评估编码的质量。所有云服务在发布前，均须完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。
	n) 记录和监测关键操作日志（数据、服务或功能的访问及其修改），并为用户提供停用机制；	客户采购的信息技术产品和服务时，信息技术产品和服务应记录和监测相关内部活动。	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。客户可在CTS上创建追踪器实现各种云资源操作记录追踪，追踪器可由客户自主启用或者停用。
	o) 为用户提供以安全、便捷且永久的方式删除全部数据和全部设置的可能；如该等数据可转移至其他信息技术产品和服务，还应确保转移过程安全。	客户采购的信息技术产品和服务时，信息技术产品和服务应为用户提供删除全部数据和设置的途径、安全的数据迁移方式。	在华为云的责任共担模型中，无论使用哪一项华为云服务，租户始终是其数据的所有者和控制者。租户负责各项具体的数据安全配置，对其保密性、完整性、可用性以及数据访问的身份验证和鉴权进行有效保障。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。华为云提供的**云数据迁移（Cloud Data Migration，简称CDM）**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。
第二部分：漏洞管理要求	1. 信息技术产品和服务的提供方应履行如下义务： a)识别并记录信息技术产品或服务中包含的漏洞和组件，并编制软件物料清单，清单需要使用通用且自动化设备可读取的格式，至少包括一级依赖关	信息技术产品和服务的供应方应建立全面的安全保障闭环。包括识别并记录产品组件与漏洞，编制软件物料清单；及时提供安全更新并修复漏洞；定期进行安	作为云服务提供商，为配合客户符合监管要求： 1.说明针对不同的云产品和服务类型不同，客户和华为云承担不同的安全责任，详见本文第 3 章华为云责任共担模型。

编号	具体控制要求	客户关注点	华为云的应答
	系； b)针对信息技术产品和服务带来的风险，及时处置和修复漏洞，包括提供安全更新；在技术上可行的情况下，新的安全更新应与功能更新分开提供； c) 对信息技术产品和服务的安全性开展有效、定期的测试和复审； d)安全更新发布后，应当向用户公开漏洞详情，包括漏洞说明、使用户能够识别受影响信息技术产品或服务的信息、漏洞影响、严重程度，以及帮助用户修复漏洞的清晰且易获取的信息；在具有充分正当理由的情况下，如披露带来的安全风险高于其安全收益，可延迟披露直至客户完成安装（符合2024年第138号法令第16条） e)建立第三方组件漏洞信息共享机制，并提供专用报送联系方式; f)建立安全可靠的更新分发机制，确保漏洞被及时修复或缓解；对于安全类更新，在适用的情况下应实现自动分发功能； g) 识别并评估第三方供应商及合作伙伴，实施供应链网络安全风险评估； h) 免费及时推送安全更新呢，并附含应对措施的安全通告。	全测试与复审。同时，需向用户清晰披露漏洞及修复信息，并建立漏洞信息共享与报告机制。更新应以安全方式分发，并尽可能自动化。此外，应对第三方供应商进行识别与风险评估，并确保在有条件时免费、及时地发布安全更新。	客户可以通过**企业主机安全（Host Security Service，简称HSS）**中的漏洞管理功能对云上资产进行漏洞检测，自动生成漏洞清单，漏洞清单包含漏洞相关组件的详细信息。 2.针对常见 CVE 漏洞，华为云将立即分析和更新规则，提供快速、专业的 CVE 漏洞扫描。客户可以部署 **Web 应用防火墙（Web Application Firewall，简称WAF）**，从多维度检测和保护网站业务流量。 3.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.华为云根据漏洞分析结果决定是否对外披露漏洞，在官网提供安全公告以及漏洞反馈页面，向客户共享、通知、披露最新的安全漏洞告警。 5.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。 6．**企业主机安全（Host Security Service，简称 HSS）**：支持检测 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞和应急漏洞。其漏洞库会实时更新，新型漏洞可在 24 小时内添加入库。HSS 可以对系统漏洞执行一键自动修复。HSS 每日凌晨自动进行漏洞检测，并将官方补丁信息推送给用户。安全云脑自动抓取和推送应急漏洞公告。当 HSS 扫描到服务器存在漏洞时，

编号	具体控制要求	客户关注点	华为云的应答
			客户可以根据漏洞的危害程度结合实际业务情况，选择自动修复、手动修复、忽略漏洞以及添加漏洞白名单方式处理漏洞 7. 华为云会安排专人积极配合客户发起的审计要求和尽职调查。华为云参照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。全方位保护客户系统和数据的保密性、完整性和可用性。 8. 华为会通过安全通告（SA） 的形式对在服务支持周期内的产品和已购买相应安全服务的客户发布漏洞修补方案推送。

6 华为云如何遵从及协助客户满足《公共行政数字基础设施和云服务条例》的要求

意大利国家网络安全局（ACN）于 2024 年 6 月 27 日发布《公共行政数字基础设施和云服务条例》，旨在构建统一监管框架，规范公共行政数字基础设施、云服务治理。该条例以数据和数字服务的关键性，将其分为“普通”、“关键”和“战略”三类，并据此设定差异化的安全标准。对于公共行政数字基础设施及公共行政云服务基础设施，条例规定不同类型数字服务应满足的最低安全水平、处理能力、节能和可靠性要求。对于公共行政云服务，条例重点规定云服务本身应具备的质量、安全、性能与可扩展性、互操作性和可移植性特征。

当客户遵循上述要求时，华为云作为云服务提供商，可能会参与到要求所涉及的部分活动中。以下内容将总结该条例中与云服务提供商直接相关的安全控制要求，并阐述华为云作为云服务提供商，会如何帮助客户满足这些安全控制要求。

6.1 数字基础设施及公共行政服务基础设施的最低标准

6.1.1 识别

编号	具体控制要求	客户关注点	华为云的应答
资产管理（ID.AM）：组织所需的数据、人员、设备、系统及设施均已明确识别，并根据组织的风险目标和策略进行管理。			
ID.AM-01 - 对组织内使用的系统和物理设备进行资产盘点	**普通类** 1_O 所有系统和物理设备均已登记造册，并存在一份由该主体内部相关人员批准的设备清单。 2_O 网络中存在的所有系统和物理设备均已登记造册，且仅允许经批准的系统和设备接入网络。 **关键类** 同普通类要求。	客户所有系统和物理设备需登记造册并形成经批准的清单。同时，网络接入应严格受限，仅允许清单内经批准的设备接入，并通过技术手段确保合规。	华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。华为云接入网络的设备通过证书与网络控制器进行身份验证，确保接入网络的设备真实可靠。

编号	具体控制要求	客户关注点	华为云的应答
	战略类 同关键类要求。		
ID.AM-02 - 对组织内使用的平台和软件应用进行盘点	**普通类** 无要求。 **关键类** 1_C 所有已安装平台和软件应用均应登记造册，并应有一份由主体内部相关方批准的软件和平台清单。 2_C 仅允许安装已获批准的平台和软件应用。 3_C 应制定政策，限制对组织资产进行未经授权的新增、移除、更新或管理。 **战略类** 同关键类要求。	对于关键类和战略类服务，所有已安装平台和软件应用均应登记造册，并应有一份由主体内部相关方批准的软件和平台清单。仅允许安装已获批准的平台和软件应用，限制对组织资产进行未经授权的新增、移除、更新或管理。	华为云定期对华为云的硬件、软件、数据、人员和服务进行识别。华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。 华为云提供的**配置审计 Config** 支持客户实现云上平台资产管理。Config提供全局资源配置的检索，资源清单，资源记录器，配置历史追溯，以及基于资源配置的持续的审计评估能力，确保云上资源配置变更符合客户预期。客户可以使用Config查看自己所拥有的资源有哪些；可以查看资源详情、资源之间的关系、资源历史；Config会在资源变更时发送消息通知，并定期（6小时）对客户的资源变更消息进行存储；Config还会定期（24小时）对客户的资源进行存储；客户还可以通过配置合规规则来对自己的资源进行合规性检查。
ID.AM-03：已识别出与该组织相关的数据流和通信	**普通类** 1_O. 所有数据和信息流，包括对外传输的数据流以及与数字基础设施相关的数据流，均由该主体内部人员进行识别、登记和审批。 **关键类** 同普通类要求。 **战略类** 同关键类要求。	客户所有数据和信息流，包括对外传输的数据流以及与数字基础设施相关的数据流，均由该主体内部人员进行识别、登记和审批。	客户可以使用华为云**数据安全中心服务（Data Security Center，简称DSC）**实现对外传输的数据流以及与数字基础设施相关的数据流的安全控制。 每个云服务在设计研发阶段都应制定数据流图，通过数据流转图展示业务中各种数据的生命周期以及华为云所执行的操作，并明确操作目的。各业务领域在充分识别本领域数据资产的基础上，形成数据资产清单与数据流图，每年例行盘点。
ID.AM-06：已明确并公布了全体员工 以及相关第三方	**普通类** 1_O. 应界定并向主体内相关部门公开其网络安全组织设置，包括面向所有人员及相关第三方的角色和职责。 2_O. 在网络安全组织架构	客户应明确并公开网络安全组织架构，包括所有人员及第三方的角色与职责；在该架构内，指定一名具备专业能力的负责人（及替补），负责整体合规实施并向	1. 在公司层面，华为云的最高管理层负责决策和批准公司总体网络安全战略。华为与安全管理部门负责制定和执行华为端到端网络安全保障体系与安全策略，并定期对策略的执行情况进行定期审视，确保安全治

编号	具体控制要求	客户关注点	华为云的应答
（例如供应商、客户、合作伙伴）在网络安全方面的职责与责任	内，应指定一名负责人及其替代人员，负责管理本规章规定的实施；该负责人应具备网络安全领域的专门专业能力，直接向主体管理层汇报，并确保本附件规定的安全措施得到有效落实。 3_O. 在网络安全组织架构内，还应指定一名技术联络人及至少一名替代人员，具备网络安全专业技术能力，负责与 CSIRT Italia 就影响云服务的事件管理进行对接。 4_O. 网络安全负责人和技术联络人应保持紧密协作。 **关键类** 5_C. 主体应将网络安全负责人以及技术联络人的姓名和联系方式报送国家网络安全局（ACN）。 6_C. 应建立一份清单，载明参与网络安全流程且具有特定角色和职责的全部内部和外部人员；该清单应传达至主体相关部门。 7_C. 就外部依赖关系而言，应建立一份第三方网络安全负责人及技术联络人相对应人员的清单；就内部依赖关系而言，也应建立主体内部对应人员清单。负责人和技术联络人的能力要求应根据依赖类型重新评估。该清单应传达至主体相关部门。 8_C. 网络安全负责人还应确保与 ACN 开展协作。 **战略类** 5_S. 该主体应向国家网络安全局（ACN）通报第2_O条所述负责人的姓名及联系方式，以及第3_O条所述技术联络人的	管理层汇报；同时指定一名具备技术能力的技术联络人（及至少一名替补），负责与国家级应急团队对接事件管理；负责人与技术联络人必须保持紧密协作。 对于关键类服务，客户应向国家网络安全局（ACN）报备网络安全负责人与技术联络人的姓名及联系方式。建立并传达一份包含所有参与网络安全流程的内外部人员及其职责的清单。 分别建立并传达外部第三方及内部对应的网络安全对接人员清单，并根据依赖关系重新评估其能力要求。 网络安全负责人需确保与ACN开展协作，包括参与法定网络安全活动及国家网络危机管理相关工作。	理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。同时，华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。 2. 华为云根据法律要求，设立了数据保护官。如有任何问题、意见或建议等，客户可以通过 **dposg@huaweicloud.com** 与数据保护官联系。

编号	具体控制要求	客户关注点	华为云的应答
	姓名及联系方式。		
治理（ID.GV）：用于管理和监控组织各项要求（包括组织要求、法律要求、风险相关要求及环境要求）的政策、程序和流程，均被纳入并应用于网络安全风险管理中。			
ID.GV-01 - 制定并公布网络安全政策	**普通类** 1_O 应有文件化网络安全政策、流程和程序并保持最新； **关键类** 2_C 网络安全文件应由主体批准，并至少每年更新一次，或在组织内部发生重大变化时更新。 **战略类** 3_S 网络安全所述文件中内部确定的最低安全等级的任何偏离，均应形成正式理由并获得授权。 4_S 应有一份最新文件，就网络安全项目的规划、角色分配、实施、运行、评估和改进提供说明，该文件既适用于内部人员，也适用于任何第三方。	客户应制定并公布网络安全政策。 对于关键类服务，文件应每年更新一次，或在组织内部发生重大变化时更新。 对于战略类服务，内部确定的最低安全等级的任何偏离，都必须形成正式文件说明理由并获得授权。同时，应制定一份最新的、适用于全体人员及任何第三方的文件，用以详细说明网络安全项目的规划、角色分配、实施、运行、评估和改进的全过程。	1. 华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批。 2. 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。 3. 华为云计算首席安全与隐私保护管负责制定华为云端到端的网络安全与隐私保护找略，推动集团安全与隐私保护战略在华为云的有效落地，组织制定华为云安全与隐私保护业务规划，管理和监督各业务部门制定安全竞争力规划并落地。 4. 华为云建立完善的安全隐私稽查机制，华为云每年将根据外部环境变化和内容情况开展稽查，同时，每年也会聘请第三方提供审计服务。审计结果的追踪通过华为云安全风险管理平台实现，包括问题记录、定级、进展跟踪和提醒，确保准时整改完成。
ID.GV-04：治理与风险管理流程包括网络安全相关风险的管理	**普通类** 无要求。 **关键类** 1_C. 已建立正式的企业风险管理（ERM）计划，其中包含用于识别、评估、归属、处理和接受基础设施安全与隐私风险的政策和程序。 **战略类** 同关键类要求。	客户应建立正式的企业风险管理（ERM）计划，其中包含用于识别、评估、归属、处理和接受基础设施安全与隐私风险的政策和程序。	华为云制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云

编号	具体控制要求	客户关注点	华为云的应答
			对外包商进行严格的安全管理，定期对供应商进行审计和评估。
风险评估（ID.RA）：企业需全面了解与组织运营（包括使命、职能、形象或声誉）、资产及人员相关的网络安全风险。			
ID.RA-01：已识别并记录组织资源（例如系统、场所、设备）的漏洞	**普通类** 1_O 应存在一份最新的安全核查和测试计划，说明旨在评估数字基础设施网络安全水平以及技术和程序性安全措施有效性的一系列活动，并载明实施频率和方式。 2_O 应存在用于管理与组织资产变更相关风险的程序，并至少每年更新一次。该等资产包括应用、系统、基础设施、配置等，无论其由内部还是外部（即外包）管理。 **关键类** 同普通类要求。 **战略类** 3_S 定期报告至少应包括： a. 已开展检查类型及其结果的总体说明； b. 已发现漏洞及其对应安全影响等级的详细说明；c. 通过利用漏洞可能访问到的系统资源暴露程度。 4_S 应有一份最新文件，说明漏洞评估和渗透测试的流程与方法。	客户应建立安全检查计划、组织资产变更风险管理程序，并至少每年更新一次。 对于战略类数据或资产，还应建立漏洞评估和渗透测试方法，并定期报告检查总体情况（含类型和接结果）、漏洞及影响等级、漏洞影响范围。	华为云内部制定完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。 华为云已发布漏洞管理和渗透测试相关的制度，明确漏洞评估和渗透测试的流程与方法，并且每年对这些制度进行审视和刷新。 华为云风险管理人员遵循制定的网络安全风险管理规范，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划，包括整改措施、计划、关键里程碑和风险降级标准，利用风险整改、风险保持、风险避免和风险转移等措施降低和消除风险至可接受范围。
ID.RA-05：威胁、脆弱性、相关发生概率及随之产生的影响被用于确定风险	**普通类** 1_O 风险分析应根据所考虑的威胁、脆弱性、其各自发生概率以及在其被利用时产生的后果影响来开展。 2_O 风险分析应考虑数字基础设施的内部和外部依赖关系。 3_O 在识别并分析所有风险因素后，应进行权衡，以确定风险等级。 **关键类** 4_C 应有一份最新的风险评估文件，至少包括： a. 内部和外部威胁的识别、适当描述与评估，以及其	客户应进行风险分析，考虑数字基础设施的内部和外部依赖关系。在识别并分析所有风险因素后，应进行权衡，以确定风险等级。 对于关键类服务，应有一份最新的风险评估文件。	华为云制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。 华为云建立并实施了文档化的网络风险安全政策和程序，为操作网络

编号	具体控制要求	客户关注点	华为云的应答
	发生概率； b. ID.RA-1 子类别和 DE.CM-8 子类别所述漏洞；c. 被认为会对基础设施产生重大影响的潜在影响，并对其进行适当描述和评估；d. 用于评估风险并确定处置优先级的标准。 **战略类** 同关键类要求。		安全管理提供指导，风险评估程序中要求进行内外部威胁识别、风险分析和定级、风险处置要求，网络安全政策和程序发布前需得到管理者审批。
供应链风险管理（ID.SC）：组织已确定其优先事项、约束条件、风险容忍度及假设，并将其用于支持与供应链风险管理相关的风险决策。组织已制定并实施了用于识别、评估和管理供应链风险的流程。			
ID.SC-01 - 识别并管理网络供应链风险管理流程	**普通类** 无要求。 **关键类** 1_C 应有网络供应链风险管理流程并保持最新。 2_C 流程应经主体高层评审批准。 **战略类** 3_S 组织应建立制定、实施和应用针对外部主体和第三方行政机构的共同安全责任模型（Shared Security Responsibility Model-SSRM）,并每年更新一次。 4_S SSRM模型应适用于包括数字基础设施在内的整个网络安全供应链。	关键类服务应建立网络供应链风险管理流程，战略类服务还应制定适用于整个网络安全供应链及相关行政机构的共享安全责任模型（SSRM）并至少每年更新一次。	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。 华为云建立了严密的安全责任体系，根据华为云安全责任共担模型，对于部署在华为云环境的部分，客户可以依赖华为云的符合性证明。 华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。
ID.SC-02 - 识别并评估第三方 IT 系统、组件和服务供应商/合作伙伴	**普通类** 无要求。 **关键类** 同普通类要求。 **战略类** 1_S 采购时应至少采取如下供应链安全措施： a. 网络安全负责人自设计阶段起参与采购流程； b. 符合可替代性要求，并允许在到期时转用其他供应	对于战略类服务，采购时应保障在网络安全负责人在设计阶段开始参与、供应商符合替代性要求、供应商多元化、对供应商进行技术可靠性评估，并且建立包括技术可靠性评估记录的供应商清单。 可行情况下，技术可靠性评估可增加源代码共享、第三方认证、使用流程和工具保障系统完	华为云会安排专人积极配合客户发起的背调要求和尽职调查。同时，华为云在采购前会对供应商资质进行评估，根据供应商所提供的产品和服务制定不同级别的评估要求，仅经过资质认证的供应商才能进入华为云的采购范围。华为云建立并维护供应商清单，每年对供应商的安全风险进行评估。 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

编号	具体控制要求	客户关注点	华为云的应答
	商，除非有被证明的技术限制； c. 实现供应商多元化，从而增强数字基础设施的韧性，除非有被证明的技术限制； d. 参照相关领域的最佳实践对供应商和第三方合作伙伴进行技术可靠性评估，评估至少考虑以下方面： 1) 供应商及第三方合作伙伴的产品质量和网络安全措施，包括其对自身供应链的管控情况以及对安全问题的重视程度； 2) 供应商及第三方合作伙伴长期保障供货、技术支持及维护的能力。 2_S 建立并维护提供数字基础设施服务的供应商（含合作伙伴、外部分支机构）清单，清单中应包括供应商的技术可靠性评估记录。 3_S 在可行的情况下，并根据以下事项的重要程度，建议： a. 评估第1_S条d款中提到的技术可靠性时，还应考虑： 1) 供应商是否愿意共享源代码； 2) 是否存在有助于评估制造商软件开发过程质量的认证或证明材料； 3) 制造商是否采用了技术流程和工具，以确保信息和通信技术资产及系统中安装的软件或固件的真实性和完整性； 4) 制造商是否采用了流程和技术工具，以确保源代码与已安装和执行的目标	整真实和代码一致性等方面的评估；采用工具评估代码质量安全、提取系统代码、检测代码一致性。	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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。

编号	具体控制要求	客户关注点	华为云的应答
	代码之间具有一一对应关系； b. 采用相应的流程和技术工具以： 1) 在制造商提供源代码的情况下，评估其代码质量和安全性； 2) 从信息和通信技术资产及系统中提取目标代码； 3) 确认已安装和执行的源代码与目标代码之间的唯一对应关系。		
ID.SC-03 - 通过与供应商和第三方合作伙伴的合同落实适当网络安全措施	**普通类** 无要求。 **关键类** 同普通类要求。 **战略类** 1_S 内部依赖方实施的安全措施应与数字基础设施的安全措施保持一致，且符合风险分析的结果。安全措施要求应纳入合同、协议或约定中。 2_S 外部服务受托方实施的安全措施，应与数字基础设施的安全措施保持一致，且符合风险分析的结果。安全措施要求应纳入合同、协议或约定中。	对于战略类服务，内部依赖方和外部服务受托方实施的安全措施需要与数字基础设施的安全措施保持一致，并且记录在合同、协议或约定中。	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。 华为云已建立供应商管理体系，维护符合资质的供应商采购名单，按照自身的网络安全与隐私要求对供应商提出要求和监督。在供应商引入前会进行尽职调查，签署合同、服务协议、保密协议，约定双方责任与义务、服务水平等要求，供应商引入后每年对供应商的安全风险进行评估及安全稽查。
ID.SC-04 - 通过审计、核查或其他方式定期评估供应商和第三方合作伙伴	**普通类** 无要求。 **关键类** 同普通类要求。 **战略类** 1_S 应有一份最新文件，说明针对供应商和第三方合作伙伴开展评估的流程、方法和频次，并与所开展风险分析的结果相适应。 2_S 应有一份关于审计、核查或其他预定评估形式的最新计划，以及已实施评估的登记册和相关文件。	对于战略类服务，应建立完整的供应商及第三方合作伙伴评估与审计体系。需制定基于风险分析的定期评估流程与计划，并实施符合行业标准的年度独立审计。所有审计政策与程序需文件化并每年审查。对于评估发现的不符合项，必须制定、批准并维护成文化的整改计划，确保问题得到纠正。	华为云已建立供应商评估机制，采购前会对供应商资质进行评估，根据供应商所提供的产品和服务制定不同级别的评估要求，仅经过资质认证的供应商才能进入华为云的采购范围。 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。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。 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

编号	具体控制要求	客户关注点	华为云的应答
	3_S 应定义并实施审计管理流程，以便按照主要行业标准，至少每年一次并根据风险制定计划，开展独立保证性评估。 4_S 审计和保证政策与程序应予以建立、形成文件、批准、维护，并至少每年审查一次。 5_S 对于在供应商和第三方合作伙伴方面发现的不符合项所对应的纠正措施，应制定、成文化、批准、传达、适用并维护整改计划。		聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计。

6.1.2 保护

编号	具体控制要求	客户关注点	华为云的应答
身份管理、身份验证与访问控制（PR.AC）：对物理和逻辑资产及其相关资源的访问仅限于经授权的人员、流程和设备，且其管理方式应与针对未经授权访问授权活动和交易的风险评估保持一致。			
PR.AC-01 - 对获授权用户、设备和进程的数字身份与访问凭证进行发放、管理和验证	**普通类** 1_O.a 应根据职责分离原则为员工配置专用登录凭证，凭证更新频率需要与权限相适应。 1_O.b应根据职责分离原则为员工或外部人员配置访问基础设施的专用登录凭证，凭证更新频率需要与权限相适应。 2_O 应建立访问凭证管理的政策和程序，至少应每年更新一次，并供行政机构查阅。 3_O 建立管理、存储、审查系统身份和访问级别的机制。 4_O 在用户发生变化（例如人员调岗）时，应及时更新凭证。 5_O 系统身份应通过数字证书或同等安全水平的替代技术进行管理。 6_O 建立涵盖上述五项要求的审查计划，实施审查并保留记录。	客户应为组织内部及外部人员配置专用的访问凭证，遵循职责分离原则，并根据权限风险按相应频率更新，人员变动时需及时调整。 建立凭证管理政策与程序并每年更新，明确管理、存储、审查系统身份和访问级别的机制，系统身份需通过数字证书或同等安全技术管理。 应制定安全审计计划，定期核查上述要求的落实情况，并保留完整的审计记录与文档。 对于关键类及战略类服务，还应增加建立数字身份及用户访问凭证管理、验证、撤销和安全审计所采用的安全政策、流程、方法及技术。	华为云制定并记录正式的逻辑安全的政策和程序。及时批准、添加、修改或禁用，并定期审查华为员工和承包商的用户帐户。华为云建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循和授予的。 华为云内部建立了运维和运营账号管理机制，华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。此外，还采用双因子认证对云为人员进行身份认证，如 USB key、Smart Card 等。所有运维账号由LDAP集中管理，通过统一运维审计平台集中监控并进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC权限管理。保证不同岗位不同职责

编号	具体控制要求	客户关注点	华为云的应答
	关键类 7_C 建立覆盖如下方面的详细文件： a. 针对数字身份的管理、验证、撤销和安全审计，以及第 1_O、2_O、3_O、4_O、5_O 和 6_O 点所述程序的安全政策； b. 针对数字身份及用户访问凭证的管理、验证、撤销和安全审计所采用的安全政策； c. 用于确保遵守上述安全政策的流程、方法和技术。 **战略类** 同关键类要求。		人员限定只能访问本角色所管辖的设备。 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。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CTS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。

编号	具体控制要求	客户关注点	华为云的应答
PR.AC-02 - 保护并管理对资源的物理访问	**普通类** 1_O 针对系统和设备清单重中识别的资产，应建立书面化的政策和流程，内容至少包括： a. 针对资产保护和物理访问管理的安全政策； b. 遵守安全政策需要的流程、方法和技术。 2_O 应界定物理安全边界，以保护人员、数据和信息系统。 **关键类** 3_C 应在办公区域与数据存储及处理区域之间建立安全边界。 **战略类** 同关键类要求。	客户应建立书面的资产保护和物理环境访问安全政策、流程、方法和技术，并界定物理安全边界。 对于关键类服务，应在办公区域与数据存储及处理区域之间设置隔离措施。	华为云建立并实施了文档化的网络安全政策和程序，为资产保护和物理访问管理提供指导。 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。在办公区域与数据存储及处理区域之间建立安全边界。
PR.AC-03 - 管理对资源的远程访问	**普通类** 1_O 远程访问活动应由网络安全组织监控。 2_O 在符合被验证的技术限制的前提下，应实施适当的访问控制措施，即采用认证、授权及集中式访问日志管理系统，并辅以与风险相称安全水平的身份认证系统。 3_O 应定义并实施集中式访问管理模型来管理行政机构资源和数据的访问，包括授权、日志记录以及报告。 4_O 应保留远程访问日志。 5_O 远程访问应采用多因素认证方式。 **关键类** 6_C 应建立针对远程访问的文件化政策，内容至少包括： a. 针对允许的远程访问活动所采用的安全政策和安全措施；	客户的网络安全组织应监控远程访问活动，并对远程访问实施认证、授权与集中式的日志记录来确保远程访问安全。远程访问应采用集中管理模型，并强制使用多因素认证，同时保留完整的远程访问日志。 对于关键类服务，客户还应制定文件化的远程访问管理政策，明确远程访问安全政策、安全措施、以及安全政策得到遵守的整套流程、方法和技术手段。 对于战略类服务，客户还应保障远程访问各项政策和程序应至少每年更新一次，在管理部门数据时，应与该部门共同定义并实施联合授权流程。	华为云建立身份与访问安全管理机制，涵盖对资源远程访问的管控要求，包括对远程访问进行限制，限制远程执行特权命令、代码等，并对操作进行审计。华为云至少每年审查一次网络安全管理政策和流程，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。 华为云不允许运维运营人员在未经授权的情况下访问客户的系统和数据。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因素认证，如USB key、SmartCard等。华为云管理员必须经过双因素认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。

编号	具体控制要求	客户关注点	华为云的应答
	b. 遵守上述安全政策的流程、方法和技术。 **战略类** 7_S 各项政策和程序应至少每年更新一次，并在主体提出具体请求时可供查阅。 8_S 在访问管理部门数据时，应与该部门共同定义并实施联合授权流程。如无法做到，主体应在最短时间内联系该部门，并记录并说明该访问行为。 9_S 所有涉及访问管理部门数据的操作，均须按照特权用户的用户管理和日志记录标准进行管理。		华为云建立数据共享机制，数据的共享应获得数据所有者的授权，并按照数据级别和数据类型获得相应的审批并留存审批记录。 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）**来实现集中式访问管理以及多因素认证： • 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。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 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。 客户也可通过云审计服务作为辅助，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。
PR.AC-04：资源访问权限及相关授权应遵循最小	**普通类** 1_O 结合资产清单，明确： a. 需要被访问的资产、对应功能以及所需授权； b. 设置用户组及其可访问的资源和权限； c. 将已登记用户分配至各	客户应明确需要被访问的资产、功能和所需授权，将这些资产和权限分配给用户组，当用户需要授权时，通过为用户分配用户组的方式进行授权。	华为云已建立文件化的身份与访问管理机制，遵循职责分离原则，不同人员的权限依据职责确认角色，实现 RBAC 权限管理，实施最小化授权，权限的获取需通过主管审批并定期复核。

编号	具体控制要求	客户关注点	华为云的应答
权限原则和职责分离原则进行管理	用户组的方式进行授权。 2_O 在实施信息系统访问权限的过程中，针对组织风险，严格遵循职责分离原则和最小权限原则。 3_O 制定并实施特权访问角色隔离的政策、流程及措施，实现数据访问管理、加密及密钥管理功能、日志功能独立和分离。 **关键类** 4_C 建立覆盖1_O的文件化流程。 **战略类** 5_S 主体应独立管理基础设施，并拥有运行底层物理与逻辑基础设施的自有能力。除非有可文件证明的技术限制，主体方才能借助具备可替代性的第三方能力。	访问权限管理遵循职责分离和最小权限原则，并且保障数据访问管理、加密及密钥管理功能、日志功能分离。 对于关键类服务，客户应建立文件化的访问管理流程。 对于战略类服务，客户应独立管理基础设施，并拥有运行底层物理与逻辑基础设施的自有能力，若因技术限制无法满足，可以借助具备可替代性的第三方。	作为云服务提供商，华为云在欧洲具备独立管理的数据中心，拥有运行底层物理与逻辑基础设施的自有能力，无需依赖第三方。客户可以使用华为云提供的华为云的**统一身份认证服务（Identity and Access Management，简称 IAM）**进行访问管理，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。
PR.AC-05：网络完整保障	**普通类** 无要求。 **关键类** 1_C 应制定网络基础设施安全政策与程序，并至少每年更新一次。 2_C 应制定系统性能监控计划，包括资源可用性、质量和容量。 **战略类** 3_S 结合资产清单建立文件化的网络策略，内容至少包括： a. 网络分段/隔离安全政策； b. 网络分段/隔离的描述； c. 遵守上述安全政策的流程、方法和技术； d. 基础设施各部分被隔离和控制的方式。	客户应制定网络基础设施安全政策与程序、包含资源可用性、质量、容量监控的监控计划。 对于战略类服务，客户还应有涵盖网络隔离安全政策、流程、方法、技术的详细指南。	华为云制定网络分区及安全管理策略，通过多种工具保护网络分区安全。华为内部网络按安全风险受控程度、资产敏感程度将网络区域分为不可信区、可信区和半可信区三大类，各区域之间明确边界及隔离要求，实施多功能区域之间的网络隔离，保证不同业务的网络通信流量得到合理和安全的分流。在网络边界部署Anti-DDoS设备、IPS等设备对异常流量进行分析和阻断。 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

编号	具体控制要求	客户关注点	华为云的应答
			管理、以及业务连续性等。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。
PR.AC-07 -用户、设备和其他资产已身份认证（例如：单因子、多因子）并与交易风险相一致（例如：个人的安全和隐私风险以及其他组织风险）	**普通类** 无要求。 **关键类** 1_C 应制定访问系统、应用程序和数据的政策与程序，其中至少应对特权用户以及对数据的访问采用多因素认证。 **战略类** 2_S 应基于资产清单和风险评估制定一份详细文件，内容至少包括： a. 可用的认证方式； b. 匹配各类交易的认证方式。	对于关键类服务，客户应制定访问系统、应用程序和数据的政策与程序。 对于战略类服务，客户还应基于资产清单和风险评估制定涵盖认证方式和各类交易应使用的认证方式的详细文档。	华为云制定了密码策略及账号口令安全相关管理规范，对秘密鉴别信息的分配进行管理。新建系统中账号缺省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，严格纳管回收特权账号。使用 IAM 对访问进行管理，支持多因素认证用于登录验证和操作保护，员工每次登陆均需要使用多重身份验证确定身份。也提供会话超时策略、账号登陆和锁定策略。 华为云定期对华为云的硬件、软件、数据、人员和服务进行识别。华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。
意识与培训（PR.AT）：：为员工和合作伙伴提供网络安全意识教育和培训，使其能够按照现行政策、程序和协议履行各自的职责和角色			
PR.AT-01 -告知和培训所有用户	**普通类** 1_O 应建立一份涵盖意识教育培训内容和内容掌握程度测试方式的文件。 2_O 主体应根据用户角色提供涵盖以下主题培训与教育： a. 保护明文或加密数据的机密性； b. 劳动关系终止时归还公司资产； c. 角色与职责的界定； d. 对系统、资产和资源的访问政策； e. 信息安全管理政策；	客户应建立文件化的意识教育与培训制度，明确培训的内容和测试方式，培训内容包括但不限于数据加密、离职资产归还、不同角色的安全职责及传达流程、资产访问政策、信息安全政策、信息保密，涉及战略类服务的人员应保留培训记录。	作为云服务提供商，为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为对全体员工从意识教育普及、宣传活动开展、商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育。参考业界优秀实践，华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，提升员工能力，向客户交付安全的产品、解决方案与服务。为了内部有序管理，消减人员管理风险对业务连续性和安

编号	具体控制要求	客户关注点	华为云的应答
	f. 向可接触信息资产的员工传达其角色与职责的流程； g. 信息不披露/保密要求。 **关键类** 同普通类要求。 **战略类** 3_S 应保留员工最新培训记录。		全性带来的潜在影响.华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。华为云内部进行电子化流程记录，每次培训都由培训记录，需要参与人员签到。
PR.AT-02 - 特权用户理解其角色与职责	**普通类** 1_O 应明确特权用户培训内容和内容掌握程度测试方式。 2_O 应明确规定特权用户拥有的权限和遵守的要求。 **关键类** 同普通类要求。 **战略类** 3_S 建立详细的文件化的特权用户培训要求及权限职责清单。	组织应明确特权用户培训内容和测试方式，并未明确每一位特权用户的权限和遵守要求。 对于战略类服务，应建立文件化的特权用户培训要求及权限职责清单。	在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的信息安全责任。对于合同方，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全责任。 华为云对关键岗位要求参加上岗培训和认证，签署网络安全与隐私保护承诺函，入职和仍然需要定期参加网络安全岗位和技能和意识培训考试。
数据安全（PR.DS）：数据应按照组织的风险管理策略进行存储和管理，以确保信息的完整性、机密性和可用性。			
PR.DS-01：保护静态数据	**普通类** 1_O. 建立包含如下内容的文件： a. 数据存储和保护采取的安全政策； b. 遵守安全政策而采用的流程、方法和技术。 2_O. 行政数据（包括用于安全目的的数据，例如门禁控制系统）均需通过位于欧盟境内的基础设施进行处理。	客户应建立数据存储安全政策，明确数据存储安全的流程方法和技术。 数据可在欧盟境外处理的情况： • 有合理监管或技术原因且属于BC/DR和CDN范围下的数据； • 仅涉及普通类和关键类数据或服务的	华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标记安全等级。同时，华为云也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

编号	具体控制要求	客户关注点	华为云的应答
	除非存在合理且有据可查的监管或技术原因，且属于基数字基础设施的如下范围： a. 业务连续性与灾难恢复，即使被外包（如云计算）； b. 具有全球地理分布的内容分发网络。 在此情况下，实施风险评估时必须充分考虑其位于欧洲境外的情况，并核实其是否符合个人数据保护相关法规。 3_O. 与基础设施运行相关的元数据可使用位于欧盟境外的基础设施进行处理，但与管理相关的元数据则必须使用位于欧盟境内的基础设施进行处理，除非存在合理且有据可查的监管或技术原因。基础设施运行相关的元数据可使用位于欧盟境外的基础设施进行处理时，风险评估必须充分考虑到基础设施位于欧盟境外的情况，同时核实其是否符合数据保护法规。若元数据被传输到非欧盟基础设施，需保障中断情况下仍能满足云服务所需的最低服务水平。 4_O.若与行政管理相关的元数据旨在提供网络安全服务或提升数字基础设施的韧性，在存在充分的技术理由且有相关证据证明其管理符合处理目的的唯一性前提下，该等元数据也可在欧洲境外进行处理。此时，风险评估须充分考虑数据位于欧洲境外的情况，并核实其是否符合个人数据保护相关法规。若元数据被传输到非欧盟基础设施，需保障中断情况下仍能满足云服务所需的	基础设施运行相关的元数据 • 仅涉及普通类数据或服务，且用于提供网络安全服务或提升数字基础设施的韧性的行政管理元数据 若涉及欧盟境外处理数据的情况，风险评估时需要充分考虑此情况并合适是否符合个人数据保护法规。 对于战略类数据或服务，非欧盟实体访问数据需要经过CAN的批准，主体需要制定密钥安全管理机制，及时销毁不再使用的密钥。	钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。 针对于静态数据，华为云 为保护租户数据的存储安全采取了一系列的保护机制。首先，华为云提供了**密码安全中心（Data Encryption Workshop，简称DEW）**。它帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（ HSM Hardware Security Module ），为租户创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。与华为云服务对接 KMS 的服务有 OBS 、云硬盘等。其次，专属加密满足租户更高合规性要求的加密场景，采用通过国家密码局认证或国际权威认证的硬件加密机，对租户业务进行 专属加密，默认双机架构以提高可靠性。最后，华为云多款存储产品如 EVS 、VBS 等均提供存储加密的机制。 华为云严格遵守欧盟GDPR要求，作为数据处理者按照数据控制者（租户）的要求处理数据，并遵守当地对网络安全与隐私保护的法律法规

编号	具体控制要求	客户关注点	华为云的应答
	最低服务水平。 **关键类** 5_C. 对于政府部门的关键数据和服务，第4_0条的规定不适用，以第3_O条为准。 **战略类** 6_S.对于非欧盟实体访问数据，该主体应： a. 向国家网络安全局（ACN）和行政部门报告任何非欧盟实体提出的访问数据或元数据的请求； b. 仅在获得行政部门明确授权后，方可向欧盟以外实体提供行政部门数据或元数据的访问权限。 7_S. 已制定并实施销毁存储在非安全环境中的密钥的程序和技术措施，并在不再需要时销毁存储在硬件安全模块（HSM）中的密钥，以符合法律和法规要求。 8_S. 对于政府部门的战略类数据和服务，第3_O条所述的要求不适用。所有类型的元数据均须通过位于欧盟境内的基础设施进行处理，但第2_O条所述服务所必需的元数据除外。		
PR.DS-02 – 保护传输中的数据	**普通类** 无要求。 **关键类** 1_C 在将服务器、服务、应用程序或数据迁移至云环境时，应使用安全、加密且获批准的最新协议的通信通道。 2_C 按照风险评估，对于识别的数据流和通信，应使用安全、加密且获批准的最新	对于关键类和战略类服务，在将服务器、服务、应用程序或数据迁移至云环境时，应使用安全、加密的通信通道。	华为云提供的**云数据迁移（Cloud Data Migration，简称CDM）**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。CDM在用户VPC中运行，网络隔离确保数据传输的安全性。支持SSL的数据源，如RDS、SFTP等，可以使用SSL。CDM还

编号	具体控制要求	客户关注点	华为云的应答
	协议的通信通道。 **战略类** 同关键类要求。		支持公网数据源的数据上云，用户可以利用VPN和SSL技术来避免传输安全风险。 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，有效地降低数据在网络传输过程中被恶意嗅探的风险。控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。
PR.DS-03 -资产在整个删除、转移和处置过程中得到正式管理	**普通类** 无要求。 **关键类** 1_C 结合资产管理，至少应明确： a. 数据存储设备的物理转移、移除和销毁所采用的安全政策； b. 遵守上述安全政策的流程、方法和技术。 **战略类** 2_S 由于移动设备遭到破坏，可能影响基础设施或其所提供服务的可用性、完整性或保密性，因此应启用受管控的移动设备的远程地理定位功能。 3_S 应制定并实施用于远程删除管理数据的技术措施。 4_S. 应建立文件化的数据存储设备物理转移、移除和销毁流程和政策。	对于关键类服务，应明确数据存储设备的物理转移、移除和销毁的安全政策。 对于战略类服务，应建立文件化的文件化的数据存储设备物理转移、移除和销毁流程和政策，并对移动设备启用远程地理定位并实施远程数据删除技术。	华为云已建立文件化的介质管理要求，使用包含存储介质的设备由专人管理，使用完毕后由专人对其进行格式化处理。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。当物理磁盘报废时，华为云通过对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保用户 隐私和数据不受未授权访问。若该等设备遭到破坏，可能影响基础设施或其所提供服务的可用性、完整性或保密性。员工可向业务主管和信息安全部门报告，并远程擦除公司数据，并取消设备绑定。
PR.DS-05 - 已采取安	**普通类** 1_O 结合资产管理，至少应	客户应根据资产面临的风险采取合适的数据访	华为云制定了数据安全策略及数据安全保护管理规定，对数据资

编号	具体控制要求	客户关注点	华为云的应答
全措施（例如访问控制）以防止数据泄露	界定： a. 数据访问安全政策； b. 遵守该安全政策的流程、方法和技术。 2_O 应采用与风险评估相一致的数据防泄漏政策。 **关键类** 同普通类要求。 **战略类** 3_S 建立文件化的数据访问安全流程和政策。	问安全政策和数据防泄漏政策；对于战略类服务，流程和政策应文件化记录。	产的分级分类标准进行了定义，同时明确了数据匿名化及标签化处理标准，对数据在整个生命周期中须遵循的安全措施进行了规范。华为云每年会对建立的数据安全管理相关规范和策略流程进行审计。 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。
PR.DS-06 - 采用数据完整性控制机制以验证软件、固件和信息的真实性与完整性	**普通类** 1_O 结合资产管理，至少应界定： a. 核验软件、固件和信息真实性的数据完整性控制机制清单； b. 为将某种机制分配给某项资源以及界定何种机制适用于何种资源而采取的安全政策； c. 遵守上述安全政策的流程、方法和技术。 **关键类** 同普通类要求。 **战略类** 2_S 建立文件化的数据完整性控制流程和政策。	客户应明确核验软件、固件和信息真实性的数据完整性控制机制清单，资源分配的安全政策。 对于战略类服务，应有一份最新的详细文件商述流程和政策。	华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。 华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件安装、软件退出等环节，均实施严格的管控。

编号	具体控制要求	客户关注点	华为云的应答
PR.DS-07 - 开发和测试环境与生产环境隔离	**普通类** 无要求。 **关键类** 1_C 结合资产管理，至少应明确： a. 各环境分离的总体架构，以及在各环境交界处该分离如何实现； b. 确保开发和测试环境与生产环境分离所采用的安全政策； c. 遵守上述安全政策的流程、方法和技术。 **战略类** 2_S 应建立文件化的开发、测试、生产环境隔离流程和政策。	对于关键类服务，客户应明确开发、测试、生产环境隔离的总体架构和实现方式， 对于战略类服务，应建立文件化的各环境隔离和实现机制。	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。 针对各环境交界处的分离实现，华为云也制定了变更管理程序，管理应用变更和基础设施变更。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。
信息保护流程与程序（PR.IP）：已实施并随时间推移不断调整的安全政策（涵盖指导方针、目标、范围、角色与职责、管理层的承诺以及各组织主体之间的协调），以及用于管理信息系统和资产保护的流程与程序。			
PR.IP-01 - 制定并管理安全配置基线实践	**普通类** 1_O 应制定应用程序安全功能规划、实施和维护的安全政策，且每年审查并更新一次。 **关键类** 同普通类要求。 **战略类** 2_S 结合资产管理，应建立文件化的应用程序安全管理政策，内容至少包括： a. 为开发 IT 系统配置并仅部署获批准配置所采用的安全政策；	客户应建立应用程序安全功能政策，对于战略类服务，应用程序安全功能政策应文件化并至少包含IT系统开发部署安全配置的要求、IT系统配置清单以及相关的政策流程和技术。 战略类服务还应定义各类程序的基本安全要求、监控技术指标、漏洞修复流程、兼容性验证流程，建立变更管理系统。	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。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

编号	具体控制要求	客户关注点	华为云的应答
	b. IT 系统配置清单及其所对应的基准或参考实践； c. 遵守上述安全政策的流程、方法和技术。 3_S. 定义并记录各类应用程序的基本安全要求。 4_S. 已定义并实施用于监控对已定义安全要求及合规义务的遵守程度的技术性指标。 5_S. 已建立应用程序漏洞缓解及安全恢复流程，并在可行时实现修复自动化。 6_S. 已建立验证设备与操作系统及应用程序兼容性的流程。 7_S. 已建立针对操作系统、补丁和/或应用程序变更的管理系统。		试、安全验收和发布、漏洞管理、变更管理等环节，确保信息安全在信息系统安全生命周期中得到设计和实现。 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。
PR.IP-03 - 启用配置变更控制流程	**普通类** 无要求。 **关键类** 1_C 应明确： a. IT 系统和工业控制系统配置更新的安全政策，以及监控实际配置与规定配置差异的安全政策； b. 遵守上述安全政策的流程、方法和技术。 2_C 应建立修改及配置过程中异常及紧急情况的管理流程。 3_C. 制定并实施在发生错误或安全问题时的回滚计划。 **战略类** 4_S 应建立文件化的变更流程和政策。	对于关键类服务，应明确配置变更和监控的安全政策，并建立配置变变更过程中异常或紧急情况的处置流程和回滚计划，针对战略类服务，这些政策、流程及回滚计划需要文件化记录。	华为云制定了详细的文件化的变更管理程序，管理应用变更和基础设施变更。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。变更方案需要包括变更范围、备份方案、实施方案、回退方案、应急方案、验证方案，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。
PR.IP-04 – 创建、维护并验	**普通类** 1_O a. 应定期对已存储数据进行备份，并确保备份数据的保密性、完整性和可用	客户应定期备份存储于云中的行政机构的数据和恢复服务所需的数据并确保备份数据的保密	华为云已建立文件化的备份机制，会根据服务合同和业务连续性要求制定包括备份方式、位置、存储介质、保留期限、备份

编号	具体控制要求	客户关注点	华为云的应答
证信息备份	性。 1_O b. 应定期备份存储于云中的、为完整恢复系统所必需的信息，其中包括行政机构的数据和恢复服务所需的数据，并确保备份数据的保密性、完整性和可用性。另外，还应确保至少在不能从系统中持续访问的介质上存有一份副本，避免在系统被攻击波及全部安全备份副本。 2_O 将备份副本的定期恢复测试作为服务等级目标（SLO），至少每年开展一次。 **关键类** 3_C 应建立文件化的备份要求，内容至少包括： a. 针对信息备份所采用的安全政策； b. 遵守上述安全政策的流程、方法和技术。 **战略类** 同关键类要求。	性、完整性和可用性。对于关键类服务，应制定备份安全政策文件。	恢复程序等信息的备份策略，并每年开展一次备份恢复演练。 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、**云备份（Cloud Backup and Recovery，简称CBR）**、**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，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保证在灾难发生时数据不丢失，客户还可依赖华为云数据中心集群的多地域（Region）和多可用区 AZ 架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。 华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。
PR.IP-09：已制定并实施了针对事故/灾难的响应（事故响应和业务连续性）及恢复（事故恢复和灾难恢复）计	**普通类** 无要求 **关键类** 1_C. 应有最新的规定数字基础设施的预期服务水平的详细文件。 2_C.应有最新的包含业务连续性计划以及事件响应计划详细文件，该文件至少包括： a. 事件优先级确认政策和流程； b. 计划实施的各阶段； c. 人员的职责与责任； d. 沟通与报告流程；	对于关键类服务，客户应有文件化的数字基础设施预期服务水平、业务连续性计划、事件响应计划。业务连续性策略和能力需要基于对业务中断的风险建设，业务连续性计划需要测试并传达给相关方，业务连续性计划和事件响应计划应定期审查并按照需提供给行政机构。 对于战略类服务客户应有文件化的预期服务水平(含数字基础设施、冷/热副本站点、灾难	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IS0 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。 华为云拥有丰富的业务连续性管

编号	具体控制要求	客户关注点	华为云的应答
划	e. 与意大利CSIRT的协调机制。 3_C. 应有最新的列出了已开展的指导、培训和演练活动文件。 4_C. 业务连续性计划已通过测试，并已传达给相关方。 5_C. 业务连续性计划以及事件响应计划详细文件，应行政机构要求予以提供，并定期进行审查； 6_C. 对中断及其相关风险的影响进行评估，以便制定业务连续性策略和能力建设的标准。 **战略类** 7_S. 应有最新的规定了数字基础设施、冷/热副本站点、灾难恢复站点的预期服务水平的详细文件。 8_S. 应有最新的包含灾难恢复计划和事故响应恢复计划的详细文件，该文件至少包括： a. 确定事件优先级的政策和流程； b. 计划实施的各阶段； c. 人员的职责与责任； d. 沟通与报告流程； e. 与意大利CSIRT的协调机制。 9_S. 应有最新的列出了已开展的指导、培训和演练活动文件。 10_S. 灾难恢复策略是否经过测试并已传达给相关方。 11_S. 对基础设施运行至关重要的设备均已实现冗余配置，若设备位于不同地点，其间距符合行业最佳实践。	恢复站点)、灾难恢复计划、事故响应恢复计划。基础设施运营重要设备冗余，灾难恢复策略定期测试演练并已传达给相关方。	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。
PR.IP-11 -网络安全纳入人	**普通类** 无要求。 **关键类**	对于战略类服务，客户应向行政机构提供查询特权账号人员的方法和清单，并支持行政机构	客户可通过华为云的IAM服务及PAM 功能可以更有效地细化管理特权账户。客户也可通过云审计

编号	具体控制要求	客户关注点	华为云的应答
员管理流程（如背景调查、账户停用）	无要求。 **战略类** 1_S 主体应向行政机构提供其用于审查对基础设施或数据具有特权访问权限人员的方法。 2_S 主体应向行政机构提供对基础设施或行政机构数据具有特权访问权限的员工名单，并且支持行政机构对名单中人员一出的要求。	对名单中人员一出的要求。	**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。 华为云对于运维人员实行基于角色的访问控制，限定不同岗位不同职责的人员只能对所授权的运维目标进行特定操作，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（提供账号/密码）登陆租户的控制台或者资源实例协助客户进行维护。
PR.IP-12 - 制定并实施漏洞管理计划	**普通类** 1_O 应建立最新的漏洞管理详细文件，至少说明： a. 漏洞管理安全政策； b. 遵守该等安全政策的流程、方法和技术。 2_O 应确定更新检测工具、威胁特征、入侵指标的流程和技术措施，至少每周进行审查更新一次。 **关键类** 同普通类要求。 **战略类** 3_S 漏洞管理详细文件应每六个月更新一次。 4_S 应建立识别使用第三方或开源库的应用程序更新的漏洞管理政策和技术措施。	客户应制定漏洞安全政策，至少每周审查更新一次检测工具、威胁特征、入侵指标。 对于战略类服务，漏洞管理应涵盖第三方或开源库的应用程序更新的识别，安全政策文件每六个月更新一次。	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。华为云安全运营中心主动通过外部舆情、开源社区等外部渠道获取最新的漏洞信息，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。华为云使用态势感知分析系统，关联各种安全设备的告警日志并统一进行分析，快速识别已经发生的攻击、并预判尚未发生的威胁。
维护（PR.MA）：工业信息与控制系统的维护工作均按照现行政策和程序进行。			
PR.MA-01 - 使用受控	**普通类** 无要求。	对于关键类服务，应明确针对资产和系统维护记录所采用的安全政	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、

编号	具体控制要求	客户关注点	华为云的应答
工具执行并记录资产和系统的维护与修复	**关键类** 1_C 结合资产管理，应明确： a. 针对资产和系统维护、修复记录所采用的安全政策； b. 遵守上述安全政策的流程、方法和技术 **战略类** 2_S 应维护最新的资产及系统维护活动登记册。 3_S 应建立最新的资产和系统管理政策和流程。 4_S 在风险分析中定义为关键的软件的更新在部署至生产环境前必须在测试环境中验证（除非存在正当的安全相关理由需要立即部署），且目标代码至少保留24个月。 5_S. 在风险分析中被视为关键的组件，其硬件或软件的每次更新，在实际部署到运行环境之前，必须在测试环境中进行验证（除非存在正当的安全相关理由需要立即部署），且目标代码必须保存至少24个月。测试环境中的活动旨在验证安全方面的问题。 6_S. 软件更新应仅从预先批准的来源下载。 7_S. 存储维护/更新活动日志的系统必须与受维护系统分离，且不得由执行维护/更新活动的用户访问。 8_S. 建立最新的涵盖5_S、6_S和7_S要求的关键组件更新流程和技术工具。	策。 对于战略类服务，需建立并维护详细的维护活动记录及流程政策文件。同时，基于风险分析，对于关键软件更新，必须在投入生产环境前于测试环境中进行充分验证。	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。对于需要通过版本、补丁修复的漏洞，在安装之前进行安全测试验证。 华为云对内外部员工的终端资产实施集中管理包括，实施软件白名单对软件的安全和使用进行限制，同时采用数据防泄露、磁盘加密技术保护终端。
PR.MA-02 - 对资源和系统的远程维护须经	**普通类** 1_O 对资源和系统开展的远程维护（包括与安全功能有关的活动）应遵守 PR.AC-03 子类别（管理对资源的远程	客户对资源和系统的远程维护仅允许必要情况下经网络安全组织授权的访问。 对于关键类服务，须采	华为建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循

编号	具体控制要求	客户关注点	华为云的应答
批准、记录在案，并以确保防止未经授权访问的方式进行	访问）中的措施以及以下各点要求。 2_O 第三方人员实施的所有远程访问均应由网络安全组织授权，并仅限于必要情形。 **关键类** 3_C 应采取严格的用于认证、身份识别和事件可追溯性的防护机制。 4_C 应采取特权账户管控机制，包括权限有效期、限制可用管理功能。 5_C 应使用与被访问系统隔离的系统收集和存储远程通信会话和活动日志，且远程用户无法访问日志。 **战略类** 6_S 应建立远程维护的流程和技术工具文件。	用认证、身份识别与事件追溯防护机制，并对特权账户实施管理控制（包括有效期与功能限制）。同时，所有与远程会话及系统活动相关的日志，都必须防止被未授权篡改或删除，并依据内部政策进行保留。 对于战略类服务，还应应制定远程安全政策文件。	和授予的。堡垒主机提供基于密码和邮箱验证码的双因素身份验证功能，以验证用户的身份。用户通过 互联网访问华为云办公子网，需要根据注册设备及其账号和密码进行双因素认证。华为云员工可以在 Cloud Scope 中进行逻辑访问管理， Cloud Scope 涵盖 Cloud Mnet System 、CBC 帐户中心、堡垒机、 FUXI 和 SVN 等多种支撑工具。支持工具涵盖本报告范围内所有产品的操作系统，包括但不限于虚拟服务器和基础设施设备的支持工具。在所有相关层的支持工具中的访问授权基于最小权限强制实施。高于最低权限的访问需要获得指定人的批准。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。 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。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。 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VPN、HTTPS等加密传输方式供

编号	具体控制要求	客户关注点	华为云的应答
			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。
防护技术 (PR.PT)：安全技术解决方案的实施旨在确保系统和资产的安全性与韧性，并符合相关政策、程序和协议。			
PR.PT-01 - 制定并落实用于定义、实施和审查系统日志的政策	**普通类** 无要求。 **关键类** 1_C 日志应以安全的、集中化方式保存，保存期限至少为 24 个月。 2_C 应明确： a. 系统日志管理安全政策； b. 遵守上述安全政策的流程、方法和技术，尤其应关注日志的完整性和可用性 **战略类** 3_S 应有一份最新的文件化的系统日志管理安全政策。	对于关键类服务，日志应以安全的、集中化方式保存，保存期限至少为 24 个月。 对于战略类服务，应有文件化的日志管理流程和政策。	华为云建立并实施了文档化的日志管理政策和程序，为操作网络安全管理提供指导，华为云也建立了集中、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。 客户可以使用华为云的**云审计服务（Cloud Trace Service，简称CTS）**，可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 华为云的**云日志服务 （Log Tank Service，简称LTS）**服务，用于收集来自主机和云服务的日志服务，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为客户提供实时、高效、安全的日志处理能力。华为云的CTS，可提供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。 CTS最多可支持日志存储365天，如需存储根长时间，可将日志转储至OBS，实现长久存储。

编号	具体控制要求	客户关注点	华为云的应答
PR.PT-04 - 保护通信网络和控制网络	**普通类** 1_O 应部署网络边界安全系统（如防火墙，包括应用层防火墙），维护得当且配置正确。 **关键类** 2_C 应部署、更新、维护并妥善配置入侵防御系统（IPS）。 3_C 第 1_O 和 2_C 点所述技术工具应有助于遵守 ID.AM（资产管理）、ID.GV（治理）、ID.SC（供应链风险管理）、PR.AC（身份管 理、认证和访问控制） 和 PR.DS（数据安全） 类别所述政策。 **战略类** 1_S 应部署、更新、维护并妥善配置边界系统，例如防火墙，包括应用层防火墙。 2_S 应部署、更新、维护并妥善配置入侵防御系统（IPS）。 3_S 第 1_O 和 2_C 点所述技术工具应有助于遵守 ID.AM（资产管理）、ID.GV（治理）、ID.SC（供应链风险管理）、PR.AC（身份管 理、认证和访问控制） 和 PR.DS（数据安全） 类别所述政策。 4_S. 第1_O.和2_C.条所述技术工具的更新、维护和配置，应遵循ID.AM（资产管理）、ID.GV（治理）、ID.SC（供应链风险管理）、PR.AC（身份管 理、认证和访问控制） 和 PR.DS（数据安全）类别中的相关政策。 5_S. 第1_O.和2_C.点所述的技术工具亦用于DETECT (DE)功能所指的目的。 6_S. 存在一份最新的文件，	组织应部署边界系统，例如防火墙，并确保其保持更新、得到维护且配置适当。 对于关键类服务，应部署、更新、维护并妥善配置入侵防御系统。 对于战略类服务，应部署、更新、维护并妥善配置边界系统，例如防火墙，以及妥善配置入侵防御系统（IPS）	华为云建立了稳固、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；为了检测和拦截来自Internet的攻击以及租户虚拟网络之间的东西向攻击，华为云的网络中部署了网络IPS设备，包括但不限于面向公众的网络边界、安全区域信任边界、租户空间边界。华为云的IPS可以实时分析网络流量，触发对协议攻击、暴力破解、端口和漏洞扫描、病毒和木马攻击、针对特定漏洞的攻击等各种入侵的拦截。 此外，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 、 web shell 、 CC 等攻击实现实时的高性能防护。华为云 WAF 给用户提供简便的管理界面，用户可根据自身业务需要进行相关防护设置，亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。 更多信息可参考 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的回答。

编号	具体控制要求	客户关注点	华为云的应答
	其中至少描述了用于实现第1_O.、2_C.、3_C.、4_S.和5_S.点所采用的流程和技术工具。		
PR.PT-05 - 实施机制（如故障安全、负载均衡、热插拔）以支持韧性和连续性	**普通类** 无要求。 **关键类** 1_C 就 PR.IP-09 （制定并管理响应计 划和恢 复计划）所述计划而言： a. 应采用冗余的网络、连接和应用架构。 2_C 应建立机制，以在遵守此处列明安全措施的前提下确保业务连续性。 3_C 应明确： a. 针对第 1_C 和 2_C 点所采用的安全政策； b. 遵守上述政策的流程、方法和技术。 **战略类** 4_S 就 PR.IP-09 （制定并管理响应计 划和恢 复计划）所述计划而言： a. 应设有与风险分析相一致的灾难恢复站点。 5_S 应有一份最新的详细文件，载明第 1_C 和 2_C 点所述流程和政策。	对于关键类服务，为确保系统的高可用性与业务持续性，需通过冗余的网络、连接和应用架构设计来提升容错能力，并建立专门的业务连续性管理机制以应对中断风险。同时，必须制定明确的安全政策，并配套相应的流程、方法和技术来确保这些要求得到有效执行。 对于战略类服务，应设有与风险分析相一致的灾难恢复站点。	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。 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IS0 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。 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

编号	具体控制要求	客户关注点	华为云的应答
			在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

6.1.3检测

编号	具体控制要求	客户关注点	华为云的应答
异常与事件 (DE.AE)：系统会检测异常活动，并分析其潜在影响。			
DE.AE-03 - 从多个传感器和来源收集并关联事件信息	**普通类** 无要求。 **关键类** 1_C 为及时发现影响数字基础设施的事件，应采用技术和程序工具，以便： a. 从多个传感器和来源获取信息； b. 接收并收集由意大利 CSIRT 以及主体内部或外部来源提供的有关数字基础设施安全的信息； c. 对所收集信息进行分析和关联以识别事件和事故，在适当情况下可自动化开展， 2_C. 应监控并记录事件信息分析和关联活动，记录（包括电子文件）应至少保存24个月。 3_C. 应明确规定： a. 用于识别第1_C条a)项所述传感器和数据源的政策； b. 获取第1_C条第a)和b)项所述信息的程序及技术工具； c. 用于第1_C条第c)项所述	对于关键类服务，应建立综合监控体系确保数字基础设施安全。该体系需利用技术和程序工具，实现从多传感器与来源及内部外部渠道持续获取安全信息。随后，应对收集到的信息进行自动化分析与关联，以主动、及时地识别安全事件与事故。 对于战略类服务，应保存主体用户的访问日志，并与第三方可直接访问的系统在逻辑层面隔离。	华为云PSIRT会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全 面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。 华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源ID(如：源IP、主机ID、用户ID等)、事件类型、日期时间、受影响的数据/组件/资源的ID（如目的IP、主机ID、服务ID等）、成功或失败等信息，以助力支撑网络

编号	具体控制要求	客户关注点	华为云的应答
	分析与关联的政策、流程及技术工具； d. 用于第2_C条所述监控与记录的流程及技术工具。 4_C. 应制定日志记录、监控、安全及访问日志保存的相关政策和程序，并至少每年更新一次。 5_C. 针对与安全信息收集、访问监控以及数据或元数据的未经授权修改或删除相关的活动使用系统开展审计。 6_C. 已制定并评估用于报告监控系统异常和故障的流程、程序及技术措施，并能立即向负责人发出通知。 **战略类** 7_S 应设有一套集中式存储库，保存主体用户的访问日志，该存储库由主体直接管理，并与第三方可直接访问的系统在逻辑层面隔离。 8_S 应有一份最新的详细文件，载明第 3_C 点所述流程和政策。		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，使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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。
安全持续监控（DE.CM）：对信息系统和资产进行监控，以识别网络安全事件并验证防护措施的有效性。			
DE.CM-01：对计算机网络进行监控，以发现潜在的网络安全事件	**普通类** 1_O. 应部署入侵检测系统（IDS）。 2_O. 应建立监测应用程序及其底层基础设施安全事件的流程。 **关键类** 与普通类一致。 **战略类** 3_S. 为了识别网络安全事件，系统应对进出流量、路由器和防火墙等边界系统的活动、重要的管理事件、对网络资源和终端用户工作站	客户应部署入侵检测系统，建立流程，用于监测与应用及其底层基础设施安全有关的事件；建立访问监测系统，以发现可疑活动，及时响应。 对于战略类服务，应对网络边界活动、重要管理事件、成功或失败访问等多方面关联分析来识别网络安全事件，且需要保障获取信息及分析事件的工具及时更新和正确配置，网络安全事件监控的政策流程应	华为云部署了IDS/IPS实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。 华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户 数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联 （DCI－Data Center

编号	具体控制要求	客户关注点	华为云的应答
	的成功或失败访问尝试进行监控和关联分析。 4_S. 第1_O.和3_S.条所述的技术工具应得到更新、维护和正确配置，符合PR.AC（身份管 理、认 证和访 问控制）、PR.DS（数据安全）、PR.IP（信息保护流程与程序）和PR.MA（维护）中的政策，并有助于遵守ID.AM（资产管理）、ID.GV（治理）、ID.SC（供应链风险管理）、PR.AC（身份管 理、认 证和访 问控制）和PR.DS（数据安全）中的政策。 5_S. 第 1_O. 点所述的技术工具亦用于 DE.AE （异常与事件）所述的目的。 6_S. 应建立最新的文件，其中至少描述： a. 针对第 2_O. 点采取的安全政策； b. 遵守安全政策的流程、方法和技术。	被文件化记录。	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。 在网络边界防护方面，华为云建立了稳固、完善的边界和多层立体的安全防护系统，部署了Anti-DDoS、IDS/IPS、WAF等防护机制。Anti-DDoS快速发现和防护DDoS攻击，实时对流量型攻击和应用层攻击进行全面防护；WAF实时检测和防御Web攻击，对高危攻击进行告警并立刻自动阻断。 华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源ID、事件类型、日期时间、受影响的数据/组件/资源的ID、成功或失败等信息，以助力支撑网络安全事件回溯。
DE.CM-04 - 检测恶意代码	**普通类** 1_O 应部署并使用适当的恶意软件预防和检测工具，以及终端保护系统（EPS）。 2_O 应制定反恶意软件保护政策；该等政策至少应每年审查一次。 **关键类** 同普通类要求。 **战略类** 3_S 应在所有设备上配置专门的软件防火墙。 4_S 所有传入的文件（通过电子邮件、下载、可移动存储介质等途径）都会经过扫描，包括通过沙箱技术进行检测。 5_S 第 1_O、3_S 和 4_S 点所述技术工具应在符合	组织应部署并使用适当的恶意软件预防和检测工具和终端保护系统，并制定反恶意软件保护政策。 对于战略类服务，应设置软件防火墙，传入文件应进行分析，制定反恶意软件、设备软件防火墙相关的安全政策。	华为云通过防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能，并且华为云终端设备均安装数据防泄漏（DLP）软件、浏览器和电子邮件安全管控措施。 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

编号	具体控制要求	客户关注点	华为云的应答
	PR.AC（身份管 理、认 证和访 问控制）、PR.DS（数据安全）、PR.IP（信息保护流程与程序） 和 PR.MA（维护）所述政策的前提下进行更新、维护和妥善配置，以协助落实这些政策。 6_S. 应建立一份至少描述区如下内容的文件： a. 针对第1_O、2_O、3_S和4_S条所采取的安全政策； b. 为确保遵守安全政策而采用的流程、方法和技术。		管理、以及业务连续性等。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。
DE.CM-07 - 开展监测以识别未经授权的人员、连接、设备或软件	**普通类** 无要求。 **关键类** 1_C 关于 PR.AC-03 （管理对资源的远程访问），应部署自动化的监控和访问控制系统发现对资源具有潜在未授权物理或远程访问权限的人员。 2_C 关于 ID.AM-01 （对组织内使用的系统及物理设备进行资产盘点），应部署适当的网络访问控制系统（除非有被验证的技术限制）以发现未经批准的设备（包括物理设备）。 3_C. 第1_C.和2_C.点所述的技术工具应保持最新、得到维护且配置妥当，符合 PR.AC（身份管 理、认 证和访 问控制）、PR.DS（数据安全）、PR.IP（信息保护流程与程序） 和 PR.MA（维护）的政策要求，并有助于遵守ID.AM（资产管理）、ID.GV（治理）、ID.SC（供应链风险管理）、PR.AC （身份管 理、认 证和访 问控制）和PR.DS（数据安全）的政策。 4_C. 应有一份最新的文件，	对于关键类服务，客户应部署监控未授权物理或远程访问、未经批准的设备接入的自动化系统，系统应及时更新且配置合理，符合数据安全、资产管理等相关安全要求。 对于战略类服务，客户应部署控制系统以发现未经批准的软件/未经授权的连接，系统应及时更新且配置合理，符合数据安全、资产管理等相关安全要求。	参考PR.AC-03、ID.AM-01、PR.AC、PR.DS、PR.IP 和 PR.M ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS回答。 客户除了通过**统一身份认证服务（ Identity and Access Management，简称IAM ）**，对远程接入人员的身份和权限进行管理外，华为云还提供了加密传输的方式供客户自行选择，比如VPN、HTTPS等。 同时，对于华为云内部系统的远程访问仅可以通过堡垒机和SVN的方式。华为云统一管理堡垒机和SVN的权限，对华为云运维人员进行身份认证，并且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。 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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全

编号	具体控制要求	客户关注点	华为云的应答
	其中至少应描述： a. 针对第1_C.和2_C.点所采取的安全政策； b. 协助遵守安全政策的流程、方法和技术。 **战略类** 5_S 关于 ID.AM-02 （盘点组织内使用的平台和应用），应部署控制系统以发现未经批准的软件（除非有被证明的技术限制）。 6_S 关于 ID.AM-03 （数据流和通信识别），应部署控制系统以发现未经授权的连接。 7_S 第 5_S 和 6_S 点所述技术工具应进行更新、维护并妥善配置。符合PR.AC（身份管 理、认 证和访 问控制）、PR.DS（数据安全）、PR.IP（信息保护流程与程序） 和 PR.MA（维护）的政策要求，并有助于遵守ID.AM（资产管理）、ID.GV（治理）、ID.SC（供应链风险管理）、PR.AC（身份管 理、认 证和访 问控制）和PR.DS（数据安全）的政策。 8_S. 应有一份最新的文件，其中至少应描述： a. 针对第5_S.和6_S.点所采取的安全政策； b. 协助遵守安全政策的流程、方法和技术。		管理提供指导。 华为云通过实施网络准入控制措施和远程访问限制，以限制设备的网络接入，以及未经授权的连接或者与越权操作。
DE.CM-08 - 执行漏洞识别扫描	**普通类** 1_O 风险分析中被识别为关键的平台和软件应在投入运行前开展渗透测试和漏洞评估。 2_O 应根据第 1_O 点所述平台和软件应用的关键程度，定期开展渗透测试和漏洞评估。	客户应在关键平台和软件投入运行前开展渗透测试和漏洞评估，运行后基于平台和软件的关键程度确定测试/评估频率。 客户还应建立文件化的渗透测试和漏洞评估计划，并保留评估记录。	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。

编号	具体控制要求	客户关注点	华为云的应答
	3_O 应存在一份最新文件，载明计划开展的渗透测试和漏洞评估的类型。 4_O 应存在一份最新登记册，记录已开展的渗透测试和漏洞评估，并附有相关文档。 **关键类** 同普通类要求。 **战略类** 同关键类要求。		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。
检测流程（DE.DP）：已制定、维护并验证了监测流程和程序，以确保对异常风况的理解。			
DE.DP-01：合理定义检测的角色和职责，以确保问责制	**普通类** 1_O. 网络安全的任命已在该主体内部公布。 2_O. 针对可能对数字基础设施造成影响的事件进行检测的准备工作，其职责、流程及责任已明确界定，并已向该机构的相关部门公布。 **关键类** 1_C. 网络安全的任命已在该主体内部公布。 2_C. 针对涉及数字基础设施的事件检测的准备工作的角色、流程和职责已明确界定，并已向该主体的相关部门公布。 3_C. 存在一份最新的详细文件，其中至少包含： a. 第 2_O 点所述的角色、流程和职责； b. 用于发布第 1_O 点和第 2_O 点所述的任命、角色和流程的流程。 4_C. 已建立并实施了一套根	客户应定义安全检测相关人员的角色和职责，并向相关部门公布。对于关键类服务，客户还应建立文件化的数据自处设施检测及报告流程。	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。 华为云制定了突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。华为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

编号	具体控制要求	客户关注点	华为云的应答
	据预先商定的指标向管理部门通报影响应用程序及底层基础设施的异常情况的机制。 **战略类** 同关键类要求。		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。

6.1.4响应

编号	具体控制要求	客户关注点	华为云的应答
响应规划（RS.RP）：执行并维护响应程序和流程，以确保对已发现的网络安全事件作出响应。			
RS.RP-01 -在事件发生期间或之后执行响应计划	**普通类** 无要求。 **关键类** 1_C 该响应计划规定，应通过DETECT（DE）类别中所述的分析和关联，对已发现的事件进行及时评估，并将评估结果立即传达给组织内的相关部门，包括向行政部门通报，以及在自愿基础上向CSIRT Italia通报影响数字基础设施的事件。 **战略类** 2_S 关于及时管理安全事件的政策和程序应至少每年审查一次。 3_S 第 1_C 和 2_S 点所述响应计划及相关政策和程序应涵盖关键内部部门、相关行政机构（如受到影响）以及所有相关第三方。 4_S 事件响应计划应按预定间隔进行测试并更新。 5_S. 已制定并监控与网络安全相关的重大事件指标。 6_S. 已制定并实施支持企业流程的流程、程序及措施，用于对安全相关事件进行分级处理。	对于关键类服务，客户应关联分析所检测到的事件，及时进行并立即将结果传达至组织内相关部门，以及在自愿基础上向CSIRT Italia通报。 对于战略类服务，客户应建立安全事件管理的政策与程序、安全事件分级处理机制、应急响应小组，并安排管理层定期参与相关事件的通报与审查。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。根据内部管理的要求，华为云每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。 华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。

编号	具体控制要求	客户关注点	华为云的应答
	7_S. 必须组建计算机应急响应小组（CERT），负责协调事件处理阶段，并遵循 ISO/IEC 27035-2 指南的规定。此外，应安排管理层定期参与相关事件状况的通报与审查，并在适当情况下参与事件处理，相关事宜亦应依据相关合同协议执行。		
通信（RS.CO）：应对工作需与内部及外部各方进行协调（例如，可能需要法律机构或执法部门提供支持）。			
RS.CO-01 -当需要响应时，人员知道他们的角色和操作顺序	**普通类** 1_O 明确界定事故响应各阶段和各流程的角色与职责，应，并告知相关部门。 **关键类** 1_C. 明确界定事故响应各阶段和各流程的角色与职责，应，并告知相关部门。 2_C. 定期开展演练。 3_C. 存在一份最新的详细文件，其中至少应包括： a. 第1_O.和2_C.条所述的阶段、流程、角色和职责； b. 通报第1_O.和2_C.条所述阶段、流程、角色和职责的流程； c. 第3条所述演练的具体实施方式。 4_C. 该主体须在事件记录并分类后1小时内，向管理部门通报任何安全事件或数据泄露。 5_C. 已制定安全事件管理、电子取证及云取证的相关政策与程序，并应至少每年进行一次审查和更新。 **战略类** 5_S 应制定关于安全事件管理、电子取证和云取证的政策与程序，并至少每年审查和更新一次。	组织应界定开展事故响应各阶段和各流程的角色与职责。 对于关键类服务，客户应进建立文件化事件响应机制，界定并向主体内有权负责的部门通报开展事件响应各阶段和流程的角色与职责，明确演练方案、安全事件管理、电子取证及云取证的相关政策与程序。 对于战略类服务，客户需制定并年审安全与取证政策，保留演练记录。实施证据保全流程，建立合规违规报告机制。安全事件及恢复工作须及时通报内外部相关方（含意大利CSIRT），确保全链路响应与协同。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。根据内部管理的要求，华为云每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。 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。 华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批。 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。 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

编号	具体控制要求	客户关注点	华为云的应答
	6_S 应保留一份已开展演练及参加人员的最新登记册，并附相关经验教训。 7_S 应定义并实施流程、程序和技术措施，以保全证据并支持取证分析。 8_S. 针对任何实际或疑似的安全违规（包括供应链相关的违规），均设有报告机制，且该机制符合服务水平协议（SLA）及适用的法律法规。 9_S. 针对安全事件开展的响应活动将通报给组织内部和外部的相关方，包括组织的管理层和高层领导。特别是，事故后的恢复工作应通报给内部和外部相关方（例如受害者、互联网服务提供商、受攻击系统的所有者、供应商、CERT/CSIRT），包括该主体的相关部门，以便与意大利CSIRT进行必要的沟通。		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。
RS.CO-05 - 主动与相关外部方共享信息	**普通类** 无要求。 **关键类** 1_C 应界定并保持与数字基础设施和网络安全相关的利益相关方群体之联系，以及与其他符合主体数字基础设施实际情况的相关主体之联系。 2_C 应界定并保持与适用监管机构、国家和地方执法机关以及其他相关主管机关的联系点。 **战略类** 同关键类要求。	对于关键类及战略类服务，应建立并维护与数字基础设施及网络安全相关的利益相关方及其他主体的联系机制。同时，应明确并保持与适用监管机构、执法机关等相关主管机关的固定联系点。	华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的沟通与交流。
分析（RS.AN）：开展分析工作，以确保对恢复工作提供有效的响应和支持。			
RS.AN-05 - 建立接	**普通类** 1_O 对CSIRT Italia（2019年8月8日部长会议主席令第4条	客户应监测CSIRT Italia主管机构、CERT 和信息共享与分析中心	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程并持续优化该机制。

编号	具体控制要求	客户关注点	华为云的应答
收、分析并响应网络安全相关信息的流程	所指）相关部门主管机构的通信渠道，以及任何相关CERT和信息共享与分析中心（ISAC）的通信渠道进行监控。 **关键类** 1_C. 对CSIRT Italia（2019年8月8日部长会议主席令第4条所指）相关部门主管机构的通信渠道，以及任何相关CERT和信息共享与分析中心（ISAC）的通信渠道进行监控。 2_C. 已将子类别DE.AE-03（从多个传感器和来源收集并关联事件信息）所述评估结果，以及子类别DE.CM-08所述渗透测试和漏洞评估结果传达给该主体的相关部门。 3_C. 存在一份最新文件，其中至少描述： a. 接收、分析并至少对通过第1_O.和2_O.项所述活动收集的信息作出响应的方式； b. 开展第1_O.和2_O.项所述活动所需的流程、角色、职责及技术工具。 **战略类** 同关键类要求。	（ISAC）的通信渠道及时接收、分析并响应相关要求。 对于关键类服务，客户还应将事件关联分析结果及渗透测试和漏洞评估结果传达给相关部门， 并建立文件化的监管响应机制。	安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。根据内部管理的要求，华为云每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。 华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。
缓解（RS.MI）：采取行动以防止安全事件扩大，减轻其影响并解决该事件。			
RS.MI-03 -缓解新识别的漏洞，或记录为可接受的风险	**普通类** 1_O 应按照漏洞管理计划（PR.IP-12）对漏洞进行缓解，或对未予缓解而产生的剩余风险进行记录并予以接受。 2_O 应界定并实施程序和技术措施，以便在识别出漏洞时，根据风险采取响应行动（无论是预先计划的还是因紧急情况触发的）。	客户须按计划缓解漏洞或记录剩余风险，并实施程序与技术措施，确保漏洞识别后能迅速响应。	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

编号	具体控制要求	客户关注点	华为云的应答
	关键类 同普通类要求。 **战略类** 同关键类要求。		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。

6.1.5恢复

编号	具体控制要求	客户关注点	华为云的应答
RC.RP-01 - 已建立恢复计划，并在网络安全事件期间或之后执行			
RC.RP-01 - 已建立恢复计划，并在网络安全事件期间或之后执行	**普通类** 1_O. 应存在一项恢复计划，至少规定在网络安全事件影响云服务时恢复其正常运行所必需的流程和程序。 **关键类** 2_C. 恢复计划应每六个月测试一次，并作为每年两次演练的一部分实施。 **战略类** 同关键类要求。	客户应建立恢复计划，并在网络安全事件期间或之后执行。对于关键类服务，恢复计划应每六个月测试一次，并作为每年两次演练的一部分实施。	客户可依赖华为云数据中心集群的多地域（ Region ）和多可用区 AZ ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。 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。
改进（RC.IM）：恢复计划及相关流程已得到改进，并吸取了经验教训以指导未来的工作。			
RC.IM-02 - 更新恢复策略	**普通类** 无要求。 **关键类** 同普通类要求。 **战略类** 1_S RC.RP-01 子类别所述计划应保持更新，并考虑既往恢复活动中获得的经验教训。	对于战略类服务，客户的恢复计划应保持更新，并考虑既往恢复活动中获得的经验教训。	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

编号	具体控制要求	客户关注点	华为云的应答
			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。 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。 华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息 安全事件的进展、处置措施与落实，对事件处置后的影响进行分 析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回 溯，并形成事件报告总结经验教训，在报告中告知事件的描述、 起因、影响、华为云已采取的措施等内容。此外，华为云每年对 高风险事件处理过程进行回顾，以确保高风险事件的处理过程满 足公司实际的业务需求。
通信（RC.CO）：事故发生后的恢复工作需与内部及外部各方（例如受害者、互联网服务提供商、受攻击系统的所有者、供应商、CERT/CSIRT）进行协调。			
RC.CO-03 - 将事件后的恢复活动通报相关方	**普通类** 无要求。 **关键类** 同普通类要求。 **战略类** 1_S 事故发生后的恢复活动应通知相关内部和外部方（例如受害者、互联网服务提供商、遭攻击系统所有者、供应商以及 CERT / CSIRT）。	对于战略类服务，事故发生后的恢复活动应通知相关内部和外部方。	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。

6.2 公共行政云服务的特征

6.2.1 识别

编号	具体控制要求	客户关注点	华为云的应答
资产管理（ID.AM）：组织所需的数据、人员、设备、系统及设施均已明确识别，并根据组织的风险目标和策略进行管理。			
ID.AM-01 - 对组织内使用的系统和物理设备进行清点登记	**普通类** 1_O. 所有系统和物理设备均应完成清点登记，并应建立一份由主体内部相关人员批准的清单。 2_O. 网络中的所有系统和物理设备均应完成清点登记，且只有获批准者方可接入网络。 **关键类** 同普通类要求。 **战略类** 同关键类要求。	客户的所有系统和物理设备均应完成清点登记，并应建立一份清单。 客户的所有系统和物理设备均应完成清点登记，且只有获批准者方可接入网络。	华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。华为云接入网络的设备通过证书与网络控制器进行身份验证，确保接入网络的设备真实可靠。
ID.AM-02 - 对组织内使用的平台和软件应用进行清点登记	**普通类** 1_O. 所有已安装的平台和软件应用均应完成清点登记，并应建立一份由主体内部相关人员批准的清单。 2_O. 仅允许安装已获批准的平台和软件应用。 3_O. 应制定政策，限制对组织资产进行未经授权的增加、删除、更新以及其他未经授权的管理行为。 **关键类** 同普通类要求。 **战略类** 同关键类要求。	1.客户所有已安装的平台和软件应用均应完成清点登记，并应建立一份由主体内部相关人员批准的清单。仅允许安装已获批准的平台和软件应用。 2.客户应制定政策，限制对组织资产进行未经授权的增加、删除、更新以及其他未经授权的管理行为。	1. 华为云定期对华为云的硬件、软件、数据、人员和服务进行识别。华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。 2. 华为云提供的**配置审计 Config** 支持客户实现云上平台资产管理。配置审计 Config（原 资源管理服务 RMS）提供全局资源配置的检索，资源清单，资源记录器，配置历史追溯，以及基于资源配置的持续的审计评估能力，确保云上资源配置变更符合客户预期。客户可以使用Config查看自己所拥有的资源有哪些；可以查看资

编号	具体控制要求	客户关注点	华为云的应答
			源详情、资源之间的关系、资源历史；Config会在资源变更时发送消息通知，并定期（6小时）对客户的资源变更消息进行存储；Config还会定期（24小时）对客户的资源进行存储；客户还可以通过配置合规规则来对自己的资源进行合规性检查。 3. 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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。
ID.AM-03 - 识别与组织相关的数据流和通信流	**普通类** 1_O. 所有数据流和信息流，包括对外流向以及与云服务有关的流量，均应被识别、登记并经主体内部相关人员批准。 **关键类** 同普通类要求。 **战略类** 同关键类要求。	客户所有数据流和信息流均应被识别、登记并经主体内部相关人员批准。	客户可以使用华为云**数据安全中心服务（Data Security Center，简称DSC）**实现对外传输的数据流以及与数字基础设施相关的数据流的安全控制。 每个云服务在设计研发阶段都应制定数据流图，通过数据流转图展示业务中各种数据的生命周期以及华为云所执行的操作，并明确操作目的。各业务领域在充分识别本领域数据资产的基础上，形成数据资产清单与数据流图，每年例行盘点。

编号	具体控制要求	客户关注点	华为云的应答
ID.AM-06 - 为全体人员及相关第三方明确并公布网络安全角色与职责	**普通类** 1_O. 应界定并向主体内相关部门公开其网络安全组织设置，包括面向所有人员及相关第三方的角色和职责。 2_O. 在第 1_O. 项所述组织架构内，应指定一名负责人及其替代人员，负责管理本规章规定的实施；该负责人应具备网络安全领域的专门专业能力，直接向主体管理层汇报，并确保本附件规定的安全措施得到有效落实。 3_O. 在第 1_O. 项所述组织架构内，还应指定一名技术联络人及至少一名替代人员，具备网络安全专业技术能力，负责与 CSIRT Italia 就影响云服务的事件管理进行对接。 4_O. 第 2_O. 项所述负责人和第 3_O. 项所述技术联络人应保持紧密协作。 **关键类** 5_C. 主体应将第 2_O. 项所述负责人以及第 3_O. 项所述技术联络人的姓名和联系方式报送国家网络安全局（ACN）。 6_C. 应建立一份清单，载明参与网络安全流程且具有特定角色和职责的全部内部和外部人员；该清单应传达至主体相关部门。 7_C. 就外部依赖关系而言，应建立一份第三方中与第 2_O. 项负责人及第 3_O. 项技术联络人相对应	1.客户应界定并向主体内相关部门公开其网络安全组织设置，包括面向所有人员及相关第三方的角色和职责。客户应指定一名负责人及其替代人员，负责管理本规章规定的实施。 2.客户应指定一名技术联络人及至少一名替代人员，具备网络安全专业技术能力，负责与 CSIRT Italia 就影响云服务的事件管理进行对接。 3.对于关键类客户应将负责人以及技术联络人的姓名和联系方式报送国家网络安全局（ACN）。建立一份清单，载明参与网络安全流程且具有特定角色和职责的全部内部和外部人员；该清单应传达至主体相关部门。 建立一份第三方中与负责人及技术联络人相对应人员的清单传达至主体相关部门。负责人还应确保与 ACN 开展协作，包括与 2019 年第 105 号法令第 5 条相关的活动，以及与 2021 年第 82 号法令赋予国家网络安全核心（NCS）的网络危机预防、准备和管理活动相关的协作。	1.在公司层面，华为云的最高管理层负责决策和批准公司总体网络安全战略。华为与安全管理部门负责制定和执行华为端到端网络安全保障体系与安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。同时，华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。 2. 华为云根据法律要求，设立了数据保护官。如有任何问题、意见或建议等，客户可以通过 dposg@huaweicloud.com 与数据保护官联系。

编号	具体控制要求	客户关注点	华为云的应答
	人员的清单；就内部依赖关系而言，也应建立主体内部对应人员清单。负责人和技术联络人的能力要求应根据依赖类型重新评估。该清单应传达至主体相关部门。 8_C. 第 2_O. 项所述负责人还应确保与 ACN 开展协作，包括与 2019 年第 105 号法令第 5 条相关的活动，以及与 2021 年第 82 号法令赋予国家网络安全核心（NCS）的网络危机预防、准备和管理活动相关的协作。 **战略类** 同关键类要求。		
治理（ID.GV）：用于管理和监控组织各项要求（包括组织要求、法律要求、风险相关要求及环境要求）的政策、程序和流程，均被纳入并应用于网络安全风险管理中。			
ID.GV-01 - 识别并公布网络安全政策	**普通类** 1_O. 应存在一份最新文件，描述网络安全政策、流程和程序。 2_O. 第 1_O. 项所述文件必须经主体批准，并至少每年更新一次，或在组织内部发生重大变化时及时更新。 **关键类** 3_C. 对第 1_O. 项所述文件中内部界定的最低安全水平的任何偏离，均应作出专门说明并纳入治理。 4_C. 应存在一份最新文件，就网络安全方案的规划、角色分配、实施、运行、评估和改进提供指引，覆盖内部人员和相关第三方。	客户应存在一份最新文件，描述网络安全政策、流程和程序。该文件必须经主体批准，并至少每年更新一次，或在组织内部发生重大变化时及时更新。文件中内部设定的最低安全水平的任何偏离，均应通过结构化治理流程予以识别、管理，并在必要时获得授权。 对于关键类服务，文件中内部界定的最低安全水平的任何偏离，均应作出专门说明并纳入治理。应存在一份最新文件，就网络安全方案的规划、角色分配、实施、运行、评估和改进提供指引，覆盖内部人员和相关第三方。	1. 华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批。 2. 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。 3. 华为云计算首席安全与隐私保护管负责制定华为云端到端的网络安全与隐私保护找略，推动集团安全与隐私保护战略在华为云的有效落地，组织制定华为云安全与隐私保护业务规划，管理和监督各业务部门制定安全竞争力规划并落地。

编号	具体控制要求	客户关注点	华为云的应答
	战略类 同关键类要求。		4.华为云建立完善的安全隐私稽查机制，华为云每年将根据外部环境变化和内容情况开展稽查，同时，每年也会聘请第三方提供审计服务。审计结果的追踪通过华为云安全风险管理平台实现，包括问题记录、定级、进展跟踪和提醒，确保准时整改完成。
ID.GV-04 - 治理和风险管理流程纳入网络安全风险管理	**普通类** 1_O. 描述风险管理流程的最新文件应包含与网络安全风险有关的部分。 2_O. 应建立正式的企业风险管理（ERM）方案，其中包括识别、评估、归属、处置和接受云安全及隐私风险的政策与程序。 **关键类** 同普通类要求。 **战略类** 同关键类要求。	客户描述风险管理流程的最新文件应包含与网络安全风险有关的部分。建立正式的企业风险管理（ERM）方案，其中包括识别、评估、归属、处置和接受云安全及隐私风险的政策与程序。	华为云制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。
风险评估（ID.RA）：企业需全面了解与组织运营（包括使命、职能、形象或声誉）、资产及人员相关的网络安全风险。			
ID.RA-01 - 识别并记录组织资源的脆弱性	**普通类** 1_O. 应存在一份最新的安全验证与测试计划，描述旨在评估云服务网络安全水平以及技术和程序性安全措施有效性的全部活动，并载明执行频率和方式。 2_O. 应建立相关程序，并至少每年更新一次，以管理组织资产变更所带来的风险，包括应用、系统、基础设施、配置等，无论该等资产由内部还是外部（即外包）管理。 **关键类** 3_C. 第 1_O. 项所述验证和测试的定期报告至少应	客户应存在一份最新的安全验证与测试计划，描述旨在评估云服务网络安全水平以及技术和程序性安全措施有效性的全部活动，并载明执行频率和方式。 客户应建立相关程序，并至少每年更新一次，以管理组织资产变更所带来的风险，包括应用、系统、基础设施、配置等，无论该等资产由内部还是外部（即外包）管理。 对于关键类服务，验证和测试的定期报告至少应包括：	1. 华为云内部制定完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。 2. 华为云已发布漏洞管理和渗

编号	具体控制要求	客户关注点	华为云的应答
	包括： a. 已实施核查类型及其结果的总体说明； b. 已发现漏洞及其安全影响等级的详细说明； c. 因利用相关漏洞而可能被访问的系统资源暴露程度。 4_C. 应存在一份漏洞修复文件，其中还应规定向相关方发出通知。 **战略类** 同关键类要求。	a. 已实施核查类型及其结果的总体说明； b. 已发现漏洞及其安全影响等级的详细说明； c. 因利用相关漏洞而可能被访问的系统资源暴露程度。应存在一份漏洞修复文件，其中还应规定向相关方发出通知。	透测试相关的制度，明确漏洞评估和渗透测试的流程与方法，并且每年对这些制度进行审视和刷新。 3. 华为云风险管理人员遵循制定的网络安全风险管理规范，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划，包括整改措施、计划、关键里程碑和风险降级标准，利用风险整改、风险保持、风险避免和风险转移等措施降低和消除风险至可接受范围。
ID.RA-05 - 利用威胁、脆弱性、发生概率及其影响来确定风险	**普通类** 1_O. 应结合威胁、漏洞、其发生概率以及在所考虑威胁背景下被利用后产生的影响开展风险分析。 2_O. 风险分析应考虑云服务的内部和外部依赖关系。 3_O. 在识别并分析全部风险因素后，应进行权衡，以确定风险等级。 **关键类** 4_C. 应存在一份最新的风险评估文件，至少包括： a. 对内外部威胁及其发生概率的识别、适当描述和评估； b. ID.RA-1 子类和 DE.CM-8 子类所述漏洞； c. 被视为对云服务具有重大意义的潜在影响，并作出适当描述和评估； d. 风险的识别、分析和权衡。 **战略类** 同关键类要求。	客户应结合威胁、漏洞、其发生概率以及在所考虑威胁背景下被利用后产生的影响开展风险分析。风险分析应考虑云服务的内部和外部依赖关系。在识别并分析全部风险因素后，应进行权衡，以确定风险等级。 对于关键类服务，客户应存在一份最新的风险评估文件，至少包括： a. 对内外部威胁及其发生概率的识别、适当描述和评估； b. ID.RA-1 子类和 DE.CM-8 子类所述漏洞； c. 被视为对云服务具有重大意义的潜在影响，并作出适当描述和评估； d. 风险的识别、分析和权衡。	华为云制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。 华为云建立并实施了文档化的网络风险安全政策和程序，为操作网络安全管理提供指导，风险评估程序中要求进行内外部威胁识别、风险分析和定级、风险处置要求，网络安全政策和程序发布前需得到管理者审批。

编号	具体控制要求	客户关注点	华为云的应答
供应链风险管理（ID.SC）：组织已确定其优先事项、约束条件、风险容忍度及假设，并将其用于支持与供应链风险管理相关的风险决策。组织已制定并实施了用于识别、评估和管理供应链风险的流程。			
ID.SC-01 - 网络供应链风险管理流程已识别、明确定义、验证、管理并获得内部批准	**普通类** 1_O. 应界定网络供应链风险管理流程。 2_O. 上述流程应由主体管理层验证并批准。 **关键类** 3_C. 组织内部应建立并至少每年更新一次有关界定、实施和适用共享安全责任模型（SSRM）的政策和程序，用于处理与外部主体和/或第三方行政机构之间的责任划分。 4_C. SSRM 应适用于整个网络供应链，包括组织使用的其他云服务。 5_C. 应对责任分担作出清晰界定。 **战略类** 6_S. 应存在一份文件，载明第 1_O. 项和第 2_O. 项所述流程。	客户应界定网络供应链风险管理流程，该流程应由主体管理层验证并批准。 对于关键类服务，组织内部应建立并至少每年更新一次有关界定、实施和适用共享安全责任模型（SSRM）的政策和程序，用于处理与外部主体和/或第三方行政机构之间的责任划分。 对于战略类服务，应存在一份文件，载明普通类和关键类所述流程。	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。 华为云建立了严密的安全责任体系，根据华为云安全责任共担模型，对于部署在华为云环境的部分，客户可以依赖华为云的符合性证明。 华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。
ID.SC-02 - 通过网络供应链风险评估流程识别、排序并评估 IT 系统、组件和服务的第三方供应商及合作伙伴	**普通类** 无要求。 **关键类** 1_C. 就云服务采购而言，应通过以下方式采取网络供应链安全措施： a. 自设计阶段起，即在采购过程中吸纳网络安全组织参与，其中包括 ID.AM-06 子类第 2_O. 项所述负责人； b. 在不违背已记录技术限制的前提下，满足可替代性要求，使在期限届满时可以转向其他供应商；	对于关键类服务，应通过网络供应链风险评估流程识别、排序并评估 IT 系统、组件和服务的第三方供应商及合作伙伴。 对于战略类服务，应对技术可靠性开展进一步评估。	华为云会安排专人积极配合客户发起的背调要求和尽职调查。同时，华为云在采购前会对供应商资质进行评估，根据供应商所提供的产品和服务制定不同级别的评估要求，仅经过资质认证的供应商才能进入华为云的采购范围。华为云建立并维护供应商清单，每年对供应商的安全风险进行评估。 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

编号	具体控制要求	客户关注点	华为云的应答
	c. 在不违背已记录技术限制的前提下，实现供应商多元化，从而提高云服务韧性； d. 参照最佳实践，对供应商和第三方合作伙伴的技术可靠性进行评估，至少应考虑其产品质量、网络安全实践、其对自身供应链的控制，以及所供应产品/组件对该服务的重要性。 2_C. 是否存在一份关于云服务提供商及受托第三方合作伙伴的最新清单，以及外部依赖关系清单，并附有第1_C条所述的评估流程相关文件。 **战略类** 3_S. 在可行且与关键性相称的情况下，建议： a. 对第 1_C. 项 d 目所述技术可靠性开展进一步评估，同时至少考虑：1）供应商是否愿意共享源代码；2）有助于评估生产者软件开发流程质量的认证或证据；3）生产者是否采用程序和技术工具，以保证安装于 ICT 产品和系统中的软件或固件的真实性和完整性；4）生产者是否采用程序和技术工具，以保证源代码与已安装/执行目标代码之间一一对应； b. 采用流程和技术工具，以便：1）在生产者提供源代码时评估其质量和安全性；2）从 ICT 产品和系统中获取目标代码；3) 确认源代码与已安装并运行的目标代码之间存在唯一对应关系。		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。 华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。 华为云已获得的ISO/IEC 27034（应用安全）认证。该标准专门关注应用生命周期中的安全流程，华为云在软件开发、构建、部署等环节建立了控制措施，以保障最终交付物（目标代码）与设计源头（源代码）的可追溯性和一致性。

编号	具体控制要求	客户关注点	华为云的应答
ID.SC-03 - 通过与第三方供应商和合作伙伴的合同落实适当措施，以实现组织网络安全计划目标和网络供应链风险管理计划	**普通类** 无要求。 **关键类** 1_C. 主体针对内部依赖关系所实施的安全措施，应结合风险分析结果，与适用于云服务的安全措施保持一致。为此，应相应更新合同、协议或安排。 **战略类** 2_S. 第三方外包服务承接方所实施的安全措施，应结合风险分析结果，与适用于云服务的安全措施保持一致。为此，应相应更新合同、协议或安排。	对于关键类服务，应通过与第三方供应商和合作伙伴的合同落实适当措施，以实现组织网络安全计划目标和网络供应链风险管理计划。 对于战略类服务，应在合同中规定第三方外包服务承接方所实施的安全措施，应结合风险分析结果，与适用于云服务的安全措施保持一致。	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。 华为云已建立供应商管理体系，维护符合资质的供应商采购名单，按照自身的网络安全与隐私要求对供应商提出要求和监督。在供应商引入前会进行尽职调查，签署合同、服务协议、保密协议，约定双方责任与义务、服务水平等要求，供应商引入后每年对供应商的安全风险进行评估及安全稽查。
ID.SC-04 - 通过审计、核查或其他评估方式定期评估第三方供应商和合作伙伴，以确认其履行合同义务	**普通类** 无要求。 **关键类** 1_C. 应存在一份最新文件，说明对供应商和第三方合作伙伴进行评估的流程、方式和频率，并与已实施风险分析结果相称。 2_C. 应存在一份最新计划，列明拟开展的审计、核查或其他评估形式，同时应建立已实施评估及其相关文档的登记册。 3_C. 应界定并实施审计管理流程，以便至少每年一次、并按照考虑风险的计划开展独立保证评估，同时符合主要行业标准。 4_C. 关于审计和标准符合性保证的政策与程序，应予建立、形成文件、批准、维护，并至少每年审查一次。	对于关键类服务，应制定对供应商和第三方合作伙伴进行评估的流程的文件。制定审计计划，方式，流程，每年审查。	华为云已建立供应商评估机制，采购前会对供应商资质进行评估，根据供应商所提供的产品和服务制定不同级别的评估要求，仅经过资质认证的供应商才能进入华为云的采购范围。 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。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。 华为云目前已获得多项国际上权威的安全与合规认证。华为云每年会聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计。

编号	具体控制要求	客户关注点	华为云的应答
	5_C. 应就供应商和第三方合作伙伴中发现的不符合项相关纠正措施，界定、记录、批准、传达、实施并维护一项整改计划（Remediation plan）。 **战略类** 同关键类要求。		

6.2.2 保护

编号	具体控制要求	客户关注点	华为云的应答
身份管理、身份验证与访问控制（PR.AC）：对物理和逻辑资产及其相关资源的访问仅限于经授权的人员、流程和设备，且其管理方式应与针对未经授权访问授权活动和交易的风险评估保持一致。			
PR.AC-01 - 对授权用户、设备和流程的数字身份与访问凭证进行管理、核验、撤销并接受安全审计	**普通类** 1_O. 访问凭证应针对主体人员或参与服务管理的其他人员实行一人一证，并遵循职能分离原则。凭证更新频率应与用户权限水平相匹配。 2_O. 应建立第 1_O. 项所述凭证的管理政策和程序；其应至少每年更新一次，并向行政机构开放查阅。 3_O. 应界定关于凭证信息、系统身份以及访问级别的管理、存储和审查机制。 4_O. 在用户状态发生变化时（例如人员调岗），应及时且无不当延迟地更新凭证。 5_O. 系统身份应通过数字证书或其他能够确保同等安全水平的技术进行管理。 6_O. 应存在一份最新的安	客户应对授权用户、设备和流程的数字身份与访问凭证进行管理、核验、撤销并接受安全审计。 对于关键类服务，客户应制定一份最新的详细文件，包括： a. 针对数字身份的管理、核验、撤销及安全审计； b. 针对用户数字身份和访问凭证的管理、核验、撤销及安全审计而采取的安全政策； c. 为遵守上述安全政策而采用的流程、方法和技术。	华为云制定并记录正式的逻辑安全的政策和程序。及时批准、添加、修改或禁用，并定期审查华为员工和承包商的用户帐户。华为建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循和授予的。 华为云内部建立了运维和运营账号管理机制，华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。此外，还采用双因子认证对云为人员进行身份认证，如 USB key、Smart Card 等。所有运维账号由LDAP集中管理，通过统一运维审计平台集中监控并进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC权限管理。保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。

编号	具体控制要求	客户关注点	华为云的应答
	全审计计划，用于核查第 1_O. 至第 5_O. 项的遵守情况，并应建立已实施审计及其相关文档的登记册。 **关键类** 7_C. 应存在一份最新的详细文件，至少包括： a. 针对数字身份的管理、核验、撤销及安全审计，以及第 1_O. 至第 6_O. 项所述程序而采取的安全政策； b. 针对用户数字身份和访问凭证的管理、核验、撤销及安全审计而采取的安全政策； c. 为遵守上述安全政策而采用的流程、方法和技术。 **战略类** 同关键类要求。		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。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CTS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。
PR.AC-03 - 对资源的	**普通类** 1_O. 远程访问应由主体的	客户应监控远程访问，实施适当的访问控制措	1. 华为云建立身份与访问安全管理机制，涵盖对资源远程

编号	具体控制要求	客户关注点	华为云的应答
远程访问进行管理	网络安全组织进行监控。 2_O. 在不违背已记录的技术限制前提下，应实施适当的访问控制措施，采用集中式认证、授权以及访问记录/计账系统，并辅以与风险相称安全水平的认证机制。 3_O. 应界定并实施集中式访问管理模型，用于对行政机构资源和数据访问的授权、日志记录和通报。 4_O. 应建立远程访问日志。 5_O. 远程访问应采用多因素认证。 **关键类** 6_C. 应存在一份最新的详细文件，至少包括： a. 对可通过远程访问实施的活动以及已采取安全措施的界定所适用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 **战略类** 7_S. 相关政策和程序应至少每年更新一次，并在行政机构提出具体请求时供其查阅。 8_S. 在访问行政机构数据时，应界定并实施与行政机构的联合授权流程。若无法做到，主体应在最短时间内通知行政机构已发生的访问行为。 9_S. 所有涉及访问行政机	施，界定并实施集中式访问管理模型，用于对行政机构资源和数据访问的授权、日志记录和通报。 对于关键类服务，客户应存在一份最新的详细文件。 对战略类服务，客户云相关政策和程序应至少每年更新一次，并在行政机构提出具体请求时供其查阅。所有涉及访问行政机构数据的操作，均必须按照特权账户管理和日志记录标准进行管理。	访问的管控要求，包括对远程访问进行限制，限制远程执行特权命令、代码等，并对操作进行审计。华为云至少每年审查一次网络安全管理政策和流程，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。 2. 华为云不允许运维运营人员在未经授权的情况下访问客户的系统和数据。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因素认证，如USB key、SmartCard等。华为云管理员必须经过双因素认证后，才能通过堡垒机接入管理平面，所有操作都 会记录日志并及时传送到集中日志审计系统。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。 3. 华为云建立数据共享机制，数据的共享应获得数据所有者的授权，并按照数据级别和数据类型获得相应的审批并留存审批记录。 4. 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）**来实现集中式访问管理以及多因素认证： 5. 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。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

编号	具体控制要求	客户关注点	华为云的应答
	构数据的操作，均必须按照特权账户管理和日志记录标准进行管理。		户映射成华为云的临时用户，并访问用户的华为云资源。 6. 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。 7. 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。
PR.AC-04 - 按照最小权限和职责分离原则管理资源访问权及相关授权	**普通类** 1_O. 参照 ID.AM 类别下的清点结果，至少应界定以下内容： a. 需要访问的已登记资源，以及为履行何种职能、凭何种授权进行访问； b. 用户组及其权限，以及其可访问何种资源、依据何种授权； c. 已登记用户与用户组之间的分配关系。 2_O. 在实施对信息系统的访问时，应根据组织风险遵循职能分离和最小权限原则。 3_O. 应界定并实施政策、程序和技术措施，对特权访问角色进行分离，使对数据的管理性访问、加密与密钥管理能力以及日志	1.客户应参照 ID.AM 类别下的清点结果，界定： a.需要访问的已登记资源，以及为履行何种职能、凭何种授权进行访问； b.用户组及其权限，以及其可访问何种资源、依据何种授权； c.已登记用户与用户组之间的分配关系。 2.客户对信息系统的访问时，应根据组织风险遵循职能分离和最小权限原则。 3.客户应界定并实施政策、程序和技术措施，对特权访问角色进行分离，使对数据的管理性访问、加密与密钥管理能力以及日志能力彼此独立分隔。	1. 华为云已建立文件化的身份与访问管理机制，遵循职责分离原则，不同人员的权限依据职责确认角色，实现RBAC权限管理，实施最小化授权，权限的获取需通过主管审批并定期复核。 2. 作为云服务提供商，华为云在欧洲具备独立管理的数据中心，拥有运行底层物理与逻辑基础设施的自有能力，无需依赖第三方。 3. 客户可以使用华为云提供的华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**进行访问管理，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

编号	具体控制要求	客户关注点	华为云的应答
	能力彼此独立分隔。 **关键类** 4_C. 应存在一份最新的详细文件，载明第 1_O. 项所述流程。 **战略类** 5_S. 主体人员和第三方对行政机构数据实施的所有特权活动（例如安装更新）和访问，均必须获得网络安全组织授权，并限于绝对必要情形。	4.对于关键类服务，客户应存在一份最新的详细文件，载明流程。 5.对于战略类服务，主体人员和第三方对行政机构数据实施的所有特权活动（例如安装更新）和访问，均必须获得网络安全组织授权，并限于绝对必要情形。	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。
PR.AC-05 - 保护网络完整性（如网络隔离、网络分段）	**普通类** 1_O. 应建立网络基础设施安全政策和程序，并至少每年更新一次。 2_O. 应制定关于资源可用性、质量和充足能力的监测规划，以保证系统达到所要求的性能。 **关键类** 同普通类要求。 **战略类** 3_S. 参照 ID.AM 类别下的清点结果，应存在一份最新的详细文件，至少包括： a. 网络分段/隔离所采用的安全政策； b. 已隔离/已分段网络的说明； c. 为遵守上述安全政策而采用的流程、方法和技术； d. 对在用网络端口、协议和服务进行限制和/或监控的方式。	客户应建立网络基础设施安全政策和程序，并至少每年更新一次。应制定关于资源可用性、质量和充足能力的监测规划，以保证系统达到所要求的性能。 对于战略类服务，客户应参照 ID.AM 类别下的清点结果，应存在一份最新的详细文件，至少包括： a. 网络分段/隔离所采用的安全政策； b. 已隔离/已分段网络的说明； c. 为遵守上述安全政策而采用的流程、方法和技术； d. 对在用网络端口、协议和服务进行限制和/或监控的方式。	华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批。 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。另外，对于数据中心的维护，华为云建立了数据中心运维管理相关的制度与流程，其中包含设备的具体管控措施、例行的维护计划等。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。 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。 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。华为云的**企业主机安全（Host Security Service，简称HSS）**是服务器的贴身安全管家，可为金融机构提供资产管理功能，包括提供账号、端口、进程、Web目录和软件等安全资产信息的管理和分析。
PR.AC-07 - 用户、设备及其他资产的认证方式与交易风险相匹配	**普通类** 1_O. 应界定并实施访问系统、应用和数据的政策与程序，其中至少应对特权用户和数据访问采用多因素认证。 2_O. 就云服务而言，必须向行政机构保证提供多因素认证功能，或允许使用第三方多因素认证解决方案。关于可用多因素认证功能及其认证机制（例如电子邮件、短信或生物识别校验）的透明信息，必须向 ACN 和行政机构提供。 **关键类** 同普通类要求。 **战略类** 3_S. 应存在一份最新的详细文件，并参照 ID.AM 类别的清点结果及 ID.RA 类别的风险评估，至少载明： a. 可用的认证方式； b. 其对应分配至各类交易的方式。	客户应界定并实施访问系统、应用和数据的政策与程序，其中至少应对特权用户和数据访问采用多因素认证。向行政机构保证提供多因素认证功能，或允许使用第三方多因素认证解决方案。 对于战略类服务，客户存在一份最新的详细文件，并参照 ID.AM 类别的清点结果及 ID.RA 类别的风险评估。	华为云制定了密码策略及账号口令安全相关管理规范，对秘密鉴别信息的分配进行管理。新建系统中账号缺省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，严格纳管回收特权账号。使用IAM对访问进行管理，支持多因素认证用于登录验证和操作保护，员工每次登陆均需要使用多重身份验证确定身份。也提供会话超时策略、账号登陆和锁定策略。 华为云定期对华为云的硬件、软件、数据、人员和服务进行识别。华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。

编号	具体控制要求	客户关注点	华为云的应答
意识与培训（PR.AT）：对员工和第三方进行网络安全意识教育，并对其进行培训，使其能够按照现行政策、程序和协议履行各自的职责和角色。			
PR.AT-01 - 对服务提供方人员开展告知与培训	**普通类** 1_O. 应存在一份最新的详细文件，说明向主体人员提供的培训和教育内容，以及验证其掌握情况的方法。 2_O. 根据角色向主体用户提供的第 1_O. 项所述培训和教育，至少应涵盖以下主题： a. 明文或加密数据的保密性保护； b. 劳动关系结束时公司资产的返还； c. 角色和职责的界定； d. 访问系统、资产和资源的政策； e. 信息与安全管理政策； f. 将角色和职责传达给可访问信息资产员工的流程； g. 信息不披露/保密要求。 **关键类** 3_C. 对主体每一名员工，均应建立一份最新登记册，载明其所接受的指示。 **战略类** 同关键类要求。	客户应存在一份最新的详细文件，说明向主体人员提供的培训和教育内容，培训涵盖数据加密，离职交接，角色责任，访问控制，保密等方面。 对于关键类服务，对主体每一名员工，均应建立一份最新登记册，载明其所接受的指示。	作为云服务提供商，为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为对全体员工从意识教育普及、宣传活动开展、商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育。参考业界优秀实践，华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，提升员工能力，向客户交付安全的产品、解决方案与服务。为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响.华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。 华为云内部进行电子化流程记录，每次培训都由培训记录，需要参与人员签到。
PR.AT-02 - 特权用户理解其角色与职责	**普通类** 1_O. 应界定向主体特权人员提供的教育内容，以及核验其掌握情况的方法。 2_O. 对主体每一名员工，均应界定其被赋予的权限及其所接受的指示。 **关键类** 同普通类要求。	客户应界定向主体特权人员提供的教育内容，以及核验其掌握情况的方法。对主体每一名员工，均应界定其被赋予的权限及其所接受的指示。 对于战略类服务，需提供关于上述内容的详细文件。	在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。员工与公司签署的聘用协

编号	具体控制要求	客户关注点	华为云的应答
	战略类 3_S. 应存在一份最新的详细文件，载明第 1_O. 项和第 2_O. 项所述流程。		议中包含保密条款，其中明确说明员工的信息安全责任。对于合同方，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全责任。 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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。 华为云对关键岗位要求参加上岗培训和认证，签署网络安全与隐私保护承诺函，入职和仍然需要定期参加网络安全岗位和技能和意识培训考试。
数据安全（PR.DS）：数据应按照组织的风险管理策略进行存储和管理，以确保信息的完整性、机密性和可用性。			
PR.DS-01 - 存储数据受到保护	**普通类** 1_O. 行政机构数据，包括与安全相关的数据（例如访问控制系统数据），应通过位于欧盟境内的基础设施进行处理。除有正当且书面化的法律或技术理由外，该等基础设施还应包括： a. 业务连续性和灾难恢复基础设施，即使该等功能已外包（例如通过云计算）； b. 具有全球地理分发能力的内容分发网络。在此情形下，适用 ID.RA-05 措施时，必须适当考虑其位于欧洲境外的事实，并核查其是否符合个人数据保	客户的行政机构数据，包括与安全相关的数据（例如访问控制系统数据），应通过位于欧盟境内的基础设施进行处理。 客户应存在一份最新的详细文件，说明加密程序、加密实施及密钥管理，并至少每年更新一次，同时明确角色与职责。还应界定并实施关于加密密钥创建、到期停用、可能暂停及管理机制的流程、程序和措施。 对于关键类服务，主体应保证由行政机构自主	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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。 华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级

编号	具体控制要求	客户关注点	华为云的应答
	护法规。 2_O. 与“服务运行相关的元数据”不同，后者可以通过位于欧盟境外的基础设施处理；与行政机构有关的元数据原则上应通过位于欧盟境内的基础设施处理，除非存在正当且书面化的法律或技术理由。在此情形下，适用 ID.RA-05 措施时，必须适当考虑其位于欧洲境外的事实，并核查其是否符合个人数据保护法规。若相关元数据被传输至欧盟外基础设施，该通信流的中断也不得导致无法满足云服务规定的最低服务等级。 3_O. 就第 2_O. 项而言，如与行政机构有关的元数据系用于提供信息安全服务或增强数字基础设施韧性，则在存在正当技术理由并有证据证明其管理方式符合处理目的唯一性的情况下，也可在欧洲境外处理。在此情形下，适用 ID.RA-05 措施时，必须适当考虑其位于欧洲境外的事实，并核查其是否符合个人数据保护法规。若相关元数据被传输至欧盟外基础设施，该通信流的中断也不得导致无法满足云服务规定的最低服务等级。 4_O. 至少还应结合 ID.AM 类别明确： a. 用于数据存储和保护的安全政策； b. 为遵守上述安全政策所采用的流程、方法和技	管理加密密钥，并为单一用途生成秘密和私有加密密钥，同时确保符合前述要求。 此外应存在一份最新的详细文件，说明用于数据存储和保护的安全政策；为遵守上述安全政策所采用的流程、方法和技术。 云服务应支持“自带密钥”（BYOK）加密机制，使行政机构能够至少自主生成主加密密钥（root key）；该密钥应通过部署于以下任一位置的 HSM 生成。 与行政机构有关的元数据，它的密钥安全需导入云环境的功能，以执行云中全部密钥管理和加密操作。应界定并实施程序和技术措施，用于销毁存储于安全环境外的密钥，并在 HSM 中存储的密钥不再需要时予以撤销，且应符合相关法律监管要求。 对于战略类服务，主体将欧盟外主体提出的任何访问数据或元数据请求，报告给国家网络安全局（ACN）和行政机构；仅在行政机构明确授权后，方可向欧盟外主体提供对行政机构数据或元数据的访问。 此外，应存在一份最新文件，说明云服务由哪些站点和基础设施提供。主体应将该清单提供给行政机构。	别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标记安全等级。同时，华为云也制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。 针对于静态数据，华为云为保护租户数据的存储安全采取了一系列的保护机制。首先，华为云提供了**密码安全中心（Data Encryption Workshop，简称 DEW）**。它帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM Hardware Security Module），为租户创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。与华为云服务对接 KMS 的服务有 OBS、云硬盘等。

编号	具体控制要求	客户关注点	华为云的应答
	术。 5_O. 关于加密密钥： a. 应存在一份最新的详细文件，说明加密程序、加密实施及密钥管理，并至少每年更新一次，同时明确角色与职责； b. 应针对系统、政策以及加密/密钥管理流程开展定期复核，以应对风险暴露增加；该等复核应通过审计进行，至少每年一次，或在任何安全事件后进行； c. 应通过密码库生成加密密钥，并说明所用算法和随机数发生器； d. 应根据密钥有效期设置轮换机制，并考虑相关风险及法律监管要求。 6_O. 关于加密密钥，经行政机构请求，主体应保证： a. 由行政机构自主管理； b. 为单一用途生成秘密和私有加密密钥。 7_O. 应建立流程、程序和技术措施，以便在密钥被破坏或某主体不再属于组织时，在有效期届满前撤销并移除加密密钥，并符合法律监管要求，且与第 5_O. 项和第 6_O. 项保持一致。 8_O. 应结合第 5_O. 项和第 6_O. 项，界定并实施关于加密密钥创建、到期停用、可能暂停及管理机制的流程、程序和措施。 **关键类** 9_C. 对于行政机构的关键		

编号	具体控制要求	客户关注点	华为云的应答
	类数据和服务，第 6_O. 项不适用。就加密密钥而言，主体应保证由行政机构自主管理，并为单一用途生成秘密和私有加密密钥，同时确保符合第 7_O. 项和第 8_O. 项要求。 10_C. 应存在一份最新的详细文件，并至少结合 ID.AM 类别载明： a. 用于数据存储和保护的安全政策； b. 为遵守上述安全政策所采用的流程、方法和技术。 11_C. 云服务应支持“自带密钥”（BYOK）加密机制，使行政机构能够至少自主生成主加密密钥（root key）；该密钥应通过部署于以下任一位置的 HSM 生成： a. 行政机构自身基础设施； b. 由提供方以专用方式向行政机构提供的基础设施； c. 由行政机构选择的第三方基础设施。 12_C. 对于行政机构的关键类数据和服务，第 3_O. 项不适用。因此，就与行政机构有关的元数据处理而言，仍适用第 2_O. 项。 13_C. 应界定并实施程序和技术措施，用于销毁存储于安全环境外的密钥，并在 HSM 中存储的密钥不再需要时予以撤销，且应符合相关法律监管要求。		

编号	具体控制要求	客户关注点	华为云的应答
	14_C. 主体应提供将第 12_C. 项所述密钥安全导入云环境的功能，以执行云中全部密钥管理和加密操作。 **战略类** 15_S. 就欧盟外主体访问数据而言，主体应： a. 将欧盟外主体提出的任何访问数据或元数据请求，报告给国家网络安全局（ACN）和行政机构； b. 仅在行政机构明确授权后，方可向欧盟外主体提供对行政机构数据或元数据的访问。 16_S. 应存在一份最新文件，说明云服务由哪些站点和基础设施提供。主体应将该清单提供给行政机构。 17_S. 对于行政机构的战略类数据和服务，第 2_O. 项不适用。因此，除提供第 1_O. 项所述服务所必需的元数据外，所有类型的元数据都必须通过位于欧盟境内的基础设施进行处理。		
PR.DS-02 - 数据在传输过程中受到保护	**普通类** 1_O. 在将服务器、服务、应用或数据迁移至云环境时，应使用安全且加密的通信通道。该等通道仅可采用最新且获批准的协议。 **关键类** 2_C. 应按照 ID.RA-05 措施所述风险分析，对 ID.AM-03 措施所述数据流和通信使用安全且加密	客户在将服务器、服务、应用或数据迁移至云环境时，应使用安全且加密的通信通道。 对于关键类服务，应按照风险分析，对所述数据流和通信使用安全且加密的通信通道以及最新、获批准的协议。	华为云提供的**云数据迁移（Cloud Data Migration，简称CDM）**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。CDM在用户VPC中运行，网络隔离确保数据传输的安全性。支持SSL的数据源，如RDS、SFTP等，可以使用SSL。CDM还支持公网数据源的数据上云，用

编号	具体控制要求	客户关注点	华为云的应答
	的通信通道以及最新、获批准的协议。 **战略类** 同关键类要求。		户可以利用VPN和SSL技术来避免传输安全风险。 针对于传输中的数据，华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过虚拟专用网络（ VPN ）和应用层 TLS 与证书管理，华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。
PR.DS-03 - 通过正式流程管理数据存储介质的物理转移、移除和销毁	**普通类** 1_O. 参照 ID.AM 类别，应界定： a. 对数据存储设备的物理转移、移除和销毁所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 **关键类** 2_C. 对所有受管移动设备，应启用远程地理定位能力；若该等设备被破坏，可能会影响服务可用性，或影响与之相关数据的可用性、完整性或保密性。 3_C. 与第 2_C. 项保持一致，应界定并实施对行政机构数据进行远程删除的适当技术。 **战略类** 4_S. 应存在一份最新的详细文件，载明第 1_O. 项所述流程和政策。	客户应界定对数据存储设备的物理转移、移除和销毁所采用的安全政策和采用的流程、方法和技术。 对于关键类服务，客户应对所有受管移动设备，启用远程地理定位能力。此外，应界定并实施对行政机构数据进行远程删除的适当技术。 对于战略类服务，客户应存在一份最新的详细文件，说明流程和政策。	华为云已建立文件化的介质管理要求，使用包含存储介质的设备由专人管理，使用完毕后由专人对其进行格式化处理。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。当物理磁盘报废时，华为云通过对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保用户 隐私和数据不受未授权访问。若该等设备遭到破坏，可能影响基础设施或其所提供服务的可用性、完整性或保密性。员工可向业务主管和信息安全部门报告，并远程擦除公司数据，并取消设备绑定。

编号	具体控制要求	客户关注点	华为云的应答
PR.DS-05 - 实施防止数据泄露的保护技术	**普通类** 1_O. 参照 ID.AM 类别，至少应界定： a. 数据访问所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 2_O. 应采用与风险评估一致的数据防泄漏（Data Loss Prevention）政策。 **关键类** 同普通类要求。 **战略类** 3_S. 应存在一份最新的详细文件，载明第 1_O. 项所述流程和政策。	客户应对数据访问所采用的安全政策。应采用与风险评估一致的数据防泄漏（Data Loss Prevention）政策。 对于战略类服务，客户应存在一份最新的详细文件，载明流程和政策。	华为云制定了数据安全策略及数据安全保护管理规定，对数据资产的分级分类标准进行了定义，同时明确了数据匿名化及标签化处理标准，对数据在整个生命周期中须遵循的安全措施进行了规范。华为云每年会对建立的数据安全管理相关规范和策略流程进行审计。 为配合客户满足合规要求，华为云向客户提供一系列数据存储服务，服务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，保证租户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。
PR.DS-06 - 采用数据完整性控制来验证软件、固件和信息的真实性	**普通类** 1_O. 参照 ID.AM 类别，至少应界定： a. 用于核验软件、固件和信息真实性的数据完整性控制机制清单； b. 为向资源分配控制机制以及明确何种机制适用于何种资源所采用的安全政策； c. 为遵守上述安全政策而采用的流程、方法和技术。 **关键类** 同普通类要求。 **战略类** 2_S. 应存在一份最新的详细文件，载明第 1_O. 项所述流程和政策。	客户应建立用于核验软件、固件和信息真实性的数据完整性控制机制清单，资源分配控制机制以及明确何种机制适用于何种资源所采用的安全政策。 对于战略类服务，应建立关于流程和政策的详细文件。	华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。 华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件安装、软件退出等环节，均实施严格的管控。
PR.DS-07 - 开发和测试环境与生产环境	**普通类** 1_O. 参照 ID.AM 类别，应界定： a. 用于实现环境分离的高	客户应将开发和测试环境与生产环境隔离。 对于战略类服务，应建	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

编号	具体控制要求	客户关注点	华为云的应答
隔离	层架构，以及在存在接触点时该分离如何实现； b. 为保证开发和测试环境与生产环境相分离所采用的安全政策； c. 为遵守上述安全政策而采用的流程、方法和技术。 **关键类** 同普通类要求。 **战略类** 2_S. 应存在一份最新的详细文件，载明第 1_O. 项所述流程和政策。	立关于流程和政策的详细文件。	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。 针对各环境交界处的分离实现，华为云也制定了变更管理程序，管理应用变更和基础设施变更。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。
信息保护流程与程序（PR.IP）：已实施并随时间推移不断调整的安全政策（涵盖指导方针、目标、范围、角色与职责、管理层的承诺以及各组织主体之间的协调），以及用于管理信息系统和资产保护的流程与程序。			
PR.IP-01 - 定义并管理 IT 与工业控制系统配置基线实践，并纳入安全原则	**普通类** 1_O. 应就应用安全制定相关政策和程序，以为应用安全功能的规划、实施和维护提供充分支持；该等政策和程序应至少每年审查并更新一次。[IaaS、SaaS]。 **关键类** 2_C. 应存在一份最新的详细文件，并至少结合 ID.AM 类别载明： a. 为开发 IT 系统配置并仅部署已批准配置而采用的安全政策； b. 已使用 IT 系统配置清单以及各自对应的基线要求； c. 为遵守上述安全政策而	客户应制定应用安全相关政策和程序，该等政策和程序应至少每年审查并更新一次。 对于关键类服务，客户应制定一份文件说明开发 IT 系统配置，IT 系统配置清单以及各自对应的基线要求，应用安全缓解与恢复流程等。	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。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、变更管理等环节，确保信息安全在信息系统安全生命周期中得到设计和实现。

编号	具体控制要求	客户关注点	华为云的应答
	采用的流程、方法和技术。[SaaS]。 3_C. 应界定并记录不同应用的基线安全要求。 4_C. 应界定并实施技术性指标，用于监测对既定安全要求和合规义务的遵守程度。 5_C. 应建立应用安全缓解与恢复流程，并在可能时实现漏洞修复自动化。 6_C. 应建立验证设备与操作系统和应用兼容性的流程。[PaaS、SaaS]。 7_C. 应建立与操作系统、补丁和/或应用有关变更的管理体系。[PaaS、SaaS]。 **战略类** 同关键类要求。		华为云对支撑业务运营的服务器操作系统、数据库管理系统及网络设备建立了统一的基线配置标准，以实现对服务基线配置的统一管理。此外，华为云构建了配置监控平台，实现对服务器异时，差异分析结果会通过邮件自动发送至巡检管理员进行后续跟进处理。此外，华为云会基于现有的防火墙配置策略与现网实施情况定期执行一致性审视，对识别出的差异项进行修复。 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。
PR.IP-02 - 实施系统生命周期管理流程	**普通类** 无要求。 **关键类** 1_C. 应实施关于云服务安全开发的指南以及技术/组织措施，并遵循 OWASP 关于软件开发安全（需求、设计、实现、测试和验证）的指导。已开展的 OWASP 测试报告应提供给国家网络安全局（ACN）和行政机构，并应保证不存在“高危”或“严重”级别漏洞。 **战略类** 同关键类要求。	对于关键类服务，应实施关于云服务安全开发的指南以及技术/组织措施，并遵循 OWASP 关于软件开发安全的内容。	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。 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。
PR.IP-03 - 已启用配置变更控制流程	**普通类** 1_O. 应界定： a. 对 IT 系统和工业控制系统配置更新以及对实际在用配置相对于预期配置的变更控制所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 2_O. 应实施一项程序，用于管理变更和配置过程中的例外情形，包括紧急情况。 3_O. 在发生错误或安全问题时，应界定并实施回滚计划。 **关键类** 同普通类要求。 **战略类** 4_S. 应存在一份最新的详细文件，载明第 1_O. 项所述流程和政策。	客户应建立IT 系统和工业控制系统配置变更控制流程。 对于战略类服务，应提供相关文件。	华为云制定了详细的文件化的变更管理程序，管理应用变更和基础设施变更。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。变更方案需要包括变更范围、备份方案、实施方案、回退方案、应急方案、验证方案，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。
PR.IP-04 - 执行、管理并验证信息备份	**普通类** 1_O. 至少还应结合 ID.AM 类别界定： a. 信息备份所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 2_Oa. 应定期对存储于云中的数据进行备份，并确保备份数据的保密性、完整性和可用性。 2_Ob. 应定期备份存储于云中的、用于完整恢复系统所必需的信息，包括行政机构数据以及恢复服务	客户应执行、管理并验证信息备份，定期备份存储于云中的、用于完整恢复系统所必需的信息。 对于关键类服务，应提供上述详细文档。	华为云已建立文件化的备份机制，会根据服务合同和业务连续性要求制定包括备份方式、位置、存储介质、保留期限、备份恢复程序等信息的备份策略，并每年开展一次备份恢复演练。 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（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，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到

编号	具体控制要求	客户关注点	华为云的应答
	所必需的数据，并确保备份数据的保密性、完整性和可用性。为此，还应保证至少包含一份备份副本的介质不会永久性地可从系统访问，以避免对该系统的攻击同时波及其全部备份副本。 3_O. 云服务的信息、软件和系统镜像的备份副本，应采用最先进的密码标准和行业最佳实践进行保护，并定期存档于远端站点（同时遵守 PR.DS 类别的要求）。如通过网络向远端站点传输备份，传输过程也必须采用最先进的密码标准和行业最佳实践予以保护。 4_O. 应定期验证备份副本恢复（restore test），并将其作为目标（SLO），至少每年一次。 **关键类** 5_C. 应存在一份最新的详细文件，并至少结合 ID.AM 类别载明： a. 信息备份所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 6_C. 应存在一份最新的详细文件，载明第 1_O. 项所述流程。 **战略类** 同关键类要求。		华为云，保证在灾难发生时数据不丢失，客户还可依赖华为云数据中心集群的多地域（ Region ）和多可用区 AZ 架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。 此外，华为云的专属加密满足租户更高合规性要求的加密场景，采用通过国家密码局认证或国际权威认证的硬件加密机，对租户业务进行 专属加密，默认双机架构以提高可靠性。 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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。
PR.IP-09 - 在事件/灾难情况下，响应	**普通类** 1_O. 应确定业务中断带来的影响及相关风险，以据此建立制定业务连续性策	客户应在事件/灾难情况下，建立相关流程或程序，保证响应与恢复计划处于有效并受管理	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IS0 22301认证。华为云每

编号	具体控制要求	客户关注点	华为云的应答
与恢复计划处于有效并受管理状态	略和能力的标准。 2_O. 应存在一份最新的详细文件，载明业务连续性计划以及事件响应计划，至少包括： a. 用于识别事件优先级的政策和流程； b. 计划实施阶段； c. 人员角色与职责； d. 沟通和报告流程； e. 与 CSIRT Italia 的衔接。 3_O. 应存在一份最新文件，列明已开展的教育、培训和演练活动。 4_O. 业务连续性计划应进行测试并向相关方通报。 5_O. 第 2_O. 项所述文件在行政机构提出要求时应予提供，并应定期审查。 **关键类** 6_C. 应存在一份最新的详细文件，说明云服务预期服务级别，以及在适用情况下热备份和/或冷备份以及灾难恢复站点的预期服务级别。 7_C. 应存在一份最新的详细文件，载明灾难恢复计划以及事故响应和恢复计划，至少包括： a. 用于识别事件优先级的政策和流程； b. 计划实施阶段； c. 人员角色与职责； d. 沟通和报告流程； e. 与 CSIRT Italia 的衔接。 8_C. 应存在一份最新文	状态。 对于关键类服务，客户应存在一份最新的详细文件，说明云服务预期服务级别，以及在适用情况下热备份和/或冷备份以及灾难恢复站点的预期服务级别。	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。 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。

编号	具体控制要求	客户关注点	华为云的应答
	件，列明已开展的教育、培训和演练活动。 9_C. 灾难恢复策略应进行测试并向相关方通报。 10_C. 对云服务运行具有关键意义的设备应具备冗余；如位于不同地点，则其间距离应符合行业最佳实践。 **战略类** 同关键类要求。		
PR.IP-12 - 制定并实施漏洞管理计划	**普通类** 1_O. 应存在一份最新的详细文件，至少载明： a. 为管理漏洞而采取的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 2_O. 应界定并实施相关程序和技术措施，用于更新检测工具、威胁特征和妥协指标；该等内容应频繁审查和更新，或至少每周更新一次。[SaaS]。 **关键类** 3_C. 应界定并实施技术措施，以识别使用第三方库或开源库应用的更新，并符合内部漏洞管理政策。 4_C. PR.IP-12 措施第 1_O. 项所述文件应每六个月更新一次。 **战略类** 同关键类要求。	客户应制定并实施漏洞管理计划。用于更新检测工具、威胁特征和妥协指标至少每周更新一次 对于关键类服务，应界定并实施技术措施，以识别使用第三方库或开源库应用的更新，并符合内部漏洞管理政策。漏洞文件应该每六个月更新一次。	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。华为云安全运营中心主动通过外部舆情、开源社区等外部渠道获取最新的漏洞信息，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。华为云使用态势感知分析系统，关联各种安全设备的告警日志并统一进行分析，快速识别已经发生的攻击、并预判尚未发生的威胁。
维护（PR.MA）：工业信息与控制系统的维护工作均按照现行政策和程序进行。			
PR.MA-01 - 使用受控且经授权	**普通类** 1_O. 至少还应结合维护类别界定：	客户应对资源和系统维护、修理活动进行记录，明确为遵守上述安	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、

编号	具体控制要求	客户关注点	华为云的应答
的工具执行并记录资源和系统的维护维修	a. 对资源和系统维护、修理活动进行记录所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 **关键类** 2_C. 应存在一份最新的详细文件，载明第 1_O. 项所述流程和政策。 3_C. 第 1_O. 项所述活动还应以核查安全方面为目的。 4_C. 软件更新仅允许来自预先授权的来源。 5_C. 与维护和更新活动有关的全部日志，均应在与被操作系统相分离且执行该等活动的用户无法访问的系统上生成并保存。 6_C. 应存在一份最新文件，至少说明用于实现第 3_C.、4_C. 和 5_C. 项的流程和技术工具。 **战略类** 7_S. 应建立一份最新的已执行维护和修理活动登记册。 8_S. 根据风险分析，对被认定为关键的软件更新，除出于安全原因具有需要迅速实施的正当情形外，均应在测试环境中验证后方可在生产环境中实际使用。 9_S. 与第 4_C. 项所述更新有关的目标代码应至少保存 24 个月。	全政策而采用的流程、方法和技术。 对于关键类服务，客户应存在一份流程和政策的详细文件。 客户的软件更新仅允许来自预先授权的来源，与维护和更新活动有关的全部日志，均应在与被操作系统相分离且执行该等活动的用户无法访问的系统上生成并保存。 对于战略类服务，客户应建立一份最新的已执行维护和修理活动登记册。	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。对于需要通过版本、补丁修复的漏洞，在安装之前进行安全测试验证。 华为云对内外部员工的终端资产实施集中管理包括，实施软件白名单对软件的安全和使用进行限制，同时采用数据防泄露、磁盘加密技术保护终端。

编号	具体控制要求	客户关注点	华为云的应答
PR.MA-02 - 资源和系统的远程维护经批准、留痕并以防止未授权访问的方式开展	**普通类** 1_O. 对资源和系统实施的远程维护，包括与安全功能相关的活动，应遵守 PR.AC-03 子类下的措施以及以下要求。 2_O. 所有由第三方人员实施的远程访问均必须经网络安全组织授权，并限于绝对必要的情形。 3_O. 应采用严格的保护机制，用于认证、身份识别和事件追踪。 4_O. 应采用特权账户管理和控制机制，包括时间限制以及可用管理功能的限制。 5_O. 与远程通信会话以及在远程访问系统上实施活动有关的全部日志，均应生成并保存于与被操作系统相分离且执行该等活动用户无法访问的系统中。 **关键类** 同普通类要求。 **战略类** 6_S. 应存在一份最新的详细文件，至少描述用于实现第 2_O.、3_O.、4_O. 和 5_O. 项的流程和技术工具。	客户应对资源和系统实施的远程维护，包括与安全功能相关的活动，所有由第三方人员实施的远程访问均必须经网络安全组织授权，并限于绝对必要的情形。 客户应采用严格的保护机制，用于认证、身份识别和事件追踪。 客户应采用特权账户管理和控制机制，包括时间限制以及可用管理功能的限制。 客户与远程通信会话以及在远程访问系统上实施活动有关的全部日志，均应生成并保存于与被操作系统相分离且执行该等活动用户无法访问的系统中。 对于战略类服务，客户应存在一份流程和政策的详细文件。	华为建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循和授予的。堡垒主机提供基于密码和邮箱验证码的双因素身份验证功能，以验证用户的身份。用户通过 互联网访问华为云办公子网，需要根据注册设备及其账号和密码进行双因素认证。华为云员工可以在 Cloud Scope 中进行逻辑访问管理， Cloud Scope 涵盖 Cloud Mnet System 、CBC 帐户中心、堡垒机、 FUXI 和 SVN 等多种支撑工具。支持工具涵盖本报告范围内所有产品的操作系统，包括但不限于虚拟服务器和基础设施设备的支持工具。在所有相关层的支持工具中的访问授权基于最小权限强制实施。高于最低权限的访问需要获得指定人的批准。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。 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。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

编号	具体控制要求	客户关注点	华为云的应答
			制列表来限制未信任网络的恶意接入。 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。
防护技术 (PR.PT)：安全技术解决方案的实施旨在确保系统和资产的安全性与韧性，并符合相关政策、程序和协议。			
PR.PT-01 - 已建立并实施用于定义、实施和审查系统日志的政策	**普通类** 1_O. 日志应以安全方式保存，最好集中保存，保存期限至少 24 个月。 2_O. 应界定： a. 系统日志管理所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术，尤其应关注日志的完整性和可用性。 **关键类** 同普通类要求。 **战略类** 3_S. 应存在一份最新的详细文件，载明第 2_O. 项所述流程和政策。	客户的系统日志应以安全方式保存，最好集中保存，保存期限至少 24 个月。同时应界定日志管理所采用的安全政策； 为遵守上述安全政策而采用的流程、方法和技术，尤其应关注日志的完整性和可用性。 战略类延用普通类要求，无特殊规定 对于战略类服务，客户应存在一份流程和政策的详细文件。	华为云建立并实施了文档化的日志管理政策和程序，为操作网络安全管理提供指导，华为云也建立了集中、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。 客户可以使用华为云的**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**云日志服务（Log Tank Service，简称LTS）**服务，用于收集来自主机和云服务的日志服务，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为客户提供实时、高效、安全的日志处理能力。华为云的云审计服务（CTS），可提供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

编号	具体控制要求	客户关注点	华为云的应答
			分析、合规审计、资源跟踪和问题定位等常见应用场景。 CTS最多可支持日志存储365天，如需存储根长时间，可将日志转储至OBS，实现长久存储。
PR.PT-04 - 通信网络和控制网络受到保护	**普通类** 1_O. 应配备边界防护系统，例如防火墙，包括应用层防火墙（含 Web 应用防火墙），并保持其更新、维护和正确配置。 **关键类** 2_C. 应配备入侵防御系统（IPS），并保持其更新、维护和正确配置。 3_C. 第 1_O. 项和第 2_C. 项所述技术工具应有助于符合 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的相关政策。 **战略类** 1_S. 应配备边界防护系统，例如防火墙，包括应用层防火墙（含 Web 应用防火墙），并保持其更新、维护和正确配置。 2_S. 应配备入侵防御系统（IPS），并保持其更新、维护和正确配置。 3_S. 第 1_O. 项和第 2_C. 项所述技术工具应有助于符合 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的相关政策。 4_S. 对第 1_O. 项和第 2_C. 项所述技术工具的更新、维护和配置，应遵守 PR.AC、PR.DS、PR.IP 和 PR.MA 类别下的政策。	客户应配备边界防护系统，例如防火墙，包括应用层防火墙（含 Web 应用防火墙），并保持其更新、维护和正确配置。 对于关键类服务，客户应配备入侵防御系统（IPS），并保持其更新、维护和正确配置。对于战略类服务，客户应配备边界防护系统，入侵防御系统（IPS），并保持其更新、维护和正确配置。应存在一份流程和政策的详细文件。	华为云建立了稳固、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；为了检测和拦截来自Internet的攻击以及租户虚拟网络之间的东西向攻击，华为云的网络中部署了网络IPS设备，包括但不限于面向公众的网络边界、安全区域信任边界、租户空间边界。华为云的IPS可以实时分析网络流量，触发对协议攻击、暴力破解、端口和漏洞扫描、病毒和木马攻击、针对特定漏洞的攻击等各种入侵的拦截。 此外，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 、 web shell 、 CC 等攻击实现实时的高性能防护。华为云 WAF 给用户提供简便的管理界面，用户可根据自身业务需要进行相关防护设置，亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。 更多信息可参考 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的回答。

编号	具体控制要求	客户关注点	华为云的应答
	5_S. 第 1_O. 项和第 2_C. 项所述技术工具还应服务于 DETECT（DE）功能的实现。 6_S. 应存在一份最新文件，至少说明用于实现第 1_O.、2_C.、3_C. 和 4_S. 项的流程和技术工具。		
PR.PT-05 - 实施相关机制，以满足正常和不利情况下的韧性要求	**普通类** 1_O. 就 PR.IP-09 子类所述计划而言： a. 应采用冗余的网络、连接和应用架构。 2_O. 应存在相关机制，以在遵守规定安全措施的前提下保障服务连续性。 3_O. 应界定： a. 与第 1_O. 项和第 2_O. 项有关的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 **关键类** 4_C. 就 PR.IP-09 子类所述计划而言： a. 应存在一处与风险分析相一致的灾难恢复站点。 **战略类** 5_S. 应存在一份最新的详细文件，载明第 2_O. 项所述流程和政策。	客户应采用冗余的网络、连接和应用架构，保证服务连续性。 对于关键类服务，客户应存在一处与风险分析相一致的灾难恢复站点。 对于战略类服务，客户应存在一份流程和政策的详细文件。	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。 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IS0 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

编号	具体控制要求	客户关注点	华为云的应答
			性进行测试。 客户可依赖华为云数据中心集群的多地域（ Region ）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

6.2.3检测

编号	具体控制要求	客户关注点	华为云的应答
异常与事件 (DE.AE)：系统会检测异常活动，并分析其潜在影响。			
DE.AE-03 - 从多个传感器和来源收集并关联事件信息	**普通类** 1_O. 为及时发现对云服务产生影响的事件，应采用技术和程序工具，以便： a. 从多个传感器和来源获取信息； b. 接收并收集由 CSIRT Italia 以及主体内部或外部来源披露的与云服务安全有关的信息； c. 对 a 项和 b 项所述数据和信息进行分析和关联（包括自动化分析），以便及时识别相关事件。 2_O. 上述分析和关联活动应受到监测并予以记录。与事件分析和调查活动有关的文档，包括电子文档，应至少保存 24 个月。 3_O. 明确规定： a. 用于识别第1_O条a项所述传感器和数据源的政	客户应采用技术和程序工具及时发现对云服务产生影响的事件。与事件分析和调查活动有关的文档，包括电子文档，应至少保存 24 个月。 客户应界定： a. 用于识别和分类相关事件的政策； b. 用于收集、分析和关联事件信息的流程、方法和技术。 对于关键类服务，客户应建立集中式存储库，保存主体用户的访问日志；该存储库应由主体直接管理，并在逻辑上与第三方可直接访问的系统相隔离。 对于战略类服务，客户应存在一份流程和政策的详细文件。	华为云PSIRT会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全 面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。 华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源ID(如：源IP、主机ID、用户ID

编号	具体控制要求	客户关注点	华为云的应答
	策； b. 用于获取第1_O条a项和b项所述信息的程序和技术工具； c. 用于进行第1_O条c项所述分析与关联的政策、流程及技术工具； d. 用于进行第2_O条所述监控与记录的流程及技术工具。 4_O. 应制定日志记录、监控、安全及访问日志保存的政策与程序，并至少每年更新一次。 5_O. 已采用审计系统，用于检测与安全相关的信息，以及监控未经授权的访问、数据或元数据的修改或删除。 6_O. 已制定并评估了用于报告监控系统异常和故障的流程、程序及技术措施，并能立即向负责人发出通知。 7_O.在云服务的日志记录与监控活动中，部署专用的错误管理与日志工具，并允许管理部门设定保留期限，以获取云服务的安全态势、数据完整性及功能运行状态等关键信息。采集的信息须详尽，以确保在适用场景下能够全面核查： a. 云服务中向用户提供的哪些数据、服务或功能被谁在何时访问过（审计日志）； b. 执行自动或手动操作过程中的故障； 8_O. 对于接受资质认证的服务，必须确保能够将日志集成到行政部门的管理和监控SIEM系统中，并且行政部门能够轻松导出		等)、事件类型、日期时间、受影响的数据/组件/资源的ID（如目的IP、主机ID、服务ID等）、成功或失败等信息，以助力支撑网络安全事件回溯。该日志分析系统有强大的数据保存及查询能力，使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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。

编号	具体控制要求	客户关注点	华为云的应答
	日志文件，最好是通过API实现。 **关键类** 9_C. 应建立集中式存储库，保存主体用户的访问日志；该存储库应由主体直接管理，并在逻辑上与第三方可直接访问的系统相隔离。 **战略类** 10_S. 应存在一份最新的详细文件，载明第 3_O. 项所述流程和政策。		
安全持续监控（DE.CM）：对信息系统和资产进行监控，以识别网络安全事件并验证防护措施的有效性。			
DE.CM-01 - 对网络进行监测以发现潜在网络安全事件	**普通类** 1_O. 应部署入侵检测系统（IDS）。 2_O. 应建立流程，用于监测与应用及其底层基础设施安全有关的事件。 3_O. 应建立访问监测系统，以发现可疑活动，并形成明确流程，以便针对发现的异常采取适当且及时的响应措施。 **关键类** 4_C. 应对进出流量、路由器和防火墙等边界系统活动、重要管理事件，以及对网络资源和终端工作站的成功或失败访问进行监测和关联分析，以识别网络安全事件。 5_C. 第 1_O.、2_O.、3_O. 和 4_C. 项所述技术工具，应按照 PR.AC、PR.DS、PR.IP 和 PR.MA 类别下的政策进行更新、维护和正确配置，并有助	客户应部署入侵检测系统（IDS）。建立流程，用于监测与应用及其底层基础设施安全有关的事件。 对于关键类服务，客户应对进出流量、路由器和防火墙等边界系统活动、重要管理事件，以及对网络资源和终端工作站的成功或失败访问进行监测和关联分析，以识别网络安全事件。	华为云部署了IDS/IPS实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。 华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户 数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联 （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。 在网络边界防护方面，华为云建立了稳固、完善的边界和多层立体的安全防护系统，部署了Anti-DDoS、IDS/IPS、WAF等防护机制。Anti-DDoS快速发现和防护DDoS攻击，实时对流量型攻击和应用层攻击进行全面防护；WAF实时检测和防御Web攻击，对高危攻击进行告警并立刻自动阻

编号	具体控制要求	客户关注点	华为云的应答
	于符合 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的政策。 6_C. 第1_O、2_O、3_O和4_C条所述的技术工具也用于DE.AE类所述的目的。 7_C. 存在一份最新的文件，其中至少描述了： a. 针对第1_O、2_O、3_O和4_C条所采取的安全政策； b. 用于确保遵守安全政策的流程、方法和技术。 **战略类** 同关键类要求。		断。 华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源ID、事件类型、日期时间、受影响的数据/组件/资源的ID、成功或失败等信息，以助力支撑网络安全事件回溯。
DE.CM-04 - 检测恶意代码	**普通类** 1_O. 应实施并使用专门的恶意软件防范和检测工具，以及终端保护系统（EPS）。 2_O. 应建立反恶意软件保护政策，并至少每年审查一次。 **关键类** 3_C. 应在所有设备上配置专门的软件防火墙。 4_C. 对输入文件（包括通过电子邮件、下载、可移动介质等进入的文件）应进行分析，包括通过沙箱方式分析。 5_C. 第 1_O.、3_C. 和 4_C. 项所述技术工具，应按照 PR.AC、PR.DS、PR.IP 和 PR.MA 类别下的政策进行更新、维护和正确配置，并有助于符合 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的政策。	客户应实施并使用专门的恶意软件防范和检测工具，以及终端保护系统（EPS），建立反恶意软件保护政策，并至少每年审查一次。 对于关键类服务，应在所有设备上配置专门的软件防火墙。对输入文件进行分析	华为云通过防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能，并且华为云终端设备均安装数据防泄漏（DLP）软件、浏览器和电子邮件安全管控措施。 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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。

编号	具体控制要求	客户关注点	华为云的应答
	6_C. 应存在一份最新文件，至少说明： a. 与第 1_O.、3_C. 和 4_C. 项有关所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。 **战略类** 同关键类要求。		
DE.CM-07 - 开展监测以发现未授权人员、连接、设备或软件	**普通类** 无要求。 **关键类** 1_C. 参照 PR.AC-03 子类，应能够检测对资源具有潜在未经授权物理或远程访问能力的人员。为此，应部署监控和访问控制系统，包括自动化系统。 2_C. 参照 ID.AM-01 子类，应能够检测未获批准的设备，包括物理设备。为此，在不违背已记录技术限制的前提下，至少应部署网络访问控制系统。 3_C. 第 1_C. 项和第 2_C. 项所述技术工具，应按照 PR.AC、PR.DS、PR.IP 和 PR.MA 类别下的政策进行更新、维护和正确配置，并有助于符合 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的政策。 4_C. 应存在一份最新文件，至少说明： a. 与第 1_C. 项和第 2_C. 项有关所采用的安全政策；	对于关键类/战略类服务，参考PR.AC-03、ID.AM-01、PR.AC、PR.DS、PR.IP 和 PR.MID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS要求。	参考 PR.AC-03 、 ID.AM-01 、 PR.AC 、 PR.DS 、 PR.IP 和 PR.MID.AM 、 ID.GV 、 ID.SC 、 PR.AC 和 PR.DS回答。 客户除了通过**统一身份认证服务（ Identity and Access Management ，简称IAM ）**，对远程接入人员的身份和权限进行管理外，华为云还提供了加密传输的方式供客户自行选择，比如VPN、HTTPS等。 同时，对于华为云内部系统的远程访问仅可以通过堡垒机和SVN的方式。华为云统一管理堡垒机和SVN的权限，对华为云运维人员进行身份认证，并且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。 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。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。

编号	具体控制要求	客户关注点	华为云的应答
	b. 为遵守上述安全政策而采用的流程、方法和技术。 **战略类** 5_S. 参照 ID.AM-02 子类，在不违背已记录技术限制的前提下，应部署用于检测未获批准软件的控制系统。 6_S. 参照 ID.AM-03 子类，应部署用于检测未经授权连接的控制系统。 7_S. 第 5_S. 项和第 6_S. 项所述技术工具，应按照 PR.AC、PR.DS、PR.IP 和 PR.MA 类别下的政策进行更新、维护和正确配置，并有助于符合 ID.AM、ID.GV、ID.SC、PR.AC 和 PR.DS 类别下的政策。 8_S. 应存在一份最新文件，至少说明： a. 与第 5_S. 项和第 6_S. 项有关所采用的安全政策； b. 为遵守上述安全政策而采用的流程、方法和技术。		华为云通过实施网络准入控制措施和远程访问限制，以限制设备的网络接入，以及未经授权的连接或者与越权操作。
DE.CM-08 - 开展扫描以识别漏洞	**普通类** 1_O. 根据风险分析，应在被视为关键的平台和软件应用投入运行前，对其开展渗透测试和漏洞评估。 **关键类** 1_C. 根据风险分析，应在被视为关键的平台和软件应用投入运行前，对其开展渗透测试和漏洞评估。 2_C. 应根据第 1_O. 项所	客户应在被视为关键的平台和软件应用投入运行前，对其开展渗透测试和漏洞评估。 对于关键类服务，应在被视为关键的平台和软件应用投入运行前，对其开展渗透测试和漏洞评估。建立一份最新登记册，记录已实施的渗透测试和漏洞评估及其相关文档。	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。 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

编号	具体控制要求	客户关注点	华为云的应答
	述平台和软件应用的关键程度，定期开展渗透测试和漏洞评估。 3_C. 应存在一份最新文件，载明拟开展的渗透测试和漏洞评估类型。 4_C. 应建立一份最新登记册，记录已实施的渗透测试和漏洞评估及其相关文档。 **战略类** 同关键类要求。		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。
检测流程（DE.DP）：已制定、维护并验证了监测流程和程序，以确保对异常风况的理解。			
DE.DP-01 - 为监测流程明确角色与职责，以确保可问责性	**普通类** 1_O. ID.AM-06 子类所述任命事项应在主体内部予以告知。 2_O. 对于发现影响云服务事件的前置活动，其角色、流程和职责应清晰界定，并向主体相关部门公开。 3_O. 应存在一份最新的详细文件，至少载明： a. 第 2_O. 项所述角色、流程和职责； b. 第 1_O. 项和第 2_O. 项所述任命、角色和流程的传达流程。 4_O. 应界定并实施一套制度，用于基于事先约定的指标，向行政机构通报涉及应用和底层基础设施的异常事件。[PaaS、SaaS]。 **关键类** 同普通类要求。 **战略类**	客户应为监测流程明确角色与职责，以确保可问责性。	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。 华为云制定了突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。华为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。

编号	具体控制要求	客户关注点	华为云的应答
	同关键类要求。		

6.2.4响应

编号	具体控制要求	客户关注点	华为云的应答
响应规划（RS.RP）：执行并维护响应程序和流程，以确保对已发现的网络安全事件作出响应。			
RS.RP-01 - 已建立响应计划，并在事件期间或之后执行	**普通类** 1_O. 响应计划应规定：对通过 DETECT（DE）类别下分析和关联活动发现的事件进行及时评估，并将结果立即传达给主体相关部门；同时，还应服务于向行政机构以及在自愿基础上向 CSIRT Italia 通报影响云服务的事件。 **关键类** 2_C. 用于及时管理安全事件的政策和程序应至少每年审查一次。 3_C. 响应计划以及第 1_O. 项和第 2_C. 项所述政策和程序，应涵盖关键内部部门、受到影响的行政机构以及所有相关第三方。 4_C. 事件响应计划应按计划周期进行测试和更新，或在组织或环境发生重大变化时更新。 5_C. 应界定并监测重大网络安全事件的指标。 6_C. 应界定并实施支持业务流程的流程、程序和措施，以开展安全事件分级处置（triage）。 7_C. 应建立一支计算机应急响应团队（CERT），按照 ISO/IEC 27035-2 指	客户应建立响应计划，并在事件期间或之后执行。 对于关键类服务，事件管理程序应每年审查一次，范围涵盖关键内部部门、受到影响的行政机构以及所有相关第三方。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。根据内部管理的要求，华为云每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。 华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。

编号	具体控制要求	客户关注点	华为云的应答
	南协调事件解决阶段；在与服务有关的情况下，还应安排行政机构定期参与。 **战略类** 同关键类要求。		
通信（RS.CO）：应对工作需与内部及外部各方进行协调（例如，可能需要法律机构或执法部门提供支持）。			
RS.CO-01 - 人员知悉在需要事件响应时其角色及应执行的操作	**普通类** 1_O. 用于开展事件响应各阶段和流程的角色与职责应清晰界定，并向主体相关部门公开。 2_O. 应定期开展演练。 3_O. 应存在一份最新的详细文件，至少载明： a. 开展事件响应阶段、流程、角色和职责； b. 开展事件响应阶段、流程、角色和职责的传达流程； c. 定期演练的实施方式。 4_O. 主体应在事件被记录并分类后 1 小时内，将事件或数据泄露情况通知行政机构。 **关键类** 5_C. 应建立一份最新登记册，记录已实施的演练、参与人员以及相关经验教训。 6_C. 应建立关于安全事件、电子取证（E-Discovery）和云取证（Cloud Forensics）管理的政策和程序，并至少每年审查和更新一次。 7_C. 应界定并实施关于安全违规通知的流程、程序	客户应确保人员知悉在需要事件响应时其角色及应执行的操作。应在事件被记录并分类后将事件或数据泄露情况通知行政机构。 对于关键类服务，应建立一份最新登记册，记录已实施的演练、参与人员以及相关经验教训。 关于安全事件、电子取证（E-Discovery）和云取证（Cloud Forensics）管理的政策和程序，并至少每年审查和更新一次。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。根据内部管理的要求，华为云每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。 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。 华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批。 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。 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

编号	具体控制要求	客户关注点	华为云的应答
	和技术措施。 8_C. 对每一次实际或疑似安全违规，包括涉及供应链的违规，都应建立通报机制，并符合适用的SLA、法律和法规。 9_C. 事件发生后的响应活动应向内部和外部相关方通报，包括组织管理人员和高层管理者。尤其是，事件后的恢复活动应向相关内部和外部方通报。 **战略类** 同关键类要求。		的有效性。
RS.CO-05 - 实施与外部相关方的自愿信息共享，以提升态势感知	**普通类** 1_O. 应界定并维护与云及网络安全相关利益群体以及与主体情境相符的其他相关主体之间的联系。 2_O. 应界定并维护与适用监管机构、国家和地方执法机关及其他法定管辖机关之间的联络点。 **关键类** 同普通类要求。 **战略类** 同关键类要求。	/	华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的沟通与交流。
分析（RS.AN）：开展分析工作，以确保对恢复工作提供有效的响应和支持。			
RS.AN-05 - 已定义流程，用于接收、分析并响应来自内部或外部来源的漏洞信息	**普通类** 1_O. DE.AE-3 子类所述评估结果，以及 DE.CM-08 子类所述渗透测试和漏洞评估结果，应传达至主体相关部门。 2_O. 应监测以下沟通渠道：依据 2019 年 8 月 8 日总理令第 4 条设立的 CSIRT Italia 渠道、主体所属行业主管机关渠道，	客户关于渗透测试和漏洞评估结果，应以文件形式记录并在需要时传达至主体相关部门。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。根据内部管理的要求，华为云每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。 华为云制定安全事件的定级原则和升级原则，根据安全事件对客

编号	具体控制要求	客户关注点	华为云的应答
	以及相关 CERT 和信息共享与分析中心（ISAC）渠道。 3_O. 应存在一份最新文件，至少描述： a. 接收、分析并响应至少通过第 1_O. 项和第 2_O. 项活动收集的信息的方法； b. 用于开展第 1_O. 项和第 2_O. 项活动的流程、角色、职责和技术工具。 **关键类** 同普通类要求。 **战略类** 同关键类要求。		户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。
缓解（RS.MI）：采取行动以防止安全事件扩大，减轻其影响并解决该事件。			
RS.MI-03 - 对新漏洞进行缓解，或将其记录为已接受风险	**普通类** 1_O. 应按照漏洞管理计划（PR.IP12）对漏洞进行缓解；如未予缓解，则应对由此产生的剩余风险进行记录并予以接受。 **关键类** 1_C. 应按照漏洞管理计划（PR.IP12）对漏洞进行缓解；如未予缓解，则应对由此产生的剩余风险进行记录并予以接受。 2_C. 应根据风险，界定并实施相关程序和技术措施，以便在识别出漏洞时采取响应行动，包括计划内行动和紧急行动。 **战略类** 同关键类要求。	客户应建立漏洞管理计划对漏洞进行缓解，如未予缓解，则应对由此产生的剩余风险进行记录并予以接受。 对于关键类服务，应根据风险，界定并实施相关程序和技术措施，以便在识别出漏洞时采取响应行动，包括计划内行动和紧急行动。	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。

6.2.5恢复

编号	具体控制要求	客户关注点	华为云的应答
恢复计划（RC.RP）：实施并维护恢复流程和程序，以确保在发生网络安全事件后，能够恢复受影响的系统或资产。			
RC.RP-01 - 已建立恢复计划，并在网络安全事件期间或之后执行	**普通类** 1_O. 应存在一项恢复计划，至少规定在网络安全事件影响云服务时恢复其正常运行所必需的流程和程序。 **关键类** 2_C. 恢复计划应每六个月测试一次，并作为每年两次演练的一部分实施。 **战略类** 同关键类要求。	客户应建立恢复计划，并在网络安全事件期间或之后执行。 对于关键类服务，恢复计划应每六个月测试一次，并作为每年两次演练的一部分实施。	客户可依赖华为云数据中心集群的多地域（ Region ）和多可用区 AZ ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。 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。
通信（RC.CO）：事故发生后的恢复工作需与内部及外部各方（例如受害者、互联网服务提供商、受攻击系统的所有者、供应商、CERT/CSIRT）进行协调。			
RC.CO-03 - 事件后开展的恢复活动会向内部和外部相关方（包括管理层和高层）通报	**普通类** 无要求。 **关键类** 1_C. 事件发生后的恢复活动，应通报给相关的内部和外部方（例如受害方、互联网服务提供商、被攻击系统所有者、供应商以及 CERT/CSIRT）。 **战略类** 同关键类要求。	对于关键类服务，事件发生后的恢复活动，应通报给相关的内部和外部方。	为配合客户符合监管要求，华为云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。
改进（RC.IM）：恢复计划及相关流程已得到改进，并吸取了经验教训以指导未来的工作。			
RC.IM-02 - 恢复策略得到更新	**普通类** 无要求。 **关键类** 同 普通类要求。 **战略类**	客户应保持云恢复计划最新并总结吸取已发生恢复活动中的经验教训。	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

编号	具体控制要求	客户关注点	华为云的应答
	1_S. RC.RP-01（恢复计划）所述计划应保持最新状态，并应考虑已发生恢复活动中的经验教训。		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。 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。 华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息 安全事件的进展、处置措施与落实，对事件处置后的影响进行分 析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回 溯，并形成事件报告总结经验教训，在报告中告知事件的描述、 起因、影响、华为云已采取的措施等内容。此外，华为云每年对 高风险事件处理过程进行回顾，以确保高风险事件的处理过程满 足公司实际的业务需求。

7 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，以满足等保合规的要求。	资产管理 漏洞管理 入侵检测
数据库安全服务 Database Security	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，	安全审计

Service (DBSS)	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。	
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

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，并对加密	数据备份

Volume Backup Service (VBS)	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

8 结语

华为云致力于为意大利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，有助于云用户详细了解华为云对于意大利网络安全监管要求的遵从性，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、构建和部署符合意大利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。

9 版本历史

日期	版本	描述
2026 年 5 月	1.0	首次发布

