华为云 CSA CCM 合规性说明（CSA CAIQ v3.1）

文档版本 01

发布日期 2020-09-30

华为技术有限公司

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 概述

1.1 适用范围

本文档提供的信息适用于华为云在国际站上开放的产品和服务。

1.2 发布目的

云安全联盟发布的云控制矩阵（Cloud Security Alliance Cloud Control Matrix，简称CSA CCM）作为针对于云安全的控制框架，融合了先进的标准、法规与最佳实践，用于帮助云服务提供商以及云客户提升云上安全性。

华为云已经获得了基于CSA CCM的云安全认证——CSA STAR金牌证书，并希望在本材料中借由CAIQ自评估表的形式，向客户展示华为云为提升云环境上的安全性所做出的努力，帮助其了解：

- CSA CCM的主要内容、相关的认证及CAIQ的作用；
- 华为云针对于CAIQ自评估表的问题所作出的回应。

1.3 基本定义

- **客户（租户）：** 指与华为云达成商业关系的注册用户，在本文中同租户含义一致，即使用华为云云服务的用户组织。
- **云安全联盟（Cloud Security Alliance）：** 世界领先的组织，致力于定义和提高最佳实践的认识，以帮助确保一个安全的云计算环境。
- **英国标准协会（BSI）：** 国际知名的标准认证机构，为全球的机构及个人提供标准认证、培训服务。
- **CSA CCM：** 即云安全联盟云控制矩阵（以下简称CCM），是世界上唯一的特定于云的安全控制元框架，框架映射到与安全、隐私等相关的领先的标准、最佳实践和法规。

- **CSA CAIQ：**即共识评估计划问卷（以下简称CAIQ），提供一种业界接受的方式来记录IaaS、PaaS和SaaS服务中存在哪些安全控制，从而提供安全控制透明性。它提供了一组云消费者和云审计人员可能希望向云服务提供商询问的Yes/No问题，以确定它们是否符合云控制矩阵(CSA CCM)。
- **CSA STAR认证：**由云安全联盟与英国标准协会BSI联合推出的针对云安全水平的权威认证，其中STAR是Security（安全）、Trust（可信）、Assurance（保证）和Risk（风险）的缩写。该认证基于CSA CCM以及ISO 27001的要求进行评估审核。
- **ISO 27001信息安全管理体系：**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 27002是基于ISO 27001的最佳实践。
- **ISO 27017 云服务信息安全管理体系：**基于ISO 27001体系框架与ISO 27002最佳实践的云服务信息安全控制的实用规则，是云服务信息安全控制的实施规程的国际标准。
- **ISO 27701 隐私信息管理体系：**对ISO 27001和 ISO 27002的隐私扩展，是隐私管理领域的权威国际标准。标准提出建立、实施、维护和持续改进隐私信息管理系统及其相关内容的要求与指引。
- **ISO 22301 业务连续性管理体系：**国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的业务连续性计划，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
- **SOC审计报告：**由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
- **PCI DSS认证：** 由VISA、JCB和万事达等五家国际信用卡组织共同建立的支付卡行业安全标准协会发布的一套支付卡行业数据安全标准，关于华为云的PCI DSS认证内容，请参考《华为云PCI DSS实践指南》。
- **PCI 3DS认证：**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。
- **NIST网络安全框架：**NIST网络安全框架由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
- **M&O认证：**Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。

2 CSA CCM 简介

2.1 CSA CCM 的框架与主要内容

CSA CCM是由国际领先的云安全组织——云安全联盟发布的云上安全指南。云安全联盟在2009年成立，致力于国际云计算安全的全面发展。目前云安全联盟已协助美国、欧盟、日本、澳大利亚、新加坡等多国政府开展国家网络安全战略、国家身份战略、国家云计算战略、国家云安全标准、政府云安全框架、安全技术研究等工作。

CCM结构包含控制域、控制措施、对于每个控制措施对应的架构内容、公司治理的相关性、涉及的云服务类型、与云服务供应商和客户的相关性以及同42个标准、法规、最佳实践的映射关系。如下图所示，CCM中共囊括了16个控制领域，共计133个控制措施，覆盖了云安全中相关的常用控制措施。

控制 ID	控制领域
AIS	1. 应用与接口安全
AAC	2. 审计保证与合规
BCR	3. 业务连续性管理与业务弹性
CCC	4. 变更控制和配置管理
DSI	5. 数据安全与信息生命周期管理
DCS	6. 数据中心安全
EKM	7. 加密与密钥管理
GRM	8. 治理和风险管理
HRS	9. 人力资源
IAM	10. 标识和访问管理

控制 ID	控制领域
IVS	11. 基础设施和虚拟化安全
IPY	12. 互操作性和可移植性
MOS	13. 移动安全
SEF	14. 安全事件管理，电子发现和云取证
STA	15. 供应链管理，透明度和问责制
TVM	16. 威胁与漏洞管理

2.2 CSA CCM 与 CAIQ、STAR 认证的关系

云安全的管控由外部第三方的独立评估以及云服务供应商的内部持续管理组成。

基于CCM与ISO 27001，云安全联盟与英国标准协会合作开发了CSA STAR云安全评估认证，通过评估云服务供应商对CCM与ISO 27001要求的控制措施的落实情况进行认证评级，评级结果存在金牌、银牌或铜牌三个等级。

云安全联盟根据CSA CCM推出了供云服务供应商评估自身控制水平的CAIQ共识评估计划问卷，问卷的控制领域和控制措施与CCM保持一致，但是将每个控制措施细分为多个可回答的问题，总共330项问题。云服务供应商可以使用CAIQ进行自评估，并利用其对自身的控制水平持续管理。

本材料第3章将展示华为云对于CAIQ的回应，帮助客户了解华为云在强化自身云安全水平以及提升云内安全性所做出的努力。本材料中使用的CAIQ版本为2020年最新发布的3.1版。

2.3 华为云的认证情况

华为云凭借自身的信息安全体系及安全控制措施管理，已获得CSA STAR的最高级别认证——CSA STAR金牌认证。评估范围涵括华为云在其官网发布的数十种产品及服务，以及遍布全球多地的数据中心。

2020年STAR认证覆盖的华为云产品及服务（具体上线区域需参见华为云官网）如下表，也可在华为云信任中心下载华为云的CSA STAR证书作为参考。

产品类型	覆盖产品
计算	弹性云服务器（ECS）、裸金属服务器（BMS）、云手机（CPH）、专属主机（DeH）、弹性伸缩（AS）、镜像服务（IMS）、GPU加速云服务器（GACS）、FPGA加速云服务器（FACS）
存储	对象存储服务（OBS）、云硬盘（EVS）、云备份（CBR）、专属企业存储服务（DESS）、专属分布式存储服务（DSS）、云硬盘备份（VBS）、云服务器备份（CSBS）、存储容灾服务（SDRS）、弹性文件服务（SFS）、数据快递服务（DES）、云存储网关（CSG）

产品类型	覆盖产品
网络	虚拟私有云（VPC）、弹性负载均衡（ELB）、NAT网关（NAT）、弹性公网IP（EIP）、云专线（DC）、虚拟专用网络（VPN）、云连接（CC）、VPC终端节点（VPCEP）
数据库	文档数据库服务（DDS）、分布式数据库中间件（DDM）、数据管理服务（DAS）、数据复制服务（DRS）、云数据库MySQL(MySQL)、云数据库PostgreSQL（PostgreSQL）、云数据库SQL Server（SQL Server）、云数据库GaussDB（for MySQL）（GaussDB for MySQL）、云数据库GeminiDB（GeminiDB）
容器服务	云容器引擎（CCE）、云容器实例（CCI）
视频	视频直播（Live）、视频点播（VOD）、媒体转码（MPC）、短视频（SVideo）
应用中间件	分布式缓存服务Redis（DCS）、分布式缓存服务Memcached（DCSMEM）、分布式消息服务DMS（DMS）、分布式消息服务Kafka（Kafka）、分布式消息队列RabbitMQ（RabbitMQ）、API网关（APIG）、应用管理与运维平台（ServiceStage）
管理工具	应用运维管理（AOM）、应用性能管理（APM）、云日志服务（LTS）、统一身份认证服务（IAM）、云监控服务（CES）、消息通知服务（SMN）、云审计服务（CTS）
域名和网站	域名注册服务（Domains）、云速建站（Cloudsite）、云解析服务（DNS）
迁移	对象存储迁移服务（OMS）、云数据迁移（CDM）
智能云提速	内容分发网络（CDN）
软件开发平台	代码托管（CodeHub）、代码检查（CodeCheck）、编译构建（CloudBuild）、项目管理（ProjectMan）、CloudIDE
安全	企业主机安全（HSS）、容器安全服务（CGS）、Web应用防火墙（WAF）、漏洞扫描服务（VSS）、Anti-DDos流量清洗（Anti-DDos）、DDoS高防（AAD）、数据库安全服务（DBSS）、数据加密服务（DEW）、态势感知（SA）、SSL证书管理（SCM）、安全专家服务（SES）、云堡垒机（CBH）
企业应用	区块链服务（BCS）、全栈专属服务（FCS）、语音通话（VoiceCall）、隐私保护通话（PrivateNumber）、消息&短信（MSG&SMS）、应用与数据集成平台（ROMA）、SD-WAN云服务（SD-WAN）、云管理网络（CMN）、华为云Welink（Welink）、会议（Meeting）、专属计算集群服务（DCC）
IoT物联网平台	设备接入（IoTDA）、设备发放（IoTDP）、全球SIM联接（GSL）、IoT数据分析（IoTA）、IoT边缘（IoTEdge）、车联网服务（IoV）、园区物联网服务（IoTC）、道路感知服务（RPS）

产品类型	覆盖产品
EI企业智能	数据搜索服务（ImageSearch）、AI开发平台（ModelArts）、华为HiLens（HiLens）、图引擎服务（GES）、视频接入服务（VIS）、云搜索服务（CSS）、自然语言处理基础（NLPF）、语言理解（Language Understanding）、语言生成（Language Generation）、定制自然语言处理（NLPC）、机器翻译（MT）、MapReduce服务（MRS）、实时流计算服务（CS）、数据湖探索（DLI）、数据仓库服务（DWS）、表格存储服务（CloudTable）、数据接入服务（DIS）、只能数据湖运营平台（DAYU）、数据可视化（DLV）、推荐系统（RES）、文字识别（OCR）、内容审核（Moderation）、内容审核-文本（Moderation（Text））、内容审核-图像（Moderation（Image））、内容审核-视频（VCM）、人脸识别服务（FRS）、图像标签（Image Tagging）、名人识别（ROC）、智能问答机器人（QABot）、任务型对话机器人（TaskBot）、智能质检（CBSSA）、定制化对话机器人（CBSC）、实时语音转写（Real-time ASR）、云隐识别（ASR）、语音合成（TTS）、定制语音识别（ASRC）、视频内容分析（VCR）、视频编辑（VCP）、视频标签（VCT）、视频指纹（VEP）、交通智能体（TrafficGo）、园区智能体（CampusGo）、供热智能体（HeatingGo）、医疗智能体（EIHealth）、工业智能体（EI_Industrial）、网络智能体（NAIE）

3 华为云 CSA CAIQ 评估表

3.1 AIS 应用程序和接口安全

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	

AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/ Software Development Lifecycle (SDLC)?	X			华为云推行快速迭代的全新DevOps流程，将华为云的安全生命周期SDL嵌入DevOps逐步形成高度自动化的DevSecOps全新安全生命周期管理流程，以及确保全新流程顺利而灵活执行的云安全工程能力和工具链。
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			华为云引入了静态代码扫描工具对代码进行每日检查，检查结果进入云服务持续集成和持续部署工具链，通过质量门限进行控制，以评估云服务产品的质量。 更多详细信息请查阅《华为云安全白皮书》。
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?		X		华为云不使用手动源代码分析，自动代码分析工具作为华为云软件开发生命周期的一部分运行。
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			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、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。在使用中，须将第三方软件作为服务或解决方案的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或解决方案中使用独立的第三方软件是否引入新的安全问题。
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			所有华为云产品与服务在发布前均需完成静态代码扫描，扫描出的漏洞告警清零才可进行发布，有效降低应用程序存在编码相关的安全问题的可能性。

AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			华为云会在提供服务之前和客户签订《华为云用户协议》、《隐私政策声明》、《可接受的使用政策》、《服务协议》、《云服务等级协议（SLA）》等，这些协议概述了服务要求的细则及双方的责任。
AIS-02.2	Are all requirements and trust levels for customers’ access defined and documented?	X			华为云会在提供服务之前和客户签订《华为云用户协议》、《隐私政策声明》、《可接受的使用政策》、《服务协议》、《云服务等级协议（SLA）》等，这些协议概述了服务要求的细则及双方的责任。
AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			数据完整性控制如SOC报告中所述，华为云制定了在数据生命周期所有阶段（包括传输、存储和处理）中维护数据的完整性控制的策略与程序，并定期依赖内部与外部审核来验证其有效性。 对于内容数据的完整性验证，客户需负责对华为云环境中使用的应用程序接口和数据库相关的数据输入输出校验控制的实现。
AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			数据完整性控制如SOC报告中所述，华为云制定了在数据生命周期所有阶段（包括传输、存储和处理）中维护数据的完整性控制的策略与程序，如存储前和存储后通过Hash校验数据一致性，确保存入数据是上传数据，并定期通过内部与外部审核来验证其有效性。 对于内容数据的完整性验证，客户需负责对华为云环境中使用的应用程序接口和数据库相关的数据输入输出校验控制的实现。

AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			华为云遵循数据安全管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为用户提供最切实有效的数据保护能力，保证租户对其数据的隐私权、所有权和控制权不受侵犯。 更多详细信息请查阅《华为云安全白皮书》。

3.2 AAC 审计保障与合规性

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			华为云建立了一个正式的、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。
AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?	X			华为云的正式、定期的审计计划中包含安全操作实施的有效性。定期评审的标准例如ISO 27001、CSA STAR认证、PCI DSS认证、SOC报告等也会对华为云的安全实施进行评审。
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			客户可以在华为云信任中心申请下载最新的包含ISO27001、SOC在内的多种合规资质证书及报告，租户在下载此类资源之前需先同意华为云保密承诺函。
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			华为云每半年都会组织内部以及外部具有一定资质的第三方进行对华为云的所有的系统及应用进行渗透测试，并对渗透测试的结果进行跟进与整改。

AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			依据PCI DSS的最佳实践，华为云每半年都会组织内部以及外部具有一定资质的第三方进行对华为云的所有的系统及应用进行渗透测试，并对渗透测试的结果进行跟进与整改。
AAC-02.4	Do you conduct internal audits at least annually?	X			华为云建立了一个正式的、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。 同时，华为云通过了ISO27001的认证，符合认证对于每年进行内部审计的要求，且每年通过第三方机构对符合性进行确认。
AAC-02.5	Do you conduct independent audits at least annually?	X			华为云建立了一个正式的、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。 华为云每年会基于美国注册会计师协会AICPA的标准进行审计并发布相关的SOC报告、以及多项标准的年度评审工作。
AAC-02.6	Are the results of the penetration tests available to tenants at their request?		X		虽然华为云定期进行渗透测试，并有专门的团队跟进测试结果。渗透测试报告及跟进情况会通过内部审计以及外部认证机构核查，但该项报告并不向租户提供。
AAC-02.7	Are the results of internal and external audits available to tenants at their request?	X			华为云为租户提供第三方审计机构根据美国注册会计师协会AICPA的相关准则出具的SOC审计报告。租户可以在华为云信任中心申请下载SOC审计报告，下载前需同意华为云保密承诺函。

AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			华为云设立了专岗同外部各方保持积极的联系，以监控法律、法规的相关要求。当发布新的、与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律法规要求的符合性。

3.3 BCR 业务连续性管理与运营恢复

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			目前，华为云已经通过ISO22301业务连续性管理体系标准的认证，在内部建立了业务连续性管理体系，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。
BCR-01.2	Do you have more than one provider for each service you depend on?	X			华为云的灾备策略中规定对于同一服务需使用多家供应商以应对突发事件，以此保留一定的冗余性维持服务的连续性。
BCR-01.3	Do you provide a disaster recovery capability?	X			华为云为客户提供存储容灾服务SDRS，可帮助客户在容灾站点迅速恢复业务，缩短业务中断时间。该服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	X			华为云的灾备策略中规定对于同一服务需使用多家供应商，当监控发现程序故障时，将判断上游提供商的服务连续性，若上游提供商服务中断，及时切换到其他服务供应商。
BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?		X		华为云不会向租户提供操作冗余报告。但华为云定期进行ISO 22301、ISO 27001等认证的外部第三方审计，对容灾冗余的控制进行检查，华为云内部定期测试冗余机制的有效性。
BCR-01.6	Do you provide a tenant-triggered failover option?	X			华为云提供的存储容灾服务SDRS提供一键容灾切换，在事件发生或需要时，将业务切换到容灾站点，避免因事件导致的业务中断。
BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?		X		华为云不会向租户提供业务连续性报告。但华为云每年均会进行ISO27001等认证的外部第三方审计对业务连续性计划进行评估，并在内部对业务连续性水平进行测试以维持其有效性。
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			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。
BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			华为云严格遵循ISO27001信息安全管理体系中关于设备的条款A11.2要求，采取控制措施防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断，并每年对此要求的落实进行审计。

BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			华为云实施了备份与冗余策略，包括内部、内外部、外部岗位互备，同城及异地多地办公场所，冗余设备及备件，采用多家人力、设备、服务供应商以及开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			华为云依据ISO27001信息安全管理体系、ISO27017云计算信息安全管理体系、ISO27701隐私信息管理体系等国际标准建立了信息系统相关文档，经授权员工皆可访问相应的文档。
BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			在物理保护方面，华为云设立了分区防护；对于可能的自然灾害制定了选址策略以消减风险；对于入侵、授权等风险，建立了监控机制及响应机制。
BCR-06.1	Are any of your data centers located in places that have a high probability/ occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		华为云数据中心会考虑在政治稳定、社会犯罪率低、地理环境友好的地区选址，远离洪水、飓风、地震等自然灾害隐患区域，避开强电磁场干扰，并对于周围的隐患区域设定了最小距离的技术要求。
BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	X			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文档，其中包含设备的具体管控措施、例行的维护计划等。

BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	X			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文档，其中包含设备的具体管控措施、例行的维护计划等。
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			华为云遵循ISO27001附录A.17.2中信息处理设备应具有足够的冗余以满足可用性要求，通过设备、网络、供应商冗余以避免服务中断，并每年对此要求的落实进行审计以维持ISO 27001证书。
BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			华为云参考ISO22301的要求，使用RPO、RTO、灾难恢复成功率、备份成功率、恢复成功率等指标来衡量灾备目标的达成情况，并在评估业务中断影响的过程中对服务的恢复优先级、灾难重要性进行定级。
BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			华为云使用RPO、RTO、灾难恢复成功率、备份成功率、恢复成功率等指标衡量灾备目标的达成，并在响应业务中断影响的过程中对服务的恢复优先级、灾难重要性进行定级。
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations’ roles?	X			华为云根据ISO27001的要求制定了业务连续性管理规定以及事件响应策略与响应流程，相关的文档提供给所有相关的员工阅读，对于响应流程中的关键岗位需进行培训，并定期展开演练。
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	X			《华为云用户协议》以及《隐私政策声明》中告知客户其个人数据的保留策略，华为云具有实现上述协议中的保留策略的技术能力。 对于客户的内容数据，客户可自行配置内容数据的保留策略，华为云严格遵循客户的指令对其内容数据进行处理。

BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			华为云建立了数据留存机制的管理规定，规定中要求遵循法律要求的最低或最长留存期限，对于不同类型的个人数据有不同的留存期限的处置方法。
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			除IAM/目标存储服务OBS以外，华为云上线的所有服务和组件的管理数据（包含操作日志等）均会备份到OBS中，而同时IAM/OBS的管理数据需要备份到非OBS存储。 客户可使用华为云提供的云备份CBR服务对云内的服务器、云硬盘、虚拟化环境进行备份。
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			客户可使用华为云云监控服务CES对服务器的运行状态、云上资源进行实时监控，当出现硬件故障时，云监控将会通过邮件、短信、HTTP/S通知客户。同时，客户可通过云硬盘EVS中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。
BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	X			华为云为客户提供镜像服务IMS产品，客户可通过该产品对云服务器的实例进行备份，当该实例的软件环境出现故障时，可以使用备份的镜像进行恢复。
BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	X			华为云为客户提供存储容灾服务，帮助客户在容灾站点迅速恢复业务，缩短业务中断时间。
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	X			华为云会定期对用户的管理数据的备份有效性进行测试。 对于客户的内容数据，客户需根据业务需求自行制定备份、冗余机制，并对机制的有效性进行测试。

3.4 CCC 变更控制和配置管理

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			华为云使用DevOps以及DevSecOps模式进行开发，并制定了相应管理制度与流程对开发、变更活动进行控制。 详情可参考《华为云安全白皮书》。
CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			华为云建立了系统的变更管理、服务上线流程，并将其要求传达给所有相关的开发人员（包含内部员工及外部合作伙伴），新上线或变更的服务应遵循华为云发布、变更管理流程的规定。
CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X			华为云建立了系统的变更管理、服务上线流程，并将其要求传达给所有相关的开发人员（包含内部员工及外部合作伙伴），新上线或变更的服务应遵循华为云发布、变更管理流程的规定。在华为云外部审核如ISO 27001、PCI DSS认证及SOC报告中，均对变更管理要求的遵循性进行了审核。
CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析，并指定威胁削减方案。同时，所有云服务发布前均需通过多轮安全测试以及代码审查。 关于华为云开发活动的安全性，可参考《华为云安全白皮书》。

CCC-03.2	Is documentation describing known issues with certain products/services available?	X			华为云在其官网公布已经发现的产品或服务的漏洞并进行预警，客户可查看**安全公告**以了解漏洞影响的范围，处置方式及威胁级别。
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性，并在华为云官网的**安全公告**对安全漏洞进行披露。
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署工具链，通过质量门限进行控制，以评估云服务产品的质量。 所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题并经过了多轮安全测试，包括但不限于Alpha阶段的认证、鉴权、会话安全等微服务级功能和接口安全测试，Beta阶段通过对API和协议的fuzzing测试验证服务集成，Gamma阶段的数据库安全等安全专项测试。
CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?	X			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、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			华为云明确规定数据及代码进入生产环境前需删除所有测试过程中的认证、凭证数据以及业务数据，并删除测试代码。

CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			华为云所有的办公计算机均须安装公司指定的安全防护软件对计算机进行监控，并仅可以安装公司规定的安全软件列表中的软件。
CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		华为云不向客户提供该种类型的文档。华为云在为客户提供服务和产品的同时，将不断优化产品，产品的重大变更将会依照《华为云用户协议》中规定的方式通知客户。
CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			华为云制定了变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响，变更委员会审批通过后才可以上线。
CCC-05.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X			华为云制定了变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响，变更委员会审批通过后才可以上线。生产环境的变更策略符合现有的云服务等级协议。

3.5 DSI 数据安全与信息生命周期管理

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	

DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/ instantiating/ transporting data in the wrong country)?	X			华为云为客户提供的弹性云服务器ECS产品中包含添加标签的功能，标签用于标记云资源，如实例、镜像和磁盘等。如果客户的帐户下有多种云资源，并且不同云资源之间有多种关联，可以为云资源添加标签，实现云资源的分类和统一管理。
DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/ metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?		X		华为云仅为客户提供虚拟机而非硬件作为服务进行交付，不支持对于硬件及数据流的标记功能。
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?			X	华为云提供服务所需的操作文档，由客户基于服务功能、相关网络、系统组件以及其自身的业务需要来决定数据的处理、使用。
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	X			客户决定内容数据存储的具体地理位置的可用区。 华为云不会在未通知客户的情况下从选定的地区移动客户的内容，除非为遵守法律或政府实体的要求所必须。

DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			华为云服务提供REST和Highway方式进行数据传输： ● REST网络通道是将服务以标准RESTful的形式向外发布，调用端直接使用HTTP客户端，通过标准RESTful形式对API进行调用实现数据传输； ● Highway通道是高性能私有协议通道，在有特殊性能需求场景时可选用。 上述两种数据传输方式均支持使用传输层安全协议TLS1.2版本进行加密传输，同时也支持基于X.509证书的目标网站身份认证。 证书管理服务则是华为云联合全球知名数字证书服务机构，为租户提供的一站式X.509证书的全生命周期管理服务，实现目标网站的可信身份认证与安全数据传输。
DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			API调用需使用TLS加密以保证传输的机密性。目前API网关所有对外部网络开放的API均使用TLS1.2版本加密协议，并且支持PFS(Perfect Forward Secrecy ）安全特性。
DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?			X	对于内容数据，客户应对其内容数据的标签和处理建立相应的管控策略以确保数据的安全性。客户可使用标签管理服务TMS集中管理弹性云服务器ECS、虚拟私有云VPC、云硬盘EVS等服务中标识资源的标签，实现云上资源标签的统一管理。
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			X	对于内容数据来说，客户应根据业务需求建立并遵循结构化数据标记标准，华为云仅依从客户的指令对数据进行处理。

DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	对于内容数据来说，客户应建立适用于其数据的标签继承机制。
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			华为云为防止生产数据被移动或复制到非生产环境进行如下控制： ● 物理和逻辑网络边界以及严格执行的变更控制政策； ● 生产与非生产环境员工职责分离； ● 高度限制对云环境的物理和逻辑访问； ● 持续的安全、隐私和安全编码实践意识和培训； ● 持续记录和审核系统访问； ● 定期进行合规性审核以确保控制有效性。
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			华为云建立了数据安全管理的制度要求，其中定义和分配了数据管理的责任，具有相应权限的员工可以访问制度的具体内容。员工入职时，将对其数据管理职责进行培训与沟通，确认了解后再上岗。
DSI-07.1	Do you support the secure deletion (e.g., degaussing/ cryptographic wiping) of archived and backed-up data?	X			华为云支持根据客户要求对数据进行安全删除，安全删除的方式包括删除加密存储的加密密钥、底层存储回收并覆写、对报废的物理介质进行消磁/折弯/粉碎。
DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			在用户确认删除数据后，华为云会彻底删除用户数据，确保数据不泄露。包括内存删除、加密数据防泄漏、存储数据删除、磁盘数据删除、物理磁盘报废。 更多详细信息请查阅《华为云安全白皮书》。

3.6 DCS 数据中心安全

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			根据ISO27001标准，华为云的信息资产分类由专门的工具进行监控和管理，形成资产清单，每个资产均被指定所有者。华为云已通过ISO27001认证，认证证书可以从信任中心获取。
DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			根据ISO27001标准，华为云的信息资产由专门的工具进行监控和管理，形成资产清单，每个资产均被指定所有者。华为云已通过ISO27001认证，认证证书可以从信任中心获取。
DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3标准。华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行7*24小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。
DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	X			华为云支持基于IP地址的访问控制，用户可在IAM配置中选择是否基于IP地址作为身份验证的条件。

DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			华为云依据ISO27001的要求进行设备的识别与管理。华为云已通过ISO27001认证，认证证书可以从信任中心获取。 客户可通过IAM开启多因素验证，支持手机、邮箱、虚拟MFA等多种多因素验证方式。
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			承载华为云服务的基础设施在华为云的数据中心中，由授权人员管理，数据中心的基础设施，包括存储介质的进出及处理由华为云根据相关的介质管理要求进行管理。
DCS-05.1	Can you provide tenants with your asset management policies and procedures?	X			华为云不直接向客户提供机密的华为云政策和程序，华为云与外部认证机构和独立审计师一起审查和验证华为云对政策的遵守情况。
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			ISO27001标准要求组织制定标准和程序以保障在办公室、房间、设施和安全区域维护安全的工作环境。华为云已通过ISO27001认证，认证证书可以从信任中心获取。
DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			ISO27001标准中要求组织员工及第三方人员完成信息安全培训。华为云已通过ISO27001认证，认证证书可以从信任中心获取。

DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行7*24小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。
DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行7*24小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			华为云通过门禁控制系统，严格审核人员出入权限。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。

3.7 EKM 加密与密钥管理

编号	一致性评估问题	回答	华为云的回应

		是	否	不适用	
EKM-01.1	Do you have key management policies binding keys to identifiable owners?	X			根据华为云密钥管理策略，每个用户具有唯一的ID标识其身份。 客户可以使用IAM的密钥管理服务KMS为可识别的所有者绑定密钥。
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	X			客户可使用华为云数据加密服务DEW进行专属加密、密钥管理及密钥对管理，支持密钥创建、授权、自动轮换以及密钥硬件保护。客户可根据需要自主选择其所需的密钥管理机制。
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	X			华为云数据加密服务DEW中支持客户授权华为云托管私钥。
EKM-02.3	Do you maintain key management procedures?	X			华为云为客户提供数据加密服务DEW，其支持密钥托管，可帮助客户轻松创建及管理密钥，基于DEW，客户可实现密钥的全生命周期管理。
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			华为云推出的数据加密服务DEW，支持密钥托管，帮助客户轻松创建及管理密钥，基于DEW，客户可实现密钥的全生命周期管理，并记录密钥的所有权。
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			为保护租户密钥安全，减少密钥外泄风险，华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云HSM供租户选择，满足不同租户的实际需求，例如通过FIPS140-2国际权威认证的第三方HSM。
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			客户负责对其内容数据进行加密存储。华为云的数据加密服务DEW可为客户提供在云硬盘EVS、对象存储OBS、云硬盘备份VBS等服务的加密存储功能。

EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过如下方式提供： 1. 虚拟专用网络（VPN）：用于在远端网络和VPC之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云。目前，华为云采用硬件实现的IKE（密钥交换协议）和IPSecVPN结合的方法对数据传输通道进行加密。 2. 应用层TLS与证书管理：华为云服务提供REST和Highway方式进行数据传输。 以上数据传输方式均支持使用传输层安全协议TLS1.2版本进行加密传输，同时也支持基于X.509证书的目标网站身份认证。
EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			华为云建立了保护技术设备上数据的加密策略与密钥管理机制，包括人员的权限与职责分配、加密级别、加密方法进行了规定。
EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			华为云自身使用行业广泛使用的AES强效加密法对平台内数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全。 客户可使用数据加密服务对数据进行加密，华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云HSM供租户选择，满足不同租户的实际需求。
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			华为云支持由客户自主选择的密钥管理方式，华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云HSM供租户选择，满足不同租户的实际需求。

EKM-04.3	Do you store encryption keys in the cloud?	X			通过密钥管理服务KMS用户能够方便地管理自己的密钥，并能随时使用数据加密密钥DEK进行数据加密，确保关键业务数据的安全。KMS的根密钥保存在HSM中，从来不会出现在HSM之外，确保根密钥不泄露。HSM采用双机部署，保证HSM的高可靠性和高可用性。CMK经过根密钥加密后，以密文的形式保存在密钥存储节点中。
EKM-04.4	Do you have separate key management and key usage duties?			X	客户自行负责其密钥管理的职责分配，并对密钥的使用权限、管控权限进行记录。

3.8 GRM 治理与风险管理

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			华为云参考互联网安全中心CIS安全基线并将其融入华为云DevSecOps流程。CIS安全基线是一套用于网络系统安全配置和操作的业界优秀实践，覆盖技术（软件、硬件）、流程（系统和网络管理）、人员（最终用户和管理行为）。华为云建立内部的技术标准规范库，库中包含基础结构中各组件的信息安全基线。
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			华为云要求服务发布前均需通过基本安全要求的验证，以保障基础架构的合规性。

GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			华为云按照ISO27001标准要求进行信息安全风险管理，定期执行信息安全风险评估，风险评估涵盖信息安全的各方面，包括数据保护和分类、数据留存和传输位置、数据保存时间对法律法规的符合。 华为云已通过ISO27001认证，相关证书可以从信任中心获取。
GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	X			华为云按照ISO27001标准要求进行信息安全风险管理，每年至少执行一次信息安全风险评估，风险评估涵盖信息安全的各方面，包括数据保护和分类、数据留存和传输位置、数据保存时间对法律法规的符合。华为云已通过ISO27001认证，相关证书可以从信任中心获取。
GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。在组织方面，华为云建立网络安全管理机构，决策和批准公司总体网络安全战略。同时，将网络安全纳入员工商业行为准则中，通过每年开展员工商业行为准则学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识，并签署网络安全承诺书，承诺遵守公司各项网络安全政策和制度要求。
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			华为云不直接向客户提供机密的信息安全管理程序，华为云邀请第三方机构对华为云的信息安全管理程序进行评估，并确认其运行符合ISO27001的标准。华为云已通过ISO27001认证，相关证书可以从信任中心获取。
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	X			华为云按照ISO27001标准要求，每年邀请第三方机构对信息安全管理计划ISMP进行审核。华为云已通过ISO27001认证，相关证书可以从信任中心获取。

GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			依据ISO27001的要求，华为云明确了自身的信息安全目标，并制定相应的信息安全计划，分配执行信息安全活动所需的资源。华为云已通过ISO27001认证，相关证书可以从信任中心获取。
GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/ function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			华为云依据ISO27001及SOC2的要求，实施文档化的信息安全政策和程序，为华为云的操作和信息安全提供指导。员工可根据授权在查看已发布的信息安全政策和程序。ISO 27001与SOC相关证书及报告可以从信任中心获取。
GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	X			根据ISO27001要求，华为云领导层建立信息安全目标、制定相应的信息安全计划、分配执行信息安全活动所需的资源，信息安全计划满足客户和华为云自身的要求。华为云已通过ISO27001认证，相关证书可以从信任中心获取。

GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			华为云在引入供应商时会与其签署保密及服务水平协议，协议中包含对于供应商的安全和隐私数据处理的要求。
GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			华为云在信任中心中展示了已获得的认证，并发布了多份法规、标准相关的白皮书，白皮书中对于华为云控制与法规要求之间的映射进行了介绍。 详情请参见华为云官网的**可信资源**页面。
GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			华为云遵守的控制、标准、认证、法规均已公开发布在华为云官网的**信任中心**。
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			华为建立了严密的安全责任体系，贯彻违规问责机制。华为云以行为和结果为主要依据对员工进行问责。根据华为云员工安全违规的性质，以及造成的后果确定问责处理等级，分级处理。对触犯法律法规的，移送司法机关处理。直接管理者和间接管理者存在管理不力或知情不作为的，须承担管理责任。违规事件处理根据违规个人态度与调查配合情况予以加重或减轻处理。
GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			华为云的违规政策供所有员工进行查看学习，并定期组织培训提升员工对违规行为、违规后果、惩罚措施的了解。
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			华为云会根据风险评估的结果每年更新安全策略、程序、标准和控制，以维持它们的有效性与相关性。

GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			当安全和隐私政策发生重大变更时，华为云将通过预留的联系方式正式通知指定的联系人。
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			华为云每年会对自身的隐私和安全政策进行审核，以评估其是否满足合规性与有效性。
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			华为云制定了信息安全风险评估方法，通过定性和定量的方法确定所有已识别风险的可能性和影响，根据可能性和影响判断风险的严重程度，按照ISO27001要求每年进行。
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			依据ISO27001的要求，华为云制定的信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	X			华为云根据ISO27001要求建立了适用于华为云组织范围内的信息安全风险管理程序来降低和管理风险，该信息安全风险管理程序由专门的部门定期检查更新。
GRM-11.2	Do you make available documentation of your organization-wide risk management program?	X			在审计PCI DSS和ISO27001等标准的合规性期间，外部认证机构会对华为云的风险管理计划及实施情况进行审查。

3.9 HRS 人力资源安全

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			华为云发布了人员安全相关管理规定，要求员工离职或离岗时向公司移交所持有的华为云资产。与合作伙伴合同/业务关系终止时，按照合作协议删除自带设备中在合作项目中产生的信息，并移交华为云提供的资产。
HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	X			华为云建立了人员离职/合作终止时的资产交接电子流，按照电子流程执行资产交接。
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			在适用法律允许的情况下，华为云会根据可接触的资产的机密性，在雇佣员工、承包商或其他第三方前对其进行背景调查。
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			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。

HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			华为云的新雇用或已上岗的员工在授予员工用户访问公司设施、资源和资产的权限之前，需先签署雇佣合同以及保密协议，并完成信息安全相关培训。
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			华为云内部发布了人员安全相关管理规定，提供员工雇佣前、雇佣中、雇佣关系结束的安全管理政策、流程支持。
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			在人员离岗、离职时撤销访问权为自动电子流，人力资源部门及IT部门跟进组织资产的返还。
HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization’s facilities)?	X			华为云制定了管理移动设备的规定，要求机要岗位不允许配备便携电脑。当便携电脑进入受控区域时需获得批准，同时便携电脑需要采取措施以防止丢失后的数据泄露。

HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			华为云专业的法务部门对保密协议的细节要求进行管理与定期审视，以维持保密协议满足业务运行的需要。
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			华为云在《华为云安全白皮书》中介绍了华为云责任共担模型，对华为云作为云服务提供商同客户之间分别承担的安全管理责任，此文档可以在信任中心的可信资源获取。
HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			华为云对终端设备、网络及系统组件的使用限额分别进行了规定，并说明了对限额的监控策略。
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X			华为云仅支持员工通过私人手机上安装应用程序访问公司邮箱、论坛等功能，并按照员工权限对应用程序的访问范围进行控制。

HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			华为云对全员进行安全意识培训，对不同类型的员工执行相应的网络安全基础培训，对典型安全的关联责任人进行精准培训，重点岗位安全培训赋能。更多详细信息请查阅《华为云安全白皮书》。
HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			华为云将网络安全纳入员工商业行为准则中，通过每年开展员工商业行为准则学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识，并签署网络安全承诺书，承诺遵守公司各项网络安全政策和制度要求。
HRS-09.3	Do you document employee acknowledgment of training they have completed?	X			华为云对每年开展员工商业行为准则学习、考试和签署活动及签署网络安全承诺书等行动进行记录，每年由内外部审计进行审核。
HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			对于涉及网络安全与隐私保护等敏感数据、系统、程序等关键岗位的员工，须进行上岗培训和相应的认证，并签署保密承诺函及保密协议。
HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	X			华为云将网络安全纳入员工商业行为准则中，通过每年开展员工商业行为准则学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识，并签署网络安全承诺书，承诺遵守公司各项网络安全政策和制度要求。

HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			华为云对全员进行安全意识培训，对不同类型的员工执行相应的网络安全基础培训，对典型安全的关联责任人进行精准培训，重点岗位安全培训赋能。更多详细信息请查阅《华为云安全白皮书》。
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			华为云将网络安全纳入员工商业行为准则中，通过每年开展员工商业行为准则学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识，并签署网络安全承诺书，承诺遵守公司各项网络安全政策和制度要求。
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			依据SOC、PCI DSS和ISO27001等标准的要求，华为云建立对于员工的职责与行为规范进行规定，第三方审核机构会对员工是否被告知维护信息安全的工作责任进行审查。
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			依据SOC、PCI DSS和ISO27001等标准的要求，华为云建立对于员工的职责与行为规范进行规定，第三方审核机构会对员工是否被告知需确保设备安全的工作责任进行审查。
HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			依据SOC、PCI DSS和ISO27001等标准的要求，华为云建立对于员工的职责与行为规范进行规定，第三方审核机构会对华为云是否对所有计算机和笔记本电脑进行配置以确保在预定义的时间之后锁定屏幕进行审查。
HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			依据SOC、PCI DSS和ISO27001等标准的要求，华为云建立对于员工的职责与行为规范进行规定，第三方审核机构会对华为云是否有政策和程序可确保无人值守的工作区没有公开可见的（例如，在桌面上）敏感的文档进行审查。

3.10 IAM 身份与访问控制

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。 客户可使用IAM限制访问权限，并通过云日志服务CLS记录对于敏感信息或安全配置的访问、修改记录。
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			华为云使用日志系统对管理员级别的访问进行监控，控制非管理员员工不具备超过其应有权限，如特权访问的权限。
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。
IAM-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/ assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。

IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。
IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			华为云承载了众多客户的数据，各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。 以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性，如块存储，数据隔离以卷（云硬盘）为单位进行，每个卷都关联了一个客户标识，挂载该卷的虚拟机也必须具有同样的客户标识，才能完成卷的挂载，确保客户数据隔离。
IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			华为云为每一位员工提供了唯一的身份标识并根据工作职责划分权限，员工在每一次登陆对其身份进行验证，出现事故时可及时追溯日志进行问责。华为云IAM可帮助客户实现AAA规则，支持云平台的身份验证、授权以及问责机制。
IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X			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，对于特权账号严格被纳管回收。员工每次登陆均需要使用多重身份验证确定身份。
IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			华为云的云监控服务对客户正在启用的系统的运行情况进行监控而无论系统的状态如何。系统删除后，该系统的访问将不再被监控。

IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。所有的端口、应用、系统组件等的访问均仅向授权的个人和应用程序开放。
IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			华为云内部的IAM系统负责对员工全生命周期的管理，对其的身份信息、职位、访问权限、账号类别进行存储与管理。
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			华为云内部的IAM系统负责对员工全生命周期的管理，对其的身份信息、职位、访问权限、账号类别进行存储与管理。
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			客户可参考华为云IAM产品文档中的最佳实践，制定自身的职责分离策略，以及如何安全使用IAM。文档中提供资源授权管理及权限设置案例供客户进行参考
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。所有的端口、应用、系统组件等的访问均仅向授权的个人和应用程序开放。
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。

IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?	X			华为云依据ISO27001的要求管理第三方供应商，并与其签署保密及服务水平协议，协议中包含安全和隐私数据处理的要求，管理其访问权限不应超过其服务所必须。
IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	X			华为云基于权限最小原则为员工分配权限，除非工作必要，不会给予员工访问客户内容数据的权限，并对所有访问操作进行日志记录。
IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。所有的端口、应用、系统组件等的访问均仅向授权的个人和应用程序开放。
IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			华为云对员工按工作需要的最小范围分配权限，依靠IAM进行身份的验证与识别，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。所有的端口、应用、系统组件等的访问均仅向授权的个人和应用程序开放。
IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?	X			华为云对员工按工作需要的最小范围分配权限，依靠IAM进行身份的验证与识别，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。访问、复制等操作均仅向授权的个人和应用程序开放。

IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			华为云为每一位用户提供单独的账户，在员工入职前评估其工作职责与工作内容，依据权限最小化原则为其提供、管理、审核权限。
IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			华为云为每一位用户提供单独的账号，在员工入职前依据其工作职责与工作内容，依据权限最小化原则为其提供权限，包含对权限范围内的数据、应用程序、基础架构、网络组件的访问。
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			与ISO27001标准的相关要求保持一致，华为云依据员工工作需要为其提供所需的最小权限，并每年对权限进行审阅，使系统用户及管理员的始终遵循最小权限原则。华为云每年会对ISO27001的证书进行维持，持续遵循标准的要求。

IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			与ISO27001标准的相关要求保持一致，华为云依据员工工作需要为其提供所需的最小权限，并每年对权限进行审阅，使系统用户及管理员的始终遵循最小权限原则。华为云每年会对ISO27001的证书进行维持，持续遵循标准的要求。
IAM-10.3	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			与ISO27001标准的相关要求保持一致，华为云依据员工工作需要为其提供所需的最小权限，并每年对权限进行审阅，使系统用户及管理员的始终遵循最小权限原则。华为云每年会对ISO27001的证书进行维持，持续遵循标准的要求。
IAM-10.4	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?		X		客户需承担其自身数据的访问控制责任，确保其访问权限有效设置以避免不当访问。华为云严格遵守租户隔离原则，不同租户间数据在逻辑上相互隔离。华为云的特权用户访问控制每年通过了SOC、ISO27001以及PCIDSS的认证审核。
IAM-11.1	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			员工及其他第三方在状态发生变化后，如离职或职位变更后，按照调动、离职安全审查清单，对内部调离、离职人员进行离岗安全审查，包括离岗权限账号的清理或修改等。

IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			员工及其他第三方在状态发生变化后，如离职或职位变更后，按照调动、离职安全审查清单，对内部调离、离职人员进行离岗安全审查，包括离岗权限账号的清理或修改等。
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			目前华为云支持两种形式的联邦身份认证： ● 浏览器页面单点登录（WebSSO）：浏览器作为通讯媒介，适用于普通用户通过浏览器访问华为云。 ● 调用API接口：开发工具/应用程序作为通讯媒介，例如OpenStackClient、Shibboleth ECPClient，适用企业或用户通过API调用方式访问华为云。
IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	X			华为云支持基于SAML2.0协议的单点登录，客户可以使用华为云的身份提供商功能，实现用户使用企业身份提供商账号单点登录华为云。 目前华为云支持两种形式的联邦身份认证： ● 浏览器页面单点登录（WebSSO）：浏览器作为通讯媒介，适用于普通用户通过浏览器访问华为云。 ● 调用API接口：开发工具/应用程序作为通讯媒介，例如OpenStackClient、ShibbolethECPClient，适用企业或用户通过API调用方式访问华为云。

IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/ authorizing users?	X			华为云支持基于SAML2.0协议的单点登录，客户可以使用华为云的身份提供商功能，实现使用企业身份提供商账号单点登录华为云。 目前华为云支持两种形式的联邦身份认证： ● 浏览器页面单点登录（WebSSO）：浏览器作为通讯媒介，适用于普通用户通过浏览器访问华为云。 ● 调用API接口：开发工具/应用程序作为通讯媒介，例如OpenStackClient、ShibbolethECPClient，适用企业或用户通过API调用方式访问华为云。
IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?			X	客户应根据其适用的法律法规对其访问权限设置约束与控制规则，并通过IAM对账户权限进行管理。
IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			客户可通过IAM对账户权限进行管理，依据业务具体需要设定角色与组，并根据安全需求配置账号锁定策略、密码复杂度策略、多因素验证等功能。
IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			华为云的IAM服务支持使用多因素认证用于登录验证和操作保护。 开启了登录验证功能后，用户登录控制台时，除了需要输入用户名和密码外，还需要在登录验证页面输入验证码；开启了操作保护后，用户进行敏感操作时，需要输入验证码确认操作。多因素认证设备支持手机、邮箱和虚拟MFA设备。

IAM-12.7	Do you allow tenants to use third-party identity assurance services?	X			华为云支持基于SAML2.0协议的单点登录，客户可以使用华为云的身份提供商功能，实现用户使用企业身份提供商账号单点登录华为云。 目前华为云支持两种形式的联邦身份认证： ● 浏览器页面单点登录（ WebSSO ）：浏览器作为通讯媒介，适用于普通用户通过浏览器访问华为云。 ● 调用API接口：开发工具/应用程序作为通讯媒介，例如OpenStackClient、ShibbolethECPClient，适用企业或用户通过API调用方式访问华为云。
IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			华为云的IAM服务支持设置密码复杂度、修改周期等策略。客户的IAM管理员可根据需要设置密码策略，例如密码最小长度、密码中同一字符连续出现的最大次数、密码不能与历史密码相同等。
IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			华为云的IAM服务支持设置账户锁定、停用等策略。如果在限定时间内达到登录失败次数后，账户会被锁定一段时间，锁定时间结束后，才能重新登录。租户管理员可以对账号锁定策略进行设置，该策略对账号以及账号下的IAM用户都生效。IAM账户在设置的有效期内没有通过界面控制台或者API访问华为云，将会被停用，该账户可以联系管理员重新启用。
IAM-12.10	Do you support the ability to force password changes upon first logon?	X			客户管理员在使用华为云统一身份认证服务IAM创建新用户时，可通过邮件发送一次性登陆链接给新用户，新用户使用链接进行登陆时需要设置密码，另外在客户管理员自定义新用户的密码可选择强制用户在激活后修改默认密码。两种方式均可避免IAM用户使用默认密码。

IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			华为云的IAM服务支持设置账户锁定、停用等策略。如果在限定时间内达到登录失败次数后，账户会被锁定一段时间，锁定时间结束后，才能重新登录。租户管理员可以对账号锁定策略进行设置，该策略对账号以及账号下的IAM用户都生效。IAM账户在设置的有效期内没有通过界面控制台或者API访问华为云，将会被停用，该账户可以联系管理员重新启用。
IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			华为云办公计算机上仅可安装限定的标准软件，不允许安装可超越系统、对象、网络、虚拟机和应用控制措施的程序，并对软件的安装进行监控。

3.11 IVS 基础设施与虚拟化安全

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；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。
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			华为云依照权限最小化原则分配员工的访问权限，员工仅可访问已授权的内容。对于日志的访问和审核权限只限于特定员工，其权限的审批需收到上级管理人员的批准，并定期进行审核。

IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X			华为云在信任中心中展示了已获得的认证，并发布了多份法规、标准相关的白皮书，白皮书中对于华为云控制与法规要求之间的映射与遵循性进行了介绍。详情请参见华为云官网的**可信资源**页面。
IVS-01.4	Are audit logs centrally stored and retained?	X			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。
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			华为云有专门的内审部门，定期对运维流程各项活动日志进行审计。
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			华为云对提供的服务的网络设备、应用系统启用安全日志，日志对设备、系统的所有更改都会进行记录。
IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			华为云为客户提供云审计服务，客户可使用云日志服务对虚拟机的配置、日志的更改进行记录，使用云审计服务对于配置的日志的完整性进行监控。
IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	X			客户可使用主机安全服务HSS对镜像文件进行完整性校验，对比的方法来确定当前文件状态是否不同于上次扫描该文件时的状态，利用这种对比来确定文件是否发生了有效或可疑的修改。当发现潜在风险，将及时提醒客户。

IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			华为云使用NTP4.2.8协议对系统内的时间进行同步。
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/ scenarios?	X			华为云在官网为客户提供SLA协议的内容，客户可查阅华为云**服务等级协议**页面获取更多信息。
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			华为云建立了完善的资源管理机制，对于华为统一虚拟化平台中的的资源进行容量规划，避免资源被过度使用的情况发生，满足客户的容量需求。
IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			华为云建立了完善的资源管理机制，对于华为统一虚拟化平台中的的资源进行容量规划，避免资源被过度使用的情况发生，满足客户的容量需求。
IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			华为云收集云服务的组件容量信息、系统性能以监控平台的稳定运营，持续满足用于向租户提供服务的所有系统的法规、合同和业务需求。

IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			针对公有云攻击的手段多样、流量巨大的特点，华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。
IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	X			华为云在官网发布了《华为云安全白皮书》、《华为云数据安全白皮书》，并提供覆盖多种行业和场景的解决方案服务咨询，可为客户提供多方面的安全体系结构指导。
IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/ zones?	X			华为云有专业的网络安全团队负责网络体系结构图的更新，并对各区域之间的防火墙规则进行检查。在华为云PCI DSS认证的年度审查中，该项内容也会通过第三方机构进行审计。
IVS-06.3	Do you regularly review for appropriateness the allowed access/ connectivity (e.g., firewall rules) between security domains/zones within the network?	X			华为云有专业的网络安全团队负责网络体系结构图的更新，并对各区域之间的防火墙规则进行检查。在华为云PCI DSS认证的年度审查中，该项内容也会通过第三方机构进行审计。
IVS-06.4	Are all firewall access control lists documented with business justification?	X			所有防火墙的控制及变更记录均被记录至安全日志中，防火墙配置需要特定管理员审批后才可变更。

IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			华为云为提升云服务的安全性，应用多种高级防护功能保护内网区域，包括： ● **DDoS**异常和超大流量清洗：在每个云数据中心边界部署华为专业的Anti-DDoS设备来完成对异常和超大流量攻击的检测及清洗。 ● 网络入侵检测与拦截：IPS具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。 ● **Web**安全防护：华为云部署了Web应用防火墙应对Web攻击，如Web应用层的DDoS攻击、SQL注入、跨站脚本攻击、跨站请求伪造、组件漏洞攻击、身份伪造等。
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			对于SaaS和PaaS产品的客户，华为云支持其使用虚拟私有云VPC服务在云上建立隔离的生产与测试环境流程。
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X			华为云发布了《华为云安全白皮书》、《华为云数据安全白皮书》，并在官网提供了覆盖多种行业和场景的解决方案服务咨询，可为客户提供多方面的安全体系结构指导。
IVS-08.3	Do you logically and physically segregate production and non-production environments?	X			华为云对于生产及非生产环境使用物理和逻辑控制并用的隔离手段，控制并用的隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力。

IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			华为云在网络边界部署DoS/DDoS防范清洗层、下代防火墙、入侵防御系统层以及网站应用防火墙层，在内部根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并使用隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力。
IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			华为云在网络边界部署DoS/DDoS防范清洗层、下代防火墙、入侵防御系统层以及网站应用防火墙层，在内根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并使用隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力。
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X			为保证租户业务不影响管理操作，确保设备、资源和流量不会脱离有效监管，华为云将其网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、BMC管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，便于实现职责分离。
IVS-09.4	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，确保客户只能访问到自己的数据。 在客户自建存储的场景下，例如在虚拟机实例上安装数据库软件时，建议客户利用华为云的虚拟私有云（VPC）服务构建出私有网络环境，通过子网规划、路由策略配置等进行网络区域划分，将存储放置在内部子网，并通过配置网络ACL和安全组规则对进出子网以和虚拟机的网络流量进行严格的管控。

IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			华为云对云端数据的隔离是通过虚拟私有云VPC实施的，VPC采用网络隔离技术，实现不同租户间在三层网络的完全隔离。 租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合VPN或云专线，将VPC与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用VPC的ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。
IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			云数据迁移服务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，用户可以利用VPN和SSL技术来避免传输安全风险。 用户数据源的访问信息（用户名和密码）存储在CDM实例的数据库中，并采用AES-256加密。
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			在应用程序或数据迁移的过程中，客户应考虑使用于生产环境相隔离的网络。

IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			华为云对接入主机操作系统的华为云管理员执行严格的权限访问控制，对其所执行的各项运维运营操作实行全面的日志审计。 华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面所有操作都会记录日志并及时传送到集中日志审计系统。
IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	云平台的基础设施不涉及无线网络环境。
IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	云平台的基础设施不涉及无线网络环境。

IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	云平台的基础设施不涉及无线网络环境。
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			华为云维护及更新自身的网络架构图，并由负责网络安全的团队对网络架构的合规性进行跟踪确认。
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			华为云在网络边界部署DoS/DDoS防范清洗层、下代防火墙、入侵防御系统层以及网站应用防火墙层，在内部根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并使用隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力。

3.12 IPY 互操作和可移植性

编号	一致性评估问题	回答	华为云的回应

		是	否	不适用	
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			租户可以通过官网的**华为云API清单**获取发布服务中提供的所有API的列表。
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			当客户需要导出其被华为云收集的个人数据时，华为云可以按照客户需求提供行业常见的标准格式数据。
IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?			X	客户应自行负责与第三方应用程序之间的互操作性。
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	X			华为云云数据迁移服务提供行业通用的虚拟机镜像格式，支持保存至客户本地数据中心，客户需自行完成镜像的移植工作。
IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?		X		华为云暂未提供此类服务级别协议。

IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			华为云使用TLS1.2对管理服务的访问及数据传输过程加密，数据在导入导出时将使用AES-256方式进行加密。
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			华为云为客户提供云数据迁移服务的产品文档及API接口文档，客户可参阅文档获取服务中与可移植性相关的信息。
IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			华为云使用行业广泛使用的虚拟化平台，如KVM、Xen、Docker等，降低客户的学习成本。
IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			华为云为客户提供基于数据库、文件存储、对象存储的迁移,并支持不同region及云至客户数据中心之间的迁移。
IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?		X		华为云管理并跟踪现有的虚拟机上的修改并会定期提供第三方机构进行审计，但这部分内容并不提供给客户进行审核。

3.13 MOS 移动安全

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X	移动设备可通过工作所需的华为云内部应用访问华为云企业办公环境，如及时沟通、邮件、论坛、人力管理等，并为此建立了响应的规章制度。但华为云不支持如IOS或安卓系统的手机、平板等移动设备对生产环境，尤其是客户内容数据的访问。
MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X	同MOS-02.1问题回复
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X	同MOS-02.1问题回复
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	同MOS-02.1问题回复

MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			X	同MOS-02.1问题回复
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X	同MOS-02.1问题回复
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X	同MOS-02.1问题回复
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	同MOS-02.1问题回复
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			X	同MOS-02.1问题回复

MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			X	同MOS-02.1问题回复
MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			X	同MOS-02.1问题回复
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			X	同MOS-02.1问题回复
MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X	同MOS-02.1问题回复
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	同MOS-02.1问题回复

MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			X	同MOS-02.1问题回复
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	同MOS-02.1问题回复
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			X	同MOS-02.1问题回复
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X	同MOS-02.1问题回复
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?			X	同MOS-02.1问题回复
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	同MOS-02.1问题回复
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	同MOS-02.1问题回复

MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	同MOS-02.1问题回复
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	同MOS-02.1问题回复
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	同MOS-02.1问题回复
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X	同MOS-02.1问题回复
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X	同MOS-02.1问题回复
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X	同MOS-02.1问题回复
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	同MOS-02.1问题回复

MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	同MOS-02.1问题回复

3.14 SEF 安全事件管理，电子发现与云取证

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			根据ISO27001标准的要求，华为云配备了专人与行业机构、风险和合规组织、地方当局和监管机构保持联系并建立联络点。华为云已经过独立审核机构的验证和认证，以确认符合ISO27001认证标准。
SEF-02.1	Do you have a documented security incident response plan?	X			华为云的事故响应程序、计划和程序是根据ISO27001标准制定的。华为云已经过独立审计机构的验证和认证，以确认符合ISO27001认证标准。
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	X			华为云制定了通用的安全事件响应计划及流程，包括响应相关人员的职责划分、响应速度、对外公布机制等内容。 客户应根据其需求自行制定适用的事件响应计划。
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			华为云发布了《华为云安全白皮书》，其中介绍华为云主要负责安全事件的响应，鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。

SEF-02.4	Have you tested your security incident response plans in the last year?	X			华为云在过去一年对于不同领域的安全事件进行了模拟演练，以测试计划的有效性。
SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			华为云建立的信息安全事件的管理流程，明确各角色的职责，华为云通过公司统一开展的年度例行学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识。员工需签署网络安全承诺书，承诺遵守公司各项网络安全政策和制度要求。对于其他外部相关人员，华为云与其签署保密协议并进行了信息安全培训，其中包含信息安全事件报告责任。
SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			华为云在官网提供安全公告以及漏洞反馈页面，通知客户最新的安全漏洞告警，为客户反馈安全漏洞提供渠道。
SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			华为云依据ISO27001、ISO27017等标准的要求，建立了安全事件响应计划及流程，并定期对安全事件响应计划在已开服国家和地区的合规性进行分析与检查。
SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			华为云依据ISO27001、ISO27017等标准的要求，建立了安全事件响应计划及流程，并定期对安全事件响应计划在已开服国家和地区的合规性进行分析与检查。

SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			华为云依据ISO27001、ISO27017等标准的要求，建立了安全事件响应计划及流程，并定期对安全事件响应计划在已开服国家和地区的合规性进行分析与检查。
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			华为云依据ISO27001、ISO27017等标准的要求，建立了安全事件响应计划及流程，并定期对安全事件响应计划在已开服国家和地区的合规性进行分析与检查。
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			华为云建立了事件管理平台，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。
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?		X		华为云的云服务有明确的职责边界，通常不会与租户进行安全事件数据的共享。 华为云提供完备的安全服务产品，租户根据自身业务情况进行配置后，通过安全服务产品进行相关的安全事件监控与数据收集

3.15 STA 供应链管理，透明与可审计

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X			华为云协同多个部门及相关供应商共同维护在供应链生命周期中，例如在交易、交付、服务水平监控等领域，客户个人数据的质量管理控制及风险管控措施。详情可参见《华为云数据安全白皮书》。 华为云不会对客户的内容数据的质量进行检查，客户具有内容数据的所有权和控制权，负责其内容数据的质量以及承担数据质量带来的风险。

STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			华为云制定了供应商安全管理要求，定期对供应商进行审查，验证其是否符合华为云安全和隐私标准。
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			华为云制定了完整的安全事件响应计划及流程，当触发安全事件时，华为云将及时开展事件处置，并华为云通过站内通知、电子邮件等方式向所有受影响的客户提供安全事件信息。
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			华为云收集云服务的组件容量信息以监控平台的稳定运营，并使用这些信息对云服务进行优化、升级。
STA-03.2	Do you provide tenants with capacity planning and use reports?	X			客户可通过购买华为云企业服务月报，每月定期查收包含云资源运行状态和服务支持的月度总结报告，以及基于华为云最佳实践的优化建议。 客户也可通过云监控服务自行监控云上服务、容量、网络的使用情况。云监控服务支持通过OpenAPI、SDK、Agent方式上报自定义指标，触发警告将及时通知客户。
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			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。此外，独立第三方评估机构也提供独立保证，这些评估员通过执行定期安全评估和合规性审计或检查（例如SOC、ISO标准、PCIDSS审计）来评估信息和资源的安全性、完整性、机密性和可用性，从而对风险管理内容/流程进行独立评估。

STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			华为云已建立供应商选择和监督体系，通过合同签订前的尽职调查以及合同签订后的定期评估来管理供应商对华为云具体的要求和合同义务的符合性。
STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			华为云已建立供应商选择和监督体系，通过合同签订前的尽职调查以及合同签订后的定期评估来管理供应商对华为云具体的要求和合同义务的符合性。
STA-05.3	Does legal counsel review all third-party agreements?	X			华为云与供应商签订的合同需要经过多轮合同评审流程，合同的内容由华为云法务团队负责审查。
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			供应商安全和隐私要求包含在已签署的合同协议中。与第三方的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			华为云为租户提供了云服务器备份服务，租户可以通过该服务将云服务器下所有云硬盘创建一致性在线备份，针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点。
STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			客户负责选择内容数据存储的具体地理位置的可用区。华为云不会在未通知客户的情况下从选定的地区移动客户的内容，除非要求遵守法律或政府实体的要求。
STA-05.7	Can you provide the physical location/ geography of storage of a tenant’s data upon request?	X			客户负责选择内容数据存储的具体地理位置的可用区，可用区的名字将标识其所在的国家及城市。
STA-05.8	Can you provide the physical location/ geography of storage of a tenant's data in advance?	X			客户负责选择内容数据存储的具体地理位置的可用区，可用区的名字将标识其所在的国家及城市。

STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			客户负责选择内容数据存储的具体地理位置的可用区。
STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			华为云建立了应对网络安全事件的响应流程，并针对关键基础设施、网络进行监控，可及时监测可能的网络攻击，避免数据泄露事件的发生。在华为云业务开展地区，若发生数据泄露事件，有专人负责通知客户及当地的监管部门。
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		华为云需要通过检测客户对于元数据的访问以根据用量计算账单。
STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		华为云暂不向客户提供子处理者及其协议副本。
STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			华为云制定了供应商安全管理要求，定期对供应商进行审查，验证其是否符合华为云安全和隐私标准，审查内容包含风险管理和治理流程。
STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			华为云已建立供应商选择和监督体系，通过合同签订前的尽职调查以及合同签订后的定期评估来管理供应商对华为云具体的要求和合同义务的符合性。

STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/ downstream)?	X			华为云已建立供应商选择和监督体系，通过合同签订前的尽职调查以及合同签订后的定期评估来管理供应商对华为云具体的要求和合同义务的符合性。 华为云法务团队也会定期对合同的条款进行审查。
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			华为云遵循供应商选择和监督体系，要求供应商提供统一的服务级别要求，并对其的遵循情况进行监督。
STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			华为云在官网为客户提供SLA协议的内容，客户可查阅华为云**服务等级协议**页面获取更多信息。
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			华为云为客户提供云监控服务、应用运维管理AOM、应用性能管理APM以帮助客户持续监控华为云提供的服务的各项指标，支持通过OpenAPI、SDK、Agent方式上报自定义指标，触发警告将及时通知客户。
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			华为云为客户提供应用性能管理APM、应用运维管理AOM服务。 APM可实时监控并管理企业应用性能和故障的云服务，AOM是面向运维、开发、运营人员及IT经理的云上运维平台，以日志、指标、事件形式实时监控运行、运营数据，为客户提供云资源、网络、中间件、上云业务等全链路的数百种运维指标。
STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?			X	此问题与华为云服务无关。
STA-07.8	Do you review all service level agreements at least annually?	X			华为云法务团队定期审查对SLA进行审查，当前可用的SLA请参阅**服务等级协议**页面

STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			华为云制定了供应商安全管理要求，并在第三方机构每年进行ISO 27001审查时，对供应商管理情况进行审查。华为云收集供应商审计报告，验证其是否符合华为云安全和隐私标准。
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			华为云制定了供应商安全管理要求，并在第三方机构每年进行ISO 27001审查时，对供应商管理情况进行审查。华为云收集供应商审计报告，验证其是否符合华为云安全和隐私标准。
STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			华为云制定了供应商安全管理要求，并在第三方机构每年进行ISO 27001审查时，对供应商管理情况进行审查。华为云收集供应商审计报告，验证其是否符合华为云安全和隐私标准。
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			华为云每季度都会组织内部以及外部具有一定资质的第三方进行对华为云的所有的系统、应用、网络进行漏洞扫描。并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。

3.16 TVM 威胁、脆弱性管理

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	

TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X			华为云所有的办公计算机均需安装公司指定的安全防护软件，仅可以安装指定软件列表的软件。对于IT基础系统、组件则通过IDS/IPS等方式进行保护。
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X			华为云所有的办公计算机均需安装公司指定的安全防护软件、基础设施组件安装杀毒软件等安全软件，并限制安全软件的配置修改权限以及对其要求强制更新。
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			与PCI DSS标准的相关要求保持一致，华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描，并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。
TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			与PCI DSS标准的相关要求保持一致，华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描，并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			与PCI DSS标准的相关要求保持一致，华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描。并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?		X		华为云将自行跟进漏洞扫描的结果，此结果不向租户提供。

TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			对于所有获知的安全漏洞信息，华为云将对每个漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后对修复情况进行验证，持续跟踪确认风险得到消除或缓解。
TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?			X	华为云不使用租户的内容数据作为服务的一部分。当华为云发现存在可能影响租户内容数据安全的漏洞或其他安全事件时，会基于与客户签署的合同内的规定，通知客户相应事项。
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	华为云所有的办公计算机均需安全公司指定的安全软件，仅可以安装指定软件列表的软件，不支持运行移动代码。
TVM-03.2	Is all unauthorized mobile code prevented from executing?	X			华为云所有的办公计算机均需安全公司指定的安全软件，仅可以安装指定软件列表的软件，不支持运行移动代码。

4 结语

华为云始终秉持着华为公司“以客户为中心”的核心价值观，积极践行信息安全实践，为此华为云构建了信息安全管理体系，应用业界通用的信息安全保护技术，通过第三方机构的认证与审核检查安全控制的有效落实，致力于保护客户的数据安全。

同时，为帮助客户应对日益复杂和开放的网络环境及日益发展的信息安全技术，华为云不断开发各种数据保护领域的工具、服务和方案，支持客户提升数据保护能力，降低风险。

本白皮书仅供客户作为参考，不具备任何法律效力或构成法律建议，也不作为任何客户在云上环境一定合规的依据。客户应酌情评估自身业务和安全需求，选用适合的云产品及服务。

5 版本历史

日期	版本	描述
2020-09-30	1.0	首次发布

