华为云 CSA CCM 遵从性说明（CSA CAIQ v4.0.2）

文档版本 2.0

发布日期 2022-05-16

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 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17个控制领域，共计197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
A&A	1. 审计和鉴证
AIS	2. 应用和接口安全
BCR	3. 业务连续性管理和业务弹性
CCC	4. 变更控制和配置管理
CEK	5. 密码加密和密钥管理
DCS	6. 数据中心安全
DSP	7. 数据安全和隐私生命周期管理
GRC	8. 治理、风险与合规
HRS	9. 人力资源安全
IAM	10. 标识和访问管理
IPY	11. 互操作性和可移植性
IVS	12. 基础设施和虚拟化安全
LOG	13. 日志记录和监控

控制 ID	控制领域
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. 威胁和漏洞管理
UEM	17. 通用端点管理

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261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2021年最新发布的4.0.2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）
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）

产品类型	覆盖产品
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 A&A 审计和鉴证

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	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。
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated 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。

A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards 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。
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	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。
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/ contractual, and statutory requirements applicable to the audit?	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，同时考虑了适用法律法规的要求。 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。
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	X			华为云已建立审计管理流程，并按该流程执行审计。审计管理流程中包括审计支持计划、风险分析、安全控制评估和总结、整改计划、报告、审阅以往报告及相关证据方面的管理要求。 华为云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。

A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	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。
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	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。 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。

3.2 AIS 应用和接口安全

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	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	X			华为云根据ISO27001要求建立了适用于华为云组织范围内的应用安全策略和流程，该策略和流程由专门的部门定期检查更新。
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。

AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	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》。 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。 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。 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-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	X			华为云会基于业务目标、安全要求及合规职责制定其安全技术和安全运营指标，并按该指标管理应用安全。
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	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-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	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-05.2	Is testing automated when applicable and possible?	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-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	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-06.2	Is the deployment and integration of application code automated where possible?	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-07.1	Are application security vulnerabilities remediated following defined processes?	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。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。

AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	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。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。

3.3 BCR 业务连续性管理和业务弹性

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	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	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。 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	Are the policies and procedures reviewed and updated at least annually?	X			在审计ISO22301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。
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	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-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	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。 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ISO27001证书。 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。 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-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	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。 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-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	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。 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-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	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-05.3	Is business continuity and operational resilience documentation reviewed periodically?	X			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-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	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-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	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-08.1	Is cloud data periodically backed up?	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-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	X			通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。

BCR-08.3	Can backups be restored appropriately for resiliency?	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。
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	X			华为云已建立灾难恢复计划，确保在发生自然灾害或认为灾害时，业务可及时恢复。
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	X			华为云至少每年或在发生重大变更时，更新已拟定的灾难恢复计划。
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	X			华为云至少每年或在发生重大变更时，更新已拟定的灾难恢复计划，并进行灾难恢复演练。
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	X			华为云每年组织进行消防演练，演练记录均在有关部门进行备案。
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	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。

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 risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	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。 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-01.2	Are the policies and procedures reviewed and updated at least annually?	X			在审计ISO27001和SOC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。
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	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-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	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-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	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	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	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。
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	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-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	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。 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。
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	X			华为云针对例外情况，会组织风险管理专家，对该例外情况进行评审，并按照专家组的评审意见进行后续工作。
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	X			与GRC-04一致。
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	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。

3.5 CEK 密码加密和密钥管理

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	

CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	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。
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated 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。
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	X			华为云按照ISO27001的要求，针对加密管理制度和流程设立了相应的角色和职责。

CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	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。 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。
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	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。 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。

CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	X			华为云建立了变更管理流程，如涉及密码学、加密管理技术等相关的变更需按照变更管理流程获得审批。
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	X			华为云针对密码学、加密管理技术等相关的变更，需按照变更管理流程获得审批，审批过程中会充分考虑变更可能造成的风险，并分析其成本效益。
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	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，风险评估涵盖加密和密钥管理相关的制度和流程。
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	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。

CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	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。
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but 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。
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	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。 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。
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	X			华为云规定对称密钥、非对称加密算法私钥仅可被分发至必须持有该密钥的实体。
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	X			华为云按照加密数据的风险等级管理密钥周期，定期轮换加密密钥。

CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	X			华为云规定确认已不再使用某密钥时，需确保密钥本身及所有与密钥有关的信息均被销毁。在销毁密钥及与密钥相关的信息时，应首先确认该密钥确实已不再任何情况下使用。
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	X			华为云在确定密钥或密钥组件已不再需要后会立即将其销毁： 1. 对于保存在内存中的密钥或密钥组件，会对内存用心的数据覆盖或下电； 2. 对于保存在磁盘中的密钥或密钥组件，会对磁盘的分区进行低级格式化或对磁盘文件重写“0”“1”、安全随机数序列执行覆盖3次以上，其中“0”“1”及安全随机数三种覆盖方式必须全部被执行； 3. 对于保存在CD磁盘上的密钥或密钥组件，会对CD进行物理粉粹等。

CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	X			华为云针对密钥的生成、分发、更新、存储、备份和销毁全生命周期，识别各个阶段可能的风险，基于可能的风险，对密钥的各个阶段制定安全管理控制。
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/ from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	X			华为云针对密钥的生成、分发、更新、存储、备份和销毁全生命周期，识别各个阶段可能的风险，基于可能的风险，对密钥的各个阶段制定安全管理控制。
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	X			华为云在确定密钥或密钥组件已不再需要后会立即将其销毁： 1. 对于保存在内存中的密钥或密钥组件，会对内存用心的数据覆盖或下电； 2. 对于保存在磁盘中的密钥或密钥组件，会对磁盘的分区进行低级格式化或对磁盘文件重写“0”“1”、安全随机数序列执行覆盖3次以上，其中“0”“1”及安全随机数三种覆盖方式必须全部被执行； 3. 对于保存在CD磁盘上的密钥或密钥组件，会对CD进行物理粉粹等。

CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	X			华为云针对密钥的生成、分发、更新、存储、备份和销毁全生命周期，识别各个阶段可能的风险，基于可能的风险，对密钥的各个阶段制定安全管理控制。
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	X			华为云针对密钥的生成、分发、更新、存储、备份和销毁全生命周期，识别各个阶段可能的风险，基于可能的风险，对密钥的各个阶段制定安全管理控制。
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	X			华为云针对密钥的生成、分发、更新、存储、备份和销毁全生命周期，识别各个阶段可能的风险，基于可能的风险，对密钥的各个阶段制定安全管理控制。

CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	X			华为云针对密钥的生成、分发、更新、存储、备份和销毁全生命周期，识别各个阶段可能的风险，基于可能的风险，对密钥的各个阶段制定安全管理控制。

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	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	X			华为云依据ISO27001及SOC2的要求，制定并实施施介质管理规定，为华为云的操作和信息安全提供指导。其中对介质清退报废进行分类操作，通过多种方式实现数据清除、磁盘消磁，并对销毁操作进行记录。
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	X			华为云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。

DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/ information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	X			华为云依据ISO27001及SOC2的要求，制定并实施移动介质管理规定，为华为云的操作和信息安全提供指导。各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对个人存储介质及数字设备进出不同安全保密级别的区域及其使用均制定了不同的安全要求。 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。
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	X			华为云制定了存储介质及设备进出机房管理规定，要求存储介质及设备进出机房前需进行登记并得到授权。物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/ information to an offsite or alternate location reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。

DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	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-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	X			华为云依据ISO27001及SOC2的要求，制定并实施存储介质及设备进出机房管理规定，为华为云的操作和信息安全提供指导。
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	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-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	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-07.1	Are physical security perimeters implemented to safeguard personnel, 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。
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	X			华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。 华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置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	Is equipment identification used as a method for connection authentication?	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。

DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	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-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	X			华为云通过门禁控制系统，严格审核人员出入权限。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。
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	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-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	X			华为云通过门禁控制系统，严格审核人员出入权限。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。

DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	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。 华为云数据中心选址时会考虑避开强电磁场干扰。华为云机房建设时规定用于任何网络布线和外接设备必须使用安全的导管和防篡改硬件。光纤电缆等通信设备穿过公开访问的区域时，管道和桥架会设置为金属材质，全程覆盖保护电缆在管内或线槽铺设，并设置了漏电检测装置。
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	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GB 50174《电子信息机房设计规范》A类和 TIA 942《数据中心机房通信基础设施标准》中的T3+ 标准。 通过精密空调、集中加湿器自动调节，华为云数据中心机房温湿度保持在设备运行所允许的范围内，使设备元器件处于良好运行状态。机柜冷热通道有合理的布置，利用架空地板下空间作为静压箱来给机柜送风，并设置了冷通道密闭，以防止局部热点。
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	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。
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?		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。

3.7 DSP 数据安全和隐私生命周期管理

编号	一致性评估问题	回答	华为云的回应

		是	否	不适用	
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	X			华为云制定了数据安全策略及数据安全保护管理规定，采取适当保护措施并严格执行，以保证数据安全。 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。
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。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。
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	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。 华为云对删除虚拟卷采用清零措施，确保数据不可恢复，有效防止被恶意租户使用数据恢复软件读出磁盘数据，杜绝信息泄漏风险。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。
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	X			华为云适用数据发现工具以识别系统、数据库或者文件里的个人数据，以了解业务是否包含个人数据以及个人数据的类型和流转情况等相关的信息，同时也可以采取恰当的隐私保护措施。数据管理服务可以帮助华为云完成数据资产注册和管理，对个人数据清单的记录、全生命周期管理提供工具化的能力。

DSP-04.1	Is data classified according to type and sensitivity levels?	X			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。
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	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。
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	X			华为云至少每年或在变更后审查数据流文档。
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	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。
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	X			华为云至少每年审查数据责任矩阵图。
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	X			华为云服务产品和组件遵从华为安全设计原则、规范、基线，在安全需求分析和设计阶段中根据业务场景、数据流图、组网模型进行威胁分析，借助高度自动化的工具及丰富的案例库，极大地提升了方案设计的效率及完备性。
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	X			华为云各服务产品的设计遵循《隐私保护设计规范》，该规范建立了隐私基线、维护隐私的完整性和指导隐私风险分析，制定对应措施并作为需求落入服务产品开发设计流程。

DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	X			华为云各服务产品的设计遵循《 隐私保护设计规范 》，该规范建立了隐私基线、维护隐私的完整性和指导隐私风险分析，制定对应措施并作为需求落入服务产品开发设计流程。
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	X			为有效地识别和控制隐私风险，华为云在云服务各项业务中广泛地开展隐私风险分析和管理工作。华为云要求在所有业务处理个人数据前必须开展隐私风险分析（ PIA ），主要包括识别业务涉及的个人数据项、业务场景及处理过程、合规分析、对数据主体可能产生的影响、风险分析并制定风险控制措施和计划等，只有将隐私风险降低至可接受的水平后才能开展业务。 对于云服务，华为云要求在云服务规划阶段即开展PIA，并在设计活动中对隐私风险进行详细的分析，并将所有隐私风险控制需求落入设计方案中。
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	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。 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。

DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	X			华为云为客户提供便捷的行使数据主体权利的渠道，客户可以通过隐私声明中的邮箱发起请求，华为云将在验证请求者身份信息后按照适用法规要求进行响应并处理。 华为云配备专业团队响应客户关于个人数据和隐私保护相关的请求，当接收到客户问题请求后在规定时间内完成响应和请求处理，反馈处理结果给客户。
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	X			华为云基于《 隐私政策声明 》中披露的目的收集个人数据，并且华为云针对涉及个人数据的产品及服务会定期进行隐私影响评估，以防产品及服务涉及的个人数据的收集超出实际目的所需最小范围，避免过度收集个人数据。
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	X			华为云对所有供应商按要求进行尽职调查及隐私安全能力评估，合同中明确供应商作为处理者/子处理者的隐私保护义务及适用法律法规的要求，确保供应商满足客户的隐私保护要求。其他华为云可能依法向第三方披露数据的场景可详见《 隐私政策声明 》。
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	X			华为云对所有供应商按要求进行尽职调查及隐私安全能力评估，合同中明确供应商作为处理者/子处理者的隐私保护义务及适用法律法规的要求，确保供应商满足客户的隐私保护要求。其他华为云可能依法向第三方披露数据的场景可详见《 隐私政策声明 》。

DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data 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： 1. 物理和逻辑网络边界以及严格执行的变更控制政策； 2. 生产与非生产环境员工职责分离； 3. 高度限制对云环境的物理和逻辑访问； 4. 持续的安全、隐私和安全编码实践意识和培训； 5. 持续记录和审核系统访问； 6. 定期进行合规性审核以确保控制有效性。
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	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。 《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。
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	X			华为云已构建全数据生命周期的安全防护能力。通过自动化敏感数据发现、动态数据脱敏、高性能低成本数据加密、快速异常操作审计、数据安全销毁等多项技术的研究与应用，实现数据在创建、存储、使用、共享、归档、销毁等多个环节的管控，保障云上数据安全。

DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	X			华为云已制定个人数据泄露响应流程，其中包括通知云客户相关的管理要求。
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	X			华为云内部设立司法协助调查处理团队，由该团队负责协助调查或响应调查请求。华为云会在司法协助后及时告知受影响的客户，有法律法规禁止的除外。
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	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。

3.8 GRC 治理、风险与合规

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	

GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	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。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。
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	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。
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	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。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。 为有效地识别和控制隐私风险，华为云在云服务各项业务中广泛地开展隐私风险分析和管理工作。华为云要求在所有业务处理个人数据前必须开展隐私风险分析（PIA） 主要包括识别业务涉及的个人数据项、业务场景及处理过程、合规分析、对数据主体可能产生的影响、风险分析并制定风险控制措施和计划等，只有将隐私风险降低至可接受的水平后才能开展业务。
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	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。

GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	X			华为云针对例外情况，会组织风险管理专家，对该例外情况进行评审，并按照专家组的评审意见进行后续工作。
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	X			华为云已制定并实施信息安全计划ISMP，其内容已涵盖CCM所有相关领域。华为云每年邀请第三方机构对信息安全管理计划ISMP进行审核。
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	X			华为云通过自上而下的治理结构实现信息安全，由领导层决策和审批信息安全策略和目标、信息安全相关角色和职责，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，同时为体系内其他角色提供支持，促进体系持续改进。
GRC-07.1	Are all relevant standards, regulations, legal/ contractual, and statutory requirements applicable to your organization identified and documented?	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。
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	X			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。

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	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties)established, documented, approved, communicated, applied, evaluated, and maintained?	X			华为云根据ISO27001要求建立了人员安全相关管理规定，其中包括人员背景调查的策略和流程。
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	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-01.3	Are background verification policies and procedures reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。

HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	X			华为云根据ISO27001要求建立并实施了资产的使用规则，包括管理原则、相关人员职责、办公计算机安全要求、办公网络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	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。
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。

HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	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，为华为云的远程工作和远程访问提供指导。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。
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	X			华为云按照ISO27001要求每年对相关策略和流程进行审阅和更新。
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	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。 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-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	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-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, 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-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	X			华为云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-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	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-10.1	Are requirements for non-disclosure/ confidentiality agreements reflecting organizational data protection needs 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-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	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》。 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-11.2	Are regular security awareness training updates provided?	X			华为云每年根据适用的法律法规、标准及业务需要，更新信息安全意识培训的内容，并组织员工进行培训。

HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	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。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-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	X			华为云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。 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-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	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。 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。

3.10 IAM 标识与访问管理

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	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	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。 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-01.2	Are identity and access management policies and procedures reviewed and updated 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。
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	X			华为云已制定并实施密码策略，包括规定密码长度、复杂度、更改周期，密码中不允许包含用户ID，不可使用易被破解的常用口令以及最近5次使用过的密码等。
IAM-02.2	Are strong password policies and procedures reviewed and updated 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。

IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	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-04.1	Is the separation of duties principle employed when implementing information system access?	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-05.1	Is the least privilege principle employed when implementing information system access?	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-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	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-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	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-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	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-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	X			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，实现合理的权限分工，同时制定了SOD权责分离管理矩阵以帮助实现该管理原则。 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-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	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-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	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-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	X			除非是为客户提供必要的服务，或者为遵守法律法规活政府机关的约束性命令，华为云不会触碰客户数据。
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	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。且收集的日志信息为“只读”模式。
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	X			华为云涉及disable日志的“read only”模式时，均需要经过上层审批，审批过程均有日志记录。

IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	X			华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。 对云服务的访问通过统一身份认证服务（IAM – Identity and Access Management）对用户进行访问控制和权限管理。 所有运维账号，设备及应用的账号均进行统一管理，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。如果账号使用人要使用账号，账号管理员可启动授权流程，通过口令或者提升账号的权限等方式进行授权；账号的申请人和审批人不能是同一个人。
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	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。 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-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	X			华为云支持基于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。
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	X			华为云制定并实施密码算法应用规范，规定了密码算法的选择规则及应用规则，同时给出了常见应用实例指导。 华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理。

IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	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。

3.11 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	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	X			华为云要求应用程序的代码应该时易于扩展、可移植的。 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-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	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-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	X			华为云要求应用程序的代码应该时易于扩展、可移植的。
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	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-01.5	Are interoperability and portability policies and procedures reviewed and updated 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。
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	X			客户可通过API Explorer搜索对应云服务的API接口文档，实现应用和数据的可移植性。
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	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。 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-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy		X		华为云在与客户终止服务后，在其规定的宽限期或保留期间内，会保留客户的内容。进入保留期后，客户不可以访问及使用云服务，但相应云服务资源及存储在云服务中的资源的内容会被系统保留。保留期届到期时如客户仍未全额付费，相应的云服务资源将被释放，您资源的内容也会被删除。

3.12 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 infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	X			华为云已制定基础设施及虚拟化安全管理策略和流程。
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	X			华为云已制定基础设施及虚拟化安全管理策略和流程，并且每年对该策略流程进行审阅和更新。

IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	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。 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。 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-03.1	Are communications between environments monitored?	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-03.2	Are communications between environments encrypted?	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。
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	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-03.4	Are network configurations reviewed 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。
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	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-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	X			为保证平台安全，华为云对主机操作系统进行最小化裁剪并对服务做安全加固。同时，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(PAM – Privilege Access Management)，对其所执行的各项运维运营操作实行全面的日志审计。
IVS-05.1	Are production and non-production environments separated?	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-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	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-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	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-08.1	Are high-risk environments identified and documented?	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-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based 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。

3.13 LOG 日志记录和监控

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	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。

LOG-01.2	Are policies and procedures reviewed and updated 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。
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	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，以确保支撑网络安全事件回溯和合规。该日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间超过180天，90天内可以实时查询。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。
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	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。 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。

LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	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。 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。
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	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。
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	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，以确保支撑网络安全事件回溯和合规。
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	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，以确保支撑网络安全事件回溯和合规。
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	X			华为云使用NTP4.2.8协议对系统内的时间进行同步。
LOG-07.1	Are logging requirements for information meta/ data system events established, documented, and implemented?		X		华为云由各个业务部门分别制定符合其业务所需的审计日志记录范围。

LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?		X		华为云由各个业务部门分别制定符合其业务所需的审计日志记录范围。
LOG-08.1	Are audit records generated, and do they contain relevant security information?	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。
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	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。
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	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。 华为云数据加密服务DEW中支持客户授权华为云托管私钥。 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。
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	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。

LOG-12.1	Is physical access logged and monitored using an auditable access control system?	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。
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	X			华为云提供的云监控服务（CES - Cloud Eye Service）可帮助客户实时监控服务器的运行状态以及云上资源的使用情况，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。华为云提供的云日志服务（LTS – Log Tank Service）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务，客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该IP地址的请求。
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	X			华为云提供的云监控服务（CES - Cloud Eye Service）可帮助客户实时监控服务器的运行状态以及云上资源的使用情况，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。华为云提供的云日志服务（LTS – Log Tank Service）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务，客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该IP地址的请求。

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	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	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。 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-01.2	Are policies and procedures reviewed and updated 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。
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	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。 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-02.2	Are policies and procedures for timely management of security incidents reviewed and updated 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。

SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	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。
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	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。
SEF-05.1	Are information security incident metrics established and monitored?	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。 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。

SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	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-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	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-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	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-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	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。

3.15 STA 供应链管理、透明度和问责制

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	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	X			华为云按照公有云、全栈专属云、混合云分别制定了不同的安全责任共担模型。
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	X			华为云每年对其制定的安全责任共担模型进行审阅，并按需更新。
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	X			华为云按照公有云、全栈专属云、混合云分别制定了不同的安全责任共担模型。
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	X			华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不但包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类各项云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。 详情见华为云安全白皮书。

STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	X			华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不但包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类各项云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。 详情见华为云安全白皮书。
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	X			华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不但包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类各项云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。 详情见华为云安全白皮书。

STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	X			华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不但包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类各项云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。 详情见华为云安全白皮书。
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	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、软件安装、软件退出等环节，均实施严格的管控。
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	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 service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? Scope, characteristics, and location of business relationship and services offered Information security requirements (including SSRM) Change management process Logging and monitoring capability Incident management and communication procedures Right to audit and third-party assessment Service termination Interoperability and portability requirements Data privacy		X		“华为云用户协议”包含以下条款： 1. 业务关系和提供服务的范围、特点和位置 2. 信息安全要求（包括SSRM） 3. 记录和监视能力 4. 事件管理和沟通规程 5. 服务终止 6. 数据隐私
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed 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-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	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-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	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-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	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-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	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。

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	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	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-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	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-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	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-02.2	Are asset management and malware protection policies and procedures reviewed and updated 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。

TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	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-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	X			华为云每周更新检测工具、威胁特征和攻击指标。
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	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。
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	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-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?		X		华为云当前每三个月对资产进行漏洞检测。
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	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-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?		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。 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-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	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。

3.17 UEM 通用端点管理

编号	一致性评估问题	回答			华为云的回应
		是	否	不适用	

UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	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。
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated 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。
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	X			华为云制定并实施桌面终端服务软件标准，办公计算机只使用其中定义的标准操作系统和软件。
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	X			华为云明确要求需要确认终端设备与操作系统和应用的兼容性。
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	X			根据ISO 27001标准，华为云对信息资产进行分类并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。

UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	X			华为云已制定并实施资产的使用规则，包括管理原则、相关人员职责、办公计算机安全要求、办公网络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	X			华为云都通过统一途径对终端资产进行管理，终端均被指了自动锁屏的策略。
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	X			华为云终端操作系统、补丁及应用的变更，均需要通过其内部制定的变更管理流程。
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	X			华为云使用业界普遍认可的强加密算法对平台内数据进行加密，在传输过程中使用加密协议保障数据安全。
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	X			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。 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，意识教育的内容包括防范恶意软件。
UEM-10.1	Are software firewalls configured on managed endpoints?	X			华为云统一配置终端上的软件防火墙，普通用户无法修改。

UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	X			华为云终端设备均安装了DLP数据防泄漏软件，并由公司统一配置管理。
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?			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。
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	X			华为云统一管理终端设备，可实现软件、数据和策略的远程停用、删除和锁定。
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?			X	华为云不允许第三方终端访问华为云的资产。

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
2022年4月	2.0	合格要求更新
2020年9月	1.0	首次发布