华为云新加坡网络安全监管要求遵从性指南

文档版本 1.0

发布日期 2025-09-19

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 背景与发布目的

在科技发展的浪潮中，越来越多的组织在逐渐寻求业务转型并希望借助先进信息技术以降低成本、提升运营效率、实现业务模式的创新。不过，在信息技术得到广泛运用的同时，网络安全事件也随之不断出现。为了规范对关键信息基础设施的运用， 巩固与提升国家网络安全水平，新加坡国会，新加坡网络安全局（CSA）以及新加坡资讯通信媒体发展局（IMDA）发布了一系列网络安全监管要求。

华为云作为云服务供应商，致力于协助客户满足这些监管要求，持续为客户提供符合监管要求的云服务及业务运行环境。本文将针对客户在使用云服务时通常需遵循的新加坡网络安全监管要求，详细阐述华为云将如何协助其满足这些监管要求。

1.2 适用的网络安全监管要求简介

新加坡国会是新加坡共和国按照立法、行政、司法权力分立的原则组织的国家机构，负责制定法律，履行批判、质询、监督政府行为与政策，并审查国家财政状况的职责。

- **《网络安全法》：**新加坡国会于 2018 年 2 月 5 日发布，与 2024 年 7 月 5 日发布的《网络安全（修订）法》组合成最新的网络安全法案内容。该法案建立了国家网络安全监督与维护的法律框架。该法案要求或授权采取措施预防、管理和应对网络安全威胁和事件，并规范了关键信息基础设施所有者，临时网络安全关注系统，特殊网络安全利益实体，第三方所有关键信息基础设施的指定供应商，主要数字基础设施服务提供商，以及与之相关的事项。
- **《计算机滥用法》：**新加坡国会于 1993 年 8 月 30 日发布，并在 2024 年 2 月 8 日发布最新修订版。该法案规定了保护计算机免受未经授权的访问或修改，防止滥用国家数字身份服务，以及处理与之相关的事项。

新加坡网络安全局（Cyber Security Agency of Singapore，以下简称 “CSA”） 成立于 2015 年，负责统筹管理政府各部门的网络安全事务，监督新加坡网络安全政策，网络安全产业。CSA 旨在保障新加坡网络空间的安全，支撑国家安全、推动数字经济。

- **《关键信息基础设施网络安全行为准则》：**CSA 于 2022 年 7 月 4 日发布，该行为准则作为《网络安全法》配套的行为准则，由 CSA 制定的技术标准和操作指

南，旨在为关键信息基础设施所有者提供具体的网络安全要求，包括风险评估、事件报告、安全审计和防御措施等。

- **《事件响应检查表》**：CSA 于 2021 年 4 月 11 日发布，该表是围绕美国国家标准与技术研究院 （NIST） 开发的 IPDRR（识别、保护、检测、响应、恢复）框架构建，旨在指导组织对网络事件的准备、响应和恢复。

新加坡资讯通信媒体发展局（Infocom Media Development Authority，以下简称“IMDA”） 负责发展和监管资讯通信及媒体行业，旨在力于发展和监管资讯通信及媒体行业，促进新加坡的数字经济和媒体产业的繁荣。

- **《数据中心韧性和安全性咨询指南》**：IMDA 于 2025 年 2 月 25 日发布，该指南为数据中心为运营商提供了框架，旨在建立一个强大的业务连续性管理系统，以最大限度地减少服务中断并确保客户的高可用性。该指南包括制定业务连续性政策、建立风险控制流程、实施持续改进机制，以及应对网络安全风险的具体防护措施。

- **《云服务韧性和安全性咨询指南》**：IMDA 于 2025 年 2 月 25 日发布，该指南为云服务涵盖 7 类措施以提升云服务的安全性和韧性。该指南建议云服务提供商实施的措施涉及安全测试、用户访问控制、适当的数据治理以及灾难恢复规划等领域。

新加坡信息技术标准委员会（The Information Technology Standards Committee，以下简称 “ITSC”） 负责制定在缺乏国际或行业标准的情况下所需的标准，并推荐采用国际标准作为新加坡标准。ITSC 旨在制定和推动新加坡标准以满足国家信息通信需求及创新要求。

- **《TR 62 : 2018 云中断事件响应指南》**：ITSC 于 2018 年 4 月 20 日发布，通过规范云服务中断事件的响应流程，进一步强化新加坡在业务连续性管理与灾难恢复计划方面的实施要求。旨在提升智能国家中云服务提供商的透明度、信任和弹性。该指南侧重于基础设施或系统故障以及环境问题（例如洪水、火灾）直接相关的云中断，但不包括网络安全和恶意行为。

1.3 名词定义

- **华为云**

  华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。

- **客户**

  指与华为云达成商业关系的注册用户。

- **云计算或云**

  是指用一种模式，用于通过自助服务配置和按需管理，使网络能够访问可扩展且弹性的可共享物理或虚拟资源池（例如服务器、操作系统、网络、软件、应用程序和存储设备）。

- **关键信息基础设施（Critical information infrastructure, CII）**

  是指新加坡持续提供基础服务所必需的计算机或计算机系统，其一旦遭受损失或危害将对新加坡境内基础服务的可用性造成严重影响。

- **所有者**

  是指服务商拥有的关键基础信息设施、第三方拥有的关键信息基础设施或临时网络安全关注系统的法律所有者，若该设施或系统由多人共同拥有，则包括所有共同所有者。

- **负责第三方所有关键信息基础设施的指定供应商（Designated provider responsible for third-party-owned critical information infrastructure）**

  是指提供基本服务所必需的计算机系统（无论位于新加坡境内或境外），一旦丢失或遭到破坏，将对新加坡境内该关键服务的可用性造成严重影响。

- **主要数字基础设施服务提供商（Major foundational digital infrastructure service provider）**

  是指提供数字基础设施服务的关键计算机或系统（无论这些服务位于新加坡境内还是境外），其服务一旦丢失或受损，可能会导致大量依赖该数字基础设施服务的企业或组织在新加坡境内或境外的运营出现中断或下降。

- **临时网络安全关注系统（System of temporary cybersecurity concern）**

  是指在短期内面临高风险、可能遭受未经授权网络攻击的系统，一旦系统丢失或受损，将严重影响新加坡的国家安全、国防、外交、经济、公共卫生、公共安全或公共秩序。

- **特殊网络安全利益实体（Entity of special cybersecurity interest）**

  其控制下的计算机或计算机系统中存储敏感信息，或使用其控制下的计算机或计算机系统执行关键功能，一旦这些功能受到干扰，将严重影响新加坡的国防、外交、经济、公共卫生、公共安全或公共秩序。

- **网络安全事件**

  是指未经合法授权，通过计算机或计算机系统实施的行为或活动，该行为或活动危及或对该计算机或计算机系统的网络安全，或对其他计算机或计算机系统的网络安全产生不利影响。

2 华为云安全合规

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

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

华为云部分标准类认证/鉴证示例：

认证	描述
ISO27001:2022	ISO27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO27017:2015	ISO27017 是针对云计算信息安全的国际认证。ISO27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO27018:2019	ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
TL 9000& ISO 9001	ISO 9001 是 ISO 9000 族标准所包括的一组质量管理体系核心标准之一，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。 TL 9000 是一个建立在 ISO9001 基础上的，由全球电信业优质供应商联盟（QuEST Forum）针对全球信息和通讯技术（ICT）行业特定设计的、为 ICT 产品和服务供方提供的一套通用的质量管理体系要求。它包括了 ISO9001 的所有要求，ISO9001 将来的任何改动也会导致 TL9000 的改动。 华为云取得了 ISO9001 / TL9000 认证证书，表明华为云可以为您提供更快，更好和更具成本效益的服务。
ISO20000-1:2018	ISO20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的 IT 服务来满足客户和业务的需求。
ISO22301:2019	ISO22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
CSA STAR 认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水

	平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
ISO27701:2019	ISO27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS10012 是 BSI 发布的个人信息数据管理体系标准，BS10012 认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
ISO 29151:2017	ISO29151 是国际个人身份信息保护实践指南。ISO29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
PCI DSS	支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
PCI 3DS	PCI 3DS 标准，旨在保护执行特定 3DS 功能或者存储 3DS 数据的 3DS 环境，支持 3DS 的实施。PCI 3DS 的评估对象为 3D 协议执行环境，包括访问控制服务器、目录服务器或 3DS 服务器功能；以及 3D 执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估 3D 协议执行环境的过程、流程、人员管理等。
ISO 27799:2016	ISO/IEC 27799 是专注于医疗行业的信息安全管理体系，为医疗行业和其相关机构提供了关于如何更好地保护个人健康信息的保密性、完整性、可审计性和可用性的指导。 华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。
ISO 27034	ISO/IEC 27034 是国际标准化组织 ISO 通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得 ISO/IEC 27034 认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。
SOC 审计报告	SOC 审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。

3 华为云责任共担模型

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

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

在监管要求可能适用于客户内容的情况下，“责任共担”模型帮助华为云和客户双方理解各自角色以及责任。

图3-1 华为云责任共担模型

华为云的责任：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在 PaaS、SaaS 场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。

客户的责任：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

在 On-prem 场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。

在 IaaS 场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。

在 PaaS 场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。

在 SaaS 场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多华为云基础设施的信息，参见华为云官网“全球基础设施”。

图4-1 新加坡 Region 和可用区（AZ）示例

5 华为云如何遵从及协助客户满足《网络安全法》

新加坡国会于 2018 年 2 月 5 日发布了《网络安全法》，与 2024 年 7 月 5 日发布了《网络安全（修订）法》组合成最新的网络安全法案内容，该法案建立了国家网络安全监督与维护的法律框架。该法案要求或授权采取措施预防、管理和应对网络安全威胁和事件，并规范了关键信息基础设施所有者，临时网络安全关注系统，特殊网络安全利益实体，第三方所有关键信息基础设施的指定供应商，主要数字基础设施服务提供商，以及与之相关的事项。

当客户遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

5.1 关键信息基础设施

编号	具体控制要求	客户关注点	华为云的内部实践
14. 报告关键信息基础设施等网络安全事件的责任	关键信息基础设施所有者知悉以下任一事件发生后，必须按规定格式和方式在规定期限内向专员报告： (a) 涉及该关键信息基础设施的法定网络安全事件； (b) 涉及所有者控制下且与该关键信息基础设施互联或通信的任何计算机或计算机系统的法定网络安全事件； (c) 专员通过书面指示特别规定的、涉及该关键信息基础设施的其他类型网络安全事件。 关键信息基础设施所有者必须根据相关行为准则的要求，建立用于检测针对关键	若客户被认定为关键信息基础设施所有者，客户应在知晓严重网络安全事件后，按规定时间、方式和格式向新加坡网络安全专员报告。 客户必须建立有效机制来监测 CII 的网络安全威胁和事件，满足相关行为准则要求。	华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。 华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。 华为云设置 7*24 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时

	信息基础设施的网络安全威胁和事件的机制与流程。		知会客户，同时执行应急预案及恢复流程，降低业务影响。
15. 关键信息基础设施的网络安全审计和风险评估	关键信息基础设施所有者必须： (a) 自根据发出通知之日起，至少每两年一次（或根据专员在特定情况下指示的更高频率），由专员批准或指定的审计机构，对该关键信息基础设施是否符合本法规定以及相关实务守则和绩效标准进行合规审计； (b) 自根据第发出通知之日起，至少每年一次，以规定形式和方式对该关键信息基础设施开展网络安全风险评估。 关键信息基础设施的所有者必须在完成审计或网络安全风险评估后 30 天内，向专员提供审计或评估报告的副本。	若客户被认定为关键信息基础设施所有者， 客户必须至少每两年进行一次（或专员可能指示的更高频率下）网络安全合规审计，每年至少进行一次（或专员可能指示的更高频率下）网络安全风险评估，并在完成后 30 天内向新加坡网络安全专员提交报告。	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。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议，同时保留审计记录免受未经授权的访问。 华为云会安排专人积极配合客户发起的审计要求。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSASTAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。 华为云各业务团队根据要求定期执行信息安全风险评估，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审，确保符合公司风险管理要求。风险评估报告完成后由高级管理层进行审批。
16. 网络安全演练	(1) 专员可组织开展网络安全演练，以检验不同关键信息基础设施所有者应对重大网络安全事件的准备状态。 (2) 关键信息基础设施所有者在收到专员的书面指令后，必须按要求参加网络安全演练。	若客户被认定为关键信息基础设施所有者，客户应配合网络安全专员组织的网络安全演练，确保能有效应对重大网络安全事件。客户需认真参与演练，检验并提升应急响应能力。	华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。同时，华为云使用eBackup 系统对备份数据进行循环冗余校验以确保备份数据的完整性和可用性，校验失败则无法成功进行备份。此外，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。

5.2 负责第三方所有关键信息基础设施的指定供应商

编号	具体控制要求	客户关注点	华为云的内部实践
16F. 供应商须确保第三方所有关键信息基础设施符合规定标准	负责第三方所有关键信息基础设施的指定供应商必须从该第三方所有关键信息基础设施的所有者处取得具有法律约束力的承诺，即该所有者将确保在该第三方所有关键信息基础设施方面维持任何适用的、与网络安全相关的规定技术或其他标准。	若客户被认定为第三方所有关键信息基础设施的所有者，应向指定供应商提供具有法律约束力的承诺，确保在其设施中持续执行适用的网络安全技术或标准。	华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域致力于为客户打造安全、可信的服务，为客户业务赋能增值、保驾护航。 客户对华为云的审计和监督权益以及法规对客户的要求会根据实际情况在与客户签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人。
16H. 第三方所有关键信息基础设施所有权变更	负责第三方所有关键信息基础设施的指定供应商必须从其负责网络安全的第三方所有关键信息基础设施的所有者处取得具有法律约束力的承诺，即该所有者将在该第三方所有关键信息基础设施的受益所有权或法律所有权（包括该所有权的任何股份）发生任何变更之日起不迟于7天内通知该供应商。 当不再符合以上的条件时，负责第三方所有关键信息基础设施的指定供应商必须在该情况变更之日起不迟于7天内将该情况变更通知专员。	若客户被认定为第三方所有关键信息基础设施的所有者，应向指定供应商做出具有法律效力的承诺，并在其关键信息基础设施的受益或法律所有权（含股份）变更时，于7天内通知指定供应商。	客户对华为云的审计和监督权益以及法规对客户的要求会根据实际情况在与客户签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人。
16I. 报告与第三方所有关	负责第三方所有关键信息基础设施的指定供应商必须从其负责网络安全的第三方所有关键信息基础设施的所有者处取得	若客户被认定为第三方拥有关键信息基础设施的所有者，应作出具有法律效力的承	华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行

键信息基础设施相关的网络安全事件的义务	具有法律约束力的承诺，即该第三方所有关键信息基础设施的所有者将在其知悉以下任何一项发生后的规定期限内通知该供应商： (a) 与该第三方所有关键信息基础设施相关的规定网络安全事件； (b) 与所有者控制或供应商控制下、并与该第三方所有关键信息基础设施相互连接或进行通信的任何计算机或计算机系统相关的规定网络安全事件； (c) 与供应商控制下、但不属于(b)段所述的任何其他计算机或计算机系统相关的规定网络安全事件； (d) 专员以书面指令通知负责第三方所有关键信息基础设施的指定供应商的、与该第三方所有关键信息基础设施相关的任何其他类型的网络安全事件。 负责第三方所有关键信息基础设施的指定供应商必须建立相关机制和流程，以便按照任何适用的操作规范，知悉与该第三方所有关键信息基础设施相关的任何网络安全威胁和事件。	诺，在发现与关键信息基础设施或相关互联系统的规定网络安全事件后，于规定期限内通知指定供应商。	应急预案及恢复流程，降低业务影响。 为配合客户满足合规要求，华为云内部制定了完善的事件管理流程，清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 同时，针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。
16J. 对第三方所有关键信息基础设施进行网络安全审计和风险评估	负责第三方所有关键信息基础设施的指定供应商必须从其负责网络安全的第三方拥有关键信息基础设施的所有者处取得具有法律约束力的承诺，即该第三方拥有关键信息基础设施的所有者将： (a) 自根据发出通知之日起，至少每两年一次（或在专员通过书面通知供应商要求的特定情况下以更高频率）委托由专员批准的审计员对该第三方所有关键信息基础设施在遵守任何与网络安全相关的、应适用于并应保持的规定技术或其他标准方面进行审计； (b) 自根据发出通知之日起，至	若客户被认定为第三方拥有关键信息基础设施的所有者，应定期进行由专员批准的网络安全审计（至少每两年一次）和风险评估（至少每年一次）频率开展网络安全审计和风险评估，使用专员批准的审计员或服务专业人员，在完成后30天内向指定供应商提交报告，并按指示配合开展额外或补充的审计和评估。	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。审计结果交由管理层进行审阅并对整改情况进行跟进。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议，同时保留审计记录免受未经授权的访问。 业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、 最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服

	少每年一次，以规定的形式或方式对该第三方所有关键信息基础设施进行网络安全风险评估； (c) 在完成(a)段所述审计或(b)段所述评估（视情况而定）后不超过30天，将该审计报告和该网络安全风险评估报告的副本提交给供应商； (d) 根据供应商依照专员的指示要求，重新执行(a)段所述审计的任何部分； (e) 根据供应商依照专员的指示要求，委托由专员批准的审计员对该第三方所有关键信息基础设施进行审计； (f) 根据供应商依照专员的指示要求，采取进一步措施评估该第三方所有关键信息基础设施的网络安全水平，或委托由专员批准的网络安全服务专业人员对该第三方所有关键信息基础设施进行另一项网络安全风险评估； (g) 根据供应商依照专员的指示要求，进行除(a)段和(b)段所述审计或网络安全风险评估之外的另一项审计或网络安全风险评估。 负责第三方所有关键信息基础设施的指定供应商必须从所有者处取得每份审计报告和每份网络安全风险评估报告。 负责第三方所有关键信息基础设施的指定供应商必须在收到所有者提交的审计报告或网络安全风险评估报告后不超过14天，将该审计或评估的报告副本提交给专员。		务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人在网络安全风险评估及报告披露方面对华为云的要求。。

16K. 通知具有法律约束力承诺重大变更的义务	如果由负责第三方所有关键信息基础设施的指定供应商，为符合第16E(1)、16F(1)、16H(1)、16I(1)或16J(1)条的要求而取得的具有法律约束力的承诺发生重大变更，该指定供应商必须在变更作出后不超过14天内，将该变更通知专员。	若客户被认定为第三方所有关键信息基础设施的所有者，应在关键网络安全承诺作出重大变更时，在14天内主动通知第三方所有关键信息基础设施的指定供应商。	客户对华为云的审计和监督权益以及法规对客户的要求会根据实际情况在与客户签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人。

5.3 临时网络安全关注系统的指定

编号	具体控制要求	客户关注点	华为云的内部实践
17F. 临时网络安全关注系统网络安全事件的报告义务	临时网络安全关注系统的所有者必须按照规定的形式和方式，在知悉以下事件发生后的规定期限内向专员报告： (a) 该临时网络安全关注系统发生规定的网络安全事件； (b) 所有者控制范围内与该系统互连或通信的任何计算机或计算机系统发生规定的网络安全事件； (c) 所有者供应商控制范围内与该系统互连或通信的任何计算机或计算机系统发生规定的网络安全事件。 临时网络安全关注系统的所有者必须按照适用的行为准则要求，建立用于检测该系统网络安全威胁和事件的机制与流程。	若客户被认定为临时网络安全关注系统的所有人，必须在规定时间内向专员报告符合条件的网络安全事件（包括自身系统、互连系统及供应商系统的事件），并建立检测威胁和事件的机制与流程。	华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。 为配合客户满足合规要求，华为云内部制定了完善的事件管理流程，清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 同时，针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。

5.4 特殊网络安全利益实体

编号	具体控制要求	客户关注点	华为云的内部实践
18F. 特殊网络安全利益实体网络安全事件的报告义务	特殊网络安全利益实体在知悉其特殊网络安全关注系统或控制范围内的其他计算机系统发生规定的网络安全事件后，必须按照规定的形式和期限向专员报告，若该事件： (a) 导致实体数据的可用性、机密性或完整性遭到破坏；或 (b) 对实体的业务运营造成重大影响。 特殊网络安全利益实体必须按照适用的行为准则要求，建立用于检测特殊网络安全关注系统网络安全威胁和事件的机制与流程。	若客户被认定为特殊网络安全利益实体，应建立检测其系统及相关计算机系统的网络安全威胁与事件的机制和流程，并在知悉任何可能破坏数据可用性、机密性或完整性，或对业务运营造成重大影响的事件后，按照规定形式和期限向专员报告。	华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。 为配合客户满足合规要求，华为云内部制定了完善的事件管理流程，清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 同时，针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。

5.5 主要数字基础设施服务提供商

编号	具体控制要求	客户关注点	华为云的内部实践
18M. 主要数字基础设施服务提供商网络安全事	主要数字基础设施服务提供商必须按照法定形式和时限，在知悉下列任一情形发生后立即向网络安全专员报告： (a) 涉及重大基础数字基础设施或该提供商管控范围内其他计算机系统的法定网络安全事	客户应确保自身使用的系统和业务运行具备及时监测、发现及配合报告重大网络安全事件的能力，以便在事件影响云服务交付或自身运营时，能	华为云建立了完善的事件通知与管理体系。 首先，基于业务连续性管理要求，制定了危机沟通策略，定义了突发事件下的沟通对象、内容和工具，并配备专人与行业机构、风险合规组织、地方当局和

件报告义务	件，且该事件已导致其被指定的基础数字基础设施服务在新加坡境内的持续服务交付出现中断或质量降级； (b) 涉及重大基础数字基础设施或该提供商管控范围内其他计算机系统的法定网络安全事件，且该事件已对该提供商在新加坡境内的商业运营造成重大影响。 主要数字基础设施服务提供商必须依照相关行为准则的规定，建立健全的网络安全威胁与事件监测机制及处置流程，专门用于保障重大基础数字基础设施的安全运行。	快速与服务提供商协同应对。	监管机构建立联络点，确保及时获取外部支持。 其次，华为云内部制定了完善的事件管理流程，清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 同时，针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。 华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。

6 华为云如何遵从及协助客户满足《CII 网络安全行为准则》

CSA 于 2022 年 7 月 4 日发布了《关键信息基础设施网络安全行为准则》，作为《网络安全法》配套的行为准则，由 CSA 制定的技术标准和操作指南，旨在为关键信息基础设施所有者提供具体的网络安全要求，包括审计要求、治理要求、识别要求和防护要求等。

当客户遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

6.1 审计要求

编号	具体控制要求	客户关注点	华为云的内部实践
2.1 审计发现问题的整改	若审计发现关键信息基础设施所有者（CIIO）存在不符合《网络安全法》要求或根据《网络安全法》颁布的行为准则、绩效标准的情形，除非专员另行书面指示，CIIO 应在收到审计报告之日起 30 个工作日内向专员提交审计发现问题整改计划。 经与 CIIO 后，若专员认为必要，可要求关键信息基础设施所有者修订其审计发现问题整改计划，并在专员规定的时限内重新提交修订后的整改计划。 CIIO 应按照整改计划规定的时间节点，自行承担费用实施整改措施直至所有整改工作完成，并达到专员认可的标准。每项整改措施完成后，CIIO 应及时向专员报告进展。	若客户被认定为关键信息基础设施所有者，当审计发现违反《网络安全法》或相关规范，须在收到报告后 30 个工作日内向专员提交整改计划，并按专员要求进行修订。关键信息基础设施所有者应实施整改措施，并在每项措施完成后向专员报备进展。	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。审计结果交由管理层进行审阅并对整改情况进行跟进。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议，同时保留审计记录免受未经授权的访问。 华为云实行严格的审计活动，在推动网络安全流程和标准落地方面上起着关键的作用。华为建立了专门的安全审计团队，审计每年进行一次，重点关注华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上的风险，确保审计发现得到整改。 客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的

			要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。

6.2 治理要求

编号	具体控制要求	客户关注点	华为云的内部实践
3.1 领导与监督	关键信息基础设施所有者（CIIO）应当以书面形式明确保障关键信息基础设施（CII）网络安全的相关岗位职责，并将每项职责分配给其内部人员或为其服务的人员。 CIIO应当确保其董事会（或同等治理机构）中至少有一名具备网络安全知识和意识的成员，负责监督CII面临的网络安全风险，并就如何管理系统性网络安全风险向高级管理层提供指导。 CIIO 应当确保其高级管理层中至少有一名具备网络安全知识和意识的成员，负责管理 CII 面临的网络安全风险，并确保各项网络安全措施得到有效实施。	若客户被认定为关键信息基础设施所有者，客户应明确网络安全相关角色、职责和审批权限，确保董事会和高级管理层中至少有一名具备网络安全知识的成员，负责监督和管理网络安全风险。	华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。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。 华为云持续监控外部监管环境的变化，明确最新外部监管要求，对相关的信息安全策略、流程及其角色和职责进行审查和更新，对识别到的法律法规的变化及时调整到内部安全要求中，确保控制的适当性和执行的有效性。华为将网络安全要求融入到任职资格标准中。员工在任职晋升过程中需要学习相应的网络安全课程，通过相应的网络安全技能考试，提升自身网络安全能力。
3.2 风险管理	关键信息基础设施所有者（CIIO）应当建立并实施网络安全风险管理框架。 CIIO应当在网络安全风险评估方法中包含风险识别、风险分析、风险评估、风险应对的步骤。 CIIO应当为每个CII建立并持续更新风险登记册。风险登记册应当记录CII面临的所有网络安全风险信息，包括通过网络安全风险评估识别的风险。	若客户被认定为关键信息基础设施所有者，客户应制定风险管理框架、识别关键资产与网络威胁、开展定期风险评估、设置风险偏好与响应机制，并将风险情况及时报告高层管理人员。	华为云建立了信息安全风险管理规范，明确风险管理应遵循的关键流程、风险管理范围、风险管理相关责任部门及风险管理中应遵循的标准，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。华为云各业务团队根据要求定期执行信息安全风险评估。 华为云各业务团队根据要求定期执行信息安全风险评估，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审，确保符合公司风险管理要求。风险评估报告完成后由高级管理层进行审批。风

	CIIO 须确保风险登记册中列明的所有网络安全风险定期接受审查与监控。		险评估的主要流程如下： ● 风险管理人员识别各业务场景中所涉及的固有风险，基于华为云面临的威胁和脆弱性进行风险评估； ● 基于固有风险清单，结合已有的风险管控措施，输出残余风险清单，并将风险及时录入风险管理平台，包括风险描述、所属领域、风险等级、风险来源等； ● 基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。风险评估报告完成后由高级管理层进行审批。华为云为配合客户向CITC 报告主要的网络安全风险以及补救计划，华为云会遵从与客户订的协议中约定的要求，会安排专人积极配合客户的需求。 风险管理人员识别各业务场景中所涉及的风险，将风险及时录入风险管理平台，包括风险描述、所属领域、风险等级、风险来源等形成风险清单，并利用风险管理平台对风险进行自动跟踪与监控。
3.3 政策、标准、指南与程序	关键信息基础设施所有者（CIIO）应制定并实施用于管理网络安全风险和保护关键信息基础设施（CII）免受网络安全威胁的政策、标准、指南和程序。 CIIO应当至少每12个月根据当前CII网络运行环境和网络安全威胁态势对政策、标准、指南和程序进行一次审查。首次审查应在相关政策、标准、指南和程序制定后不超过12个月内完成。 CIIO 必须确保实际操作和实施与政策、标准、指南和程序保持一致。如存在差异，应及时予以解决。	若客户被认定为关键信息基础设施所有者，客户需要制定清晰的网络安全政策、标准和流程，并每年审查一次，确保员工和供应商都了解并按照这些规定执行。	华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批，员工可根据授权查看已发布的信息安全政策和程序。同时，华为云针对公司政策、文化等方面每年定期开展员工培训。 秉承华为网络安全战略和规范，华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。 华为云至少每年审查一次网络安全管理策略和流程，并根据需要予以更新，以反映业务目标或风险环境的变更情况。政策及流程的变更需要获得高级管理层的审批。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议。

3.5 网络安全设计原则	关键信息基础设施所有者（CIIO）必须在人员、流程和技术方面采用纵深防御，最小权限，职责分离原则。 CIIO还应尽可能在人员、流程和技术方面采用多样化防御，零信任的原则。	1.若客户被认定为关键信息基础设施所有者，客户需要在关键系统设计和管理中用好“纵深防御”、“最小权限”、“职责分离”等原则，还要考虑用不同技术和实施零信任来提高安全性。 2. 华为云的统一身份认证服务（IAM）为客户提供云上资源访问控制。使用IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安	华为云参照业界实践并结合自身经验沉淀及业务特性从三层技术架构设计 Web应用程序，包括基础层（application layer）、平台层（platform layer）、应用层（foundation layer），实现应用的安全设计与维护，确保高内聚，低耦合。此外，华为云制定了web应用开发规范，结合多维度的安全开发原则，实现深度防御的目的。 华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。在权限复核与调整方面，华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。 华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面，确保业务能在恢复时间目标内恢复到可接受水平。 华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。另外，各可用区有各自独立的UPS和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。此外，用户可充分利用这些地域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下（包括自然灾害和系统故障）系统都能连续运行。 华为云建立了基于零信任的身份与访问管理端到端生命周期治理体系，基础设施和云服务等均基于员工个人以及工作负载的身份以及动态策略进行认证和细粒度授权。

		全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过云审计服务（CTS）作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。	
3.6 变更管理	关键信息基础设施所有者应建立变更管理流程，用于对关键信息基础设施实施的所有变更进行识别、审批、实施和验证。	若客户被认定为关键信息基础设施所有者，客户应有一套清晰的流程来管控关键系统的任何修改，做到变更有记录、有审批、有验证。	华为云制定了变更管理的管理规定和变更流程，定义了涵盖变更实施前、实施中及实施后应遵循的网络安全要求，以防止未授权变更。例如，变更前，各项变更均需通过多个环节的审核；变更实施中，会通过日志记录、操作监控及双人操作等方式确保变更安全实施，并确保变更过程可追溯；变更后，对变更实施专人验证，确保变更达到预期效果，不会造成网络安全风险。
3.7 云计算系统与服务的使用	关键信息基础设施所有者（CIIO）应始终对关键信息基础设施（CII）的网络安全监督及风险管理承担主体责任，即使该CII全部或部分部署于云计算系统。 CIIO拟将CII全部或部分部署于云计算系统时，无论考虑采用何种部署模式（如公有云、私有云或混合云）或服务模式（如软件即服务、平台即服务或基础设施即服务），均应事先向专员报备。 除非满足以下条件，否则CIIO不得将CII全部或部分部署于云计算系统： (a) 已完成云计算系统部署方案的网络安全风险评估，并确保已识别风险得到充分管控；	1. 客户将关键信息基础设施部署在云端前，必须先完成针对云计算系统实施计划相关风险的网络安全风险评估，并将报告提交给新加坡网络安全局专员，获得认可后才能实施。 2. 客户需确保服务提供商在新加坡有指定授权代表以接收通知或法律文书。	华为云会安排专人积极配合客户发起的审计要求和尽职调查。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSASTAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。此外，华为云将积极配合机构满足监管机构相关的要求。 华为云遵循ISO27001、ISO20000、ISO22301等国际标准建立完善的信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。 华为云在各个国家当地设定了授权人员，代表服务提供商接收与关键信息基础设施所有者服务相关的任何通知或法律文书。

	(b) 经CIIO正式接受的风险评估报告，须在完成后30日内提交专员审查；以及 (c) 若专员认为评估存在缺陷，CIIO应自担费用并在规定时限内完成整改直至专员认可。 当 CIIO 聘用或拟聘用云计算服务商协助实施 CII 云端部署时，应确保服务商在新加坡境内指定授权代表，代为接收与 CII 服务相关的法律文书及通知。		
3.8 外包与供应商管理	CIIO应建立监督流程，对所有被外包的职能、活动或运营保持监督，以尽量减少因外包带来的网络安全风险。 CII应在其与外部方签署的协议中纳入有助于确保CII网络安全并减少或缓解与外包相关的网络安全风险（包括外部方对CII及其运营、处理、存储、通信和其他功能的访问所带来的风险）的条款。 CIIO应建立流程，以验证外部方是否遵守以上要求的条款及协议中其他与网络安全相关的条款。 CIIO 应确保在出现新的法律或监管要求时，能够与外部方重新协商的协议条款。	客户需建立对外包管理流程，对所有外包功能活动等进行监督，并在与外包的合作协议中加入访问权限类型、安全义务和审计权等条款，同时建立验证流程以验证外部机构是否切实履行相关要求，并保留依据新法规调整合同的权利。	华为云提供了线上的《华为云用户协议》以及华为云《云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。在华为云内部，华为云建立了正式的采购审核流程，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。合同与服务协议中明确了双方的责任和义务、服务内容及服务水平等要求，同时通过保密协议对违反保密性的条款进行了约束。华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。

6.3 识别要求

编号	具体控制要求	客户关注点	华为云的内部实践
4.1 资产管理	关键信息基础设施所有者（CIIO）应建立资产识别机制和流程，对所有关键信息基础设施（CII）资产进行清点并建立资产清单。 CIIO 应在任何 CII 资产或清单记录信息发生变更时，及时更新该资产清单。	1. 客户必须建立并持续更新一个完整资产清单，涵盖硬件、软件、依赖关系、网络连接、云服务使用、外包供应商、物理位置等详细信息，并在任何资产或记录变更时及时更新该清	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享。 华为云定期对华为云的硬件、软件、数据、人员和服务进行识别。华为云通过资产管理系统（Cloud Asset Management）实

		单。 2. 华为云为客户提供统一的管理界面，以供客户查询和管理已购买的华为云资源。客户还可以使用华为云提供的企业主机安全（HSS）服务的资产管理功能，对其资产进行统一管理。建立并维护按业务关键性分类的全面 IT 资产清单。	时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。华为云并使用 IPAM 对 IP 资源进行统一的管理。同时，华为云平台部署了 HSP 主机安全平台套件，对平台资产进行网络安全防护。

6.4 防护要求

编号	具体控制要求	客户关注点	华为云的内部实践
5.1 访问控制	关键信息基础设施所有者（CIIO）应确保对关键信息基础设施（CII）及其内部各组成部分的访问权限仅限于经授权的人员、活动、流程和设备。 CIIO应根据CII的网络安全风险特征，建立与CII及其内部各组成部分访问权限相匹配的授权和认证控制机制。 CIIO应确保所有供应商对CII的访问满足以下要求： (a) 访问行为须经事先书面批准并记录在案； (b) 访问过程受CIIO全程监督； (c) 访问操作必须在现场执行。 CIIO 应实施自动终止机制，在预先设定的无操作	1. 客户需确保所有内部及供应商访问关键信息基础设施系统或组件，只有授权人员、流程、设备才能进行访问，并按照风险评估执行身份验证与权限控制。对供应商访的访问必须预先书面批准、做好记录，并由客户监督。闲置会话应自动终止，或监控并触发异常警报。 2. 华为云的统一身份认证服务（IAM）为客户提供云上资源访问控制。使用 IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户	华为云制定了内部运维账号的生命周期管理，包括帐号的开销户管理、帐号责任人/使用人管理、口令管理、开销户监控管理等，帐号一旦建立，立即纳入帐号管理员的日常维护管理工作。所有运维帐号，所有设备及应用的帐号均实现统一管理，并通过统一审计平台集中监控，并且进行自动审计，以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。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。 华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。在权限复核与调整方面，华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。

	时间后自动终止登录会话；如无法终止登录会话，则应对登录会话进行异常活动监控，并在检测到异常时触发警报以便调查。	协同操作资源时，使用 IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过云审计服务（CTS）作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。	在华为云内部，华为云建立了正式的采购审核流程，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。合同与服务协议中明确了双方的责任和义务、供应商应满足的网络安全要求、服务内容及服务水平等要求，同时通过保密协议对违反保密性的条款进行了约束。华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。 华为云制定了会话超时策略、账号登陆和锁定策略。其中明确系统支持根据账号、角色、IP 等多种特征组合来确定是否允许通过认证建立认证后的会话，同时必须使用会话 Token 对敏感和关键的操作进行校验以确保会话的真实性。此外管理员在进行系统维护时，查看或检测到非法用户会话时，可通过管理界面强制该用户下线，并清除用户的会话信息。同时设置会话超时机制，在一段时间未收到消息后，可进行会话锁定或返回登录页面，目前超时页面会话为 30 分钟。
5.2 账户管理	对于可访问关键信息基础设施（CII）的各类账户（包括用户账户、应用程序账户、服务账户及系统账户），关键信息基础设施所有者（CIIO）应： (a) 仅授予账户执行指定功能所需的最小权限； (b) 确保软件安装权限仅限经特别授权的账户； (c) 除非CII运维必需，否则不得创建共享账户； (d) 建立监控机制及流程，跟踪各账户活动行为特征，发现异常时触发警报并启动调查； (e) 及时删除或停用非必要账户及非活跃账	1.客户应对所有可访问关键信息基础设施的账户（包括用户、应用、服务账号）实施最小权限控制，杜绝不必要的权限和共享账户，除非系统运行绝对必要。 2. 客户应建立账户行为监控机制，用于识别异常活动，并按照至少每12个月的频率定期对账户有效性和权限进行审查。 3. 对于通过供应商访提供服务的账户，客户也要将其纳入统一管理和评估。	华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，如USB key、Smart Card等。员工账号用于登录VPN、堡垒机，实现用户登录的深度审计。华为云在为相关监管机构（部委或机构、执法人员）提供访问权限时，同样通过上述机构保存审计跟踪记录。 华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。在权限复核与调整方面，华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。

	户。 CIIO 应定期审查所有 CII 访问账户，以评估账户有效性并确保权限设置及时更新。该审查应至少每 12 个月执行一次，首次审查须在合规日期起 12 个月内完成。	4. 华为云的统一身份认证服务（IAM）为客户提供云上资源访问控制。使用 IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用 IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过云审计服务（CTS）作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。	
5.3 特权访问管理	针对特权账户管理，关键信息基础设施所有者（CIIO）应： (a) 确保仅向经特别授权的账户授予特权访问权限（即管理权限）； (b) 维护最新的特权账户清单，包括各账户权限分配详情； (c) 当特权账户访问关键信息基础设施（CII）或进行权限提升时（如用户登录后申请系统/网络附加权限），必须实施多因素认证； (d) 确保特权访问从网络安全强化环境中发起，且数据传输仅通过授权连接进行。	客户必须对所有用于访问其关键信息基础设施的特权账户进行严格管理，例如只向有明确授权的账户授予特权权限，维护一份最新的特权账户清单，确保所有特权访问操作均启用多因素认证，并要求这些访问只能通过安全加固的环境和授权网络连接进行。	华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求，采用双因子认证对华为云运维人员进行身份认证，如 USB key、Smart Card 等。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。

5.4 域控制器管理	关键信息基础设施所有者（CIIO）应建立以下机制和流程： (a) 监控已建立域间信任关系的变更情况； (b) 识别信任关系中的异常行为，并在检测到异常时触发调查警报。	客户应监控域控制器间的信任关系，及时识别任何不当变更，并在检测到异常时立即报警和调查。	为了加强网络安全防护，阻止网络攻击扩散，华为云参考 ITU E.408 安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域，网络层面的划分和隔离，使用了 DDoS 异常和超大流量清洗、网络入侵检测与拦截（IDS/IPS）、Web 安全防护等技术手段。
5.5 网络分段	关键信息基础设施所有者（CIIO）应根据安全等级和风险水平的差异，对关键信息基础设施（CII）的网络架构实施分段隔离。 CIIO应将CII不同网段间的通信限制在运维必需的最小范围内。 CIIO应： (a) 在CII各网段间部署网络安全机制，以检测并阻断恶意流量，保障网络通信安全；以及 (b) 建立网络安全事件发生时隔离受影响网段的应急机制和流程。	1. 客户应将基础设施网络按照风险和安全等级分段，只允许必要的通信通过，并采取措施监测及阻断不正常的网络流量。在发生安全事件时，需要能够迅速隔离受影响的区段。 2. 客户可以使用华为云提供的虚拟私有云（VPC）服务，实现不同区域之间网络隔离。VPC 可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络 ACL 和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。同时华为云为客户提供了 Anti-DDoS 流量清洗服务，客户可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。	功能及风险等级将生产及非生产环境划分为多个安全区域，DMZ 区、公共服务区（Public Service）、资源交付区（POD - Point of Delivery）、数据存储区（OBS - Object - Based Storage）、运维管理区（OM - Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制。
5.6 网络安全	关键信息基础设施所有者（CIIO）应制定并实施CII网络访问控制规则，定期审查确保其持	1. 客户应为关键基础设施制定并定期评估网络访问控制策略，只允许必要	在每个云数据中心边界部署华为专业的 Anti-DDoS 设备来完成对异常和超大流量攻击的检测及清洗。华为云在网络边界部署了 IPS 设备，包括但不限于外网边界、

	续适用。审查频率应与CII的网络安全风险特征相匹配。 CIIO应确保CII不与非CII网络连接，除非运维必需。 CIIO 应确保 CII 不连接互联网，除非运维必需。确需接入时，须采取适当措施降低由此产生的网络安全风险。	的内部或外部网络连接；若确需连接外部网络或互联网。 2. 客户应确保所有访问必须严格与风险匹配，确保通信安全。 3. 虚拟私有云服务（VPC）为弹性云服务器构建隔离的、用户自 主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。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，满足租户更细颗粒度的网络隔离需要。	安全区域边界和租户空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS 可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。
5.7 远程连接管理	关键信息基础设施所有者（CIIO）应为所有远程连接CII的操作部署有效网络安全措施，以预防和检测未授权访问，并验证所有远程连接的合法性。 CIIO应确保：	客户应确保所有远程访问关键基础设施的操作经过授权并受到严格控制，例如启用MFA、使用加密协议等，并限制远程访问仅用于必须任务。除非业务需要，应关闭远程访问功能，确保	华为云不允许运维运营人员在未经授权的情况下访问客户的系统和数据。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证，如 USB key、SmartCard 等。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。堡垒机上支持强日志审计，确保运维

	(a) 除非运维必需，否则禁用CII远程连接功能； (b) 建立CII远程连接必须通过多因素认证； (c) 远程连接需采用强加密且仅通过安全中介机制建立； (d) 实施措施保障远程连接传输安全及消息完整性； (e) 上传至CII的文件须经恶意代码扫描； (f) 远程连接的数据流严格限制在执行功能所需的最小范围内。	远程操作安全可靠并符合法规要求。	人员在目标主机上的操作行为都可以定位到个人。在客户授权访问系统的情况下，华为云通过严格的安全运维规范和流程，确保远程运维中的安全。针对运维场景，华为云通过在数据中心部署的 VPN 和堡垒机实现运维管理平台的统一运维管理和审计。数据中心外网运维人员和内网运维人员对网络、服务器等设备的本地及远程操作全部集中管理，实现用户对设备资源操作管理的统一接入、统一认证、统一授权、统一审计。
5.8 无线通信管理	关键信息基础设施所有者应确保关键信息基础设施不得接入任何无线局域网，除非该接入为关键信息基础设施运行所必需。	1. 客户应确保无线接入确为业务所需，并采用强加密技术，且只允许授权的设备连接。 2. 客户应合理配置无线策略和接入控制，防止未授权设备连接云上资源或关键网络。	华为云所有接入华为内部网络包括有线办公网络和无线办公网络的计算机设备均必须安装公司安全软件，员工可通过公司安全软件从外部网络接入华为内部办公网络。此外，未经批准，在华为办公区域内，不允许接入非华为提供的无线网络，禁止在华为办公区域私自搭建无线网络或将测试无线网络接入公司办公网络，若有业务需求，必须经过业务主管和 IT 管理部门评估和审核批准。此外，华为云根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。登录权限分为：核心网络、接入网络、安全设备、业务系统、数据库系统、硬件维护、监控维护等。不同岗位不同职责人员限定只能访问本角色所管辖的设备，其他设备无权访问。
5.9 系统加固	针对关键信息基础设施（CII）中可能存在的以下资产类型，关键信息基础设施所有者（CIIO）应根据CII的网络安全风险特征，为每类资产建立并实施相应的安全配置基线。 安全配置基线至少应包含账户管理，密码与口令管理，应用程序控制，端口与服务管理，物理连接，恶意软件防护以及软件升级与更新	1. 客户应根据自身网络安全风险状况，制定并实施各类资产的系统加固基线，明确操作系统、服务器、工作站等的配置要求，并按照至少每12个月的频率定期进行审查更新。 2. 客户应确保部署在云上的资源也符合这些基线要求，并仅使用授权设备进行云资源的管理	所有产品在上线前都经过了多轮安全测试，其中华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如SecureCat可以对业界主流的OS和DB 的安全配置进行检查。此外，产品上线前均须由安全工程实验室按照对应的安全配置规范执行检查。华为云构建了配置监控平台，实现对服务器操作系统、数据库管理系统及网络设备的配置项进行实时监控。配置监控平台会将实际的配置项同标准配置基线进行对比。当出现差异时，差异分析结果会通过邮件自动发送至巡检管理员进行后续跟进处理。

	的安全实践。 CIIO应至少每12个月审查一次安全配置基线，确保其持续有效保障CII网络安全。首次审查须在基线建立后的12个月内完成。 CIIO 应确保仅使用授权计算设备进行 CII 管理，且该设备不得用于非管理用途。	操作。 3. 客户可使用华为云的企业主机安全（HSS）服务对主机进行基线检查，包括检测系统口令复杂度策略、经典弱口令、风险账号，以及常用系统与中间件的配置，以识别不安全项目，预防安全风险。	华为云对支撑业务运营的服务器操作系统、数据库管理系统及网络设备建立了统一的基线配置标准，以实现对服务基线配置的统一管理，明确华为云生产环境中各系统/组件的安全配置要求，并确保安全配置的有效执行和持续改进。华为云参考互联网安全中心（CIS － Center of InternetSecurity）安全基线并将融入华为云 DevSecOps 流程中并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。华为云的运维团队根据内部的安全基线管理规范，定期检查并更新网络设备安全参数设置。华为云对主机操作系统、虚拟机、数据库、web 应用组件等均进行安全配置加固并进行定期检查。
5.10 补丁管理	关键信息基础设施所有者应建立并实施安全补丁管理流程。并确保管理层对安全补丁管理流程的有效性实施监督。	客户应对在云上部署的资源，如数据库、中间件等主动管理补丁，包括监控补丁发布、验证补丁完整性、测试兼容性、按风险优先级及时修补漏洞，并由管理层监督整个流程；如确实无法修补，应部署补偿性控制措施。	华为云建立安全补丁管理的流程， 保证安全补丁在IT安全标准规定的 期限内完成安装。同时，华为云制定了漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，根据漏洞整改要求，针对不同严重程度的漏洞修复时限要求及时在规定的期限内应用修补措施或补丁、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等。补丁安装时有专门的工具和平台，并且在升级实施前先在测试环境或类生产环境验证，再对生产环境升级，生产环境灰度操作，分批实施。 华为云每年会对建立的补丁管理相关规范和策略流程进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
5.11 便携式计算设备与可移动存储介质	CIIO应建立流程，对连接关键信息基础设施的便携式计算设备和可移动存储介质的使用进行授权和跟踪。 CIIO应确保所有此类授权的便携式计算设备符合安全配置基线，该基线至少满足安全实践，并满足CIIO对此类设备可能制定的其他安全标	客户应建立严格流程控制所有接入关键系统的笔记本、USB 等设备的使用，确保设备已加固、启用加密、定期查杀恶意软件，并对关键数据加密保护，防止信息在设备丢失或被入侵时泄露。	华为云制定并实施移动介质管理规定，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，规定不得用个人存储介质连接服务器，未经授权，也不得私自使用任何存储介质连接服务器。 华为云制定并实施介质管理规定，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

	准和要求。 CIIO应确保授权的可移动存储介质在连接关键信息基础设施之前已通过恶意软件扫描。 CIIO 应确保存储在便携式计算设备和可移动存储介质中的与关键信息基础设施相关的敏感信息（包括生产数据和系统配置信息）通过强加密进行保护。		行记录。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。
5.12 应用程序安全	CIIO应确保在关键信息基础设施中仅使用对CII运行及网络安全必要且经CIIO批准的应用程序，并建立和维护此类获批准应用程序的清单。 CIIO应至少每12个月审查一次获批准应用程序清单，首次审查须在清单建立后的12个月内完成。 CIIO应在应用程序用于关键信息基础设施前验证其完整性。 对于作为IT系统的CII，CIIO应实施分层架构，将应用层与数据库层分离，并在每一层部署安全控制措施。 对于包含Web应用系统的CII，CIIO在设计、开发和测试应用程序时，应参考最新版开放式Web应用程序安全项目（OWASP）或等效应用安全指南，以最小化应用安全风险。	1. 客户应确保部署的应用为“经批准且必要”的应用，定期审查清单，使用多层架构分离数据库和应用层，开发过程遵循开放Web应用程序安全项目等安全规范，并为公网Web系统部署WAF防护，防止入侵、篡改等风险。 2. 客户应限制编译器、调试器的使用，仅在授权设备中必要时使用。 3. 华为云的 Web 应用防火墙（WAF）服务，通过对 HTTP(S) 请求进行检测，为客户提供识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击的服务，保护 Web 服务安全稳定。	华为云制定并实施桌面终端服务软件标准及开源软件清单，仅可以使用其中定义的标准操作系统和软件应用程序。此外，华为云制定了安全编程规范及应用安全开发规范，其中明确了华为云可使用的软件库和数字签名脚本，避免恶意软件的入侵造成安全风险。在终端设备上的iDesk程序设有上审阅后的应用程序白名单，华为云内部办公软件仅能从该平台进行下载。 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。针对使用桌面云管理程序的华为云设备，通过在后台系统进行配置的方式确保员工无法自行卸载或禁用。 华为云每年会对建立的应用程序白名单相关规范和策略流程进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。 华为云对在公共网络上提供的应用服务采用多重机制和措施进行重点保护，包括使用IAM进行访问控制，对用户进行身份认证和鉴权；API调用使用TLS加密以保证传输的机密性；结合Anti-DDoS、入侵防御系统（IPS）和Web应用防火墙（WAF）等多层高级边界防护机制针对不同的威胁和攻击进行有效防范；对用

	对于包含面向互联网的Web应用系统的CII，CIIO还应部署Web应用防火墙（WAF），以监测、检测并阻断Web应用威胁。 CIIO 应确保编译器与调试器仅在必要时且仅在授权设备上使用于关键信息基础设施中，不再需要时应立即移除。		户调用API的频率的适当流量控制，确保基于API的访问的高可用性和连续性。 华为云参照业界实践并结合自身经验沉淀及业务特性从三层技术架构设计 Web 应用程序，包括基础层（application layer）、平台层（platform layer）、应用层（foundation layer），实现应用的安全设计与维护，确保高内聚，低耦合。此外，华为云制定了 web 应用开发规范，结合多维度的安全开发原则，实现深度防御的目的。
5.13 数据库安全	CIIO应确保仅授权账户能够连接并查询关键信息基础设施中的数据库。 CIIO应确保关键信息基础设施的系统管理职责与数据库管理职责分离，并分配给不同人员。 CIIO应制定数据库安全策略。 CIIO应监控关键信息基础设施中的数据库是否存在异常活动，并在检测到任何异常时触发告警以进行调查。 CIIO 应监控批量查询操作，若检索数据量超过预设阈值，则触发告警以进行调查。	1. 客户应确保只有授权账号可访问数据库，实施系统管理员与数据库管理员职责分离，制定数据库安全策略，例如静态数据加密、防泄漏、敏感数据访问控制，并开启数据库审计与异常监控功能。 2. 数据库安全服务（DBSS），是一个智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL 注入攻击检测，风险操作识别等功能，保障云上数据库的安全。包括用户行为发现审计、多维度分析、实时告警、提供精细化报表、敏感数据保护、审计日志备功能。数据库安全审计提供的旁路模式数据库审计功能，可以对风险行为进行实时审计和告警。同时，通过生成满足数据安全标准的合	访问控制：租户创建RDS实例时，RDS会为租户同步创建一个数据库主帐户，主帐户的密码由租户指定。此主帐户允许租户操作自己创建的RDS实例数据库。租户可以使用数据库主帐户连接RDS实例数据库，并根据需要创建数据库实例和数据库子帐户，根据自身业务规划，将数据库对象赋予数据库子帐户，以达到权限分离的目的。租户创建数据库实例时，可以选择安全组，将RDS实例业务网卡部署在对应的安全组中。租户可以通过VPC对RDS实例所在的安全组入站、出站规则进行限制，从而控制可以连接数据库的网络范围。数据库安全组仅允许数据库监听端口接受连接。配置安全组不需要重启RDS实例。 传输加密：RDS实例支持数据库客户端与服务端TLS加密传输。RDS在发放实例时，指定的CA会为每个实例生成唯一的服务证书。客户端可以使用从服务控制台上下载的CA根证书，并在连接数据库时提供该证书，对数据库服务端进行认证并达到加密传输的目的。 存储加密：支持对存储到数据库中的数据加密后存储，加密密钥由KMS管理。 此外，华为云提供的基础设施存储、数据库本身具有数据备份的机制，备份的数据副本和数据采用同样的数据安全措施。例如云硬盘提供安全的加密算法（AES-256）和功能、对象存储服务可提供服务端加密功能及防盗链功能、RDS 数据库提供存储加密机制等。通过与数据加密服务集成，备份数据可以方便、快速地实现加密存储，有效保证备份数据的安全性。

		规报告，可以对数据库的内部违规和不正当操作进行审计及定位追责。	
5.14 漏洞评估	CIIO应建立流程以识别和跟踪关键信息基础设施的网络安全漏洞。 CIIO应及时修复所有网络安全漏洞，并优先处理对CII安全或运行构成较高风险的漏洞。 CIIO应对关键信息基础设施进行漏洞评估。 CIIO还应在对CII实施任何重大系统变更后，对相关CII资产进行漏洞评估。重大系统变更包括将新系统接入CII、部署新应用模块、系统升级和技术更新。 如专员要求，CIIO 应在收到请求后 30 个工作日内，向专员提交漏洞评估报告的副本，以及 CIIO 针对每个漏洞的修复计划。	1. 客户应建立漏洞管理流程，定期对其部署在云上的系统进行漏洞评估。 2. 客户应优先修复高风险漏洞，确保在重大系统变更后立即开展漏洞评估，并在监管机构要求时，及时提交漏洞评估报告和修复计划。 3. 客户可使用华为云的企业主机安全（HSS）服务提供的资产管理、漏洞管理、基线检查、入侵检测等功能，帮助客户更方便地管理主机安全风险，实时发现并阻止黑客入侵行为，以及满足等保合规的要求。	华为云建立了安全漏洞管理流程，规范了华为云系统安全漏洞的预警、评估、修复处理的闭环流程，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。
5.15 渗透测试	关键信息基础设施所有者（CIIO）应对关键信息基础设施（CII）进行渗透测试。 CIIO在对CII实施任何重大系统变更后，应对相关CII资产进行渗透测试。 CIIO应确保对CII执行渗透测试的第三方渗透测试服务提供商及其测试人员分别具备行业认可的资质认证。 CIIO应确保所有由第三方服务提供商执行的渗	1. 客户应定期对其部署在云上的系统进行渗透测试，尤其在重大系统变更后及时开展测试。 2. 客户应确保选择的第三方渗透测试服务商和人员具备资质认证，并在监督下执行测试，确保不影响系统正常运行。客户还需配合监管要求，及时提交渗透测试报告及漏洞修复计划。	华为云建立了渗透测试与漏洞扫描管理规定，明确了华为云平台开展渗透测试时应遵循的安全要求，规范渗透测试行为，确保渗透测试活动合规与受控。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，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。 华为云相关人员遵循渗透测试与漏洞扫描管理规范中定义的实施流程，制定并实施具体的渗透测试活动，发现的漏洞和风险需与相关业务人员进行评估并形成正式的渗透测试报告，并向华为云安全管理部门的汇报。

	透测试都在CIIO监督下进行。 应专员要求，CIIO 应在收到请求后 30 个工作日内，向专员提交已完成渗透测试的报告副本及对应的修复计划。		
5.17 密钥管理	关键信息基础设施所有者（CIIO）应确保关键信息基础设施（CII）的所有加密密钥均受到保护，防止未经授权的访问。 CIIO 应建立并实施加密密钥生命周期的跟踪与管理机制及流程，且应至少每 12 个月对这些机制和流程进行一次审查，以确保其持续有效性。首次审查应在相关机制和流程实施后的 12 个月内完成。	1. 客户应管理其在云上使用的加密密钥，确保密钥安全且仅授权人员能访问。 2. 客户应制定密钥生命周期管理流程，按照至少12个月一次的频率定期审查这些流程的有效性，确保密钥在使用过程中始终受到保护，防止信息泄露和未经授权的访问。 3. 华为云的数据加密（DEW）服务是一款综合的云上数据加密服务。为客户提供专属加密、密钥管理、凭据管理、密钥对管理等服务，使用DEW 可以解决数据安全、密钥安全、密钥管理复杂等问题。	华为云各业务领域须遵照密钥管理安全规范，对密钥生成、密钥存储、密钥分发、密钥更新和密钥销毁等操作实施安全管控，防止密钥泄露和密钥丢失损坏。同时，华为云使用密钥管理服务（KMS）管理RDS和OBS用户的主密钥，RDS和OBS通过调用KMS的内部接口请求使用主密钥用于加解密工作。 华为云每年会对建立的密钥安全相关规范和策略流程进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

6.5 检测要求

编号	具体控制要求	客户关注点	华为云的内部实践
6.1 日志记录	关键信息基础设施所有者（CIIO）应生成、收集并存储以下日志记录： (a) 所有对CII的访问及访问尝试行为，包括访问期间的应用程序与数据库活动，以及对CII内数据的访问；	1. 客户应利用供应商访提供的日志功能，确保其关键系统和数据的访问、网络连接及安全设	在日志保存过程中采取安全措施防止日志被篡改，以确保支撑网络安全事件回溯和合规。为确保日志数据安全，安全日志会进行统一备份或归档，并依照数据安全管理的要求，限制安全日志使用的申请及权限，仅允许授权人员因必要原因进行安全日志的查询，确保受控使用。华为云遵从

	(b) CII与外部网络之间的网络连接； (c) CII内部的网络连接； (d) 对CII的远程连接； (e) CII与无线局域网（WLAN）之间的连接。 CIIO还应生成、收集并存储以下类别的日志，以提供CII内部及CII与外部网络之间网络活动的可视性： (a) 网络防火墙日志； (b) 域名系统（DNS）日志； (c) 网络代理日志； (d) 网络入侵检测/防御系统（NIDS/NIPS）日志。 CIIO应按专员要求提供以上所述日志，用于威胁监控、威胁分析、威胁预警及事件响应。 CIIO应确保生成、收集和存储的日志符合以下要求： (a) 采用统一的时间源； (b) 防止未经授权的访问、修改和删除； (c) 自日志相关事件发生之日起至少保存12个月； (d) 日志文件结构（即每个日志文件内数据字段的排列方式）应便于分析和共享； (e) 制定日志保留政策，以支持网络安全事件调查、威胁追踪及其他与 CII 网络安全相关的用途。	备日志完整、及时地生成和存储。 2. 客户应根据安全需求制定日志管理政策，保障日志的完整性和长期保存，用于威胁检测、事件调查和合规审计。 3. 华为云的云日志（LTS）服务，用于收集来自主机和云服务的日志服务，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为客户提供实时、高效、安全的日志处理能力。	法律法规要求，具备集中、完整的日志审计系统，具备强大的数据保存及查询能力，确保所有日志内容保存时间超过6个月。内部人员运维操作均被日志平台采集并记录。 华为云建立了集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以确保支撑网络安全事件回溯。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM–Security Information and Event Management）系统如 ArcSight、Splunk 对接。 华为云的统一日志分析平台，对SVN、堡垒机、主机、WAF、HSS等服务的安全日志进行收集并建立日志监控自动告警机制。运维平台作为华为云进行运维管理的入口，开启了操作日志记录的功能，操作日志无法被人为修改，且至少保留了6个月的日志记录，包括登录IP、登录方式及登陆时间等。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为12个月。
6.2 监控与检测	关键信息基础设施所有者（CIIO）应建立并实施以下机制和流程： (a) 监测和检测所有涉及CII的网络安全事件； (b) 收集和存储所有此类网络安全事件的记录（包括相关日志，如有）； (c) 分析所有网络安全事件，包括事件关联分析，以判定是否存在或曾发生网络安全事故；	1. 客户应在使用云服务提供商服务的基础上，建立自身的安全监控与检测机制，监控涉及其关键业务系统的安全事件，收集和分析相关日志，识别异常活动并及时	华为云建立了集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以确保支撑网络安全事件回溯。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM–Security Information and Event Management）系统如 ArcSight、Splunk 对接。

	(d) 在存在或曾发生网络安全事故时，触发适用的事件报告、响应和恢复计划。 为实现网络安全事件的监控和检测，CIIO建立的机制和流程应包括： (a) 扫描入侵指标（IOCs），包括IP地址、统一资源定位符（URL）、域名和哈希值； (b) 建立CII日常正常运营活动和网络流量的基准，并以此为基础监测异常活动和偏差； (c) 确保对所有检测到的异常活动和偏差触发警报以便进一步调查。 CIIO 应至少每 12 个月对建立的机制和流程进行一次审查，确保其持续有效。首次审查应在机制和流程实施后 12 个月内完成。	响应。 2. 客户应定期审查监控流程和基准线，确保能及时发现和处理网络安全事故。 3. 华为云的云监控（CES）服务可实现对客户自身云资源的使用情况和绩效的监控。华为云可以根据客户的需求按照 SLA 向客户提供服务报告。同时华为云为客户提供了 Anti-DDoS 流量清洗服务，客户可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。	对于集中存储安全日志的日志分析平台，系统管理员会定期例行对采集状态、存储状态进行检查，保证安全日志的可用性。华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理，异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录。 华为云的统一日志分析平台，对 SVN、堡垒机、主机、WAF、HSS等服务的安全日志进行收集并建立日志监控自动告警机制。运维平台作为华为云进行运维管理的入口，开启了操作日志记录的功能，操作日志无法被人为修改，且至少保留了6个月的日志记录，包括登录IP、登录方式及登陆时间等。 华为云每年会对建立的安全日志管理相关规范和策略流程进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
6.3 威胁狩猎	关键信息基础设施所有者（CIIO）应当至少每24个月对关键信息基础设施（CII）开展一次威胁狩猎，以搜寻和识别针对CII的网络安全威胁。首次威胁狩猎工作应在合规日期后12个月内完成。 CIIO应将通过威胁狩猎识别的网络安全威胁纳入网络安全风险评估，确保在整个CII系统开发生命周期中对这些威胁产生的风险进行评估、缓解和跟踪。	1. 客户应每24个月至少进行一次威胁狩猎活动，例如从云服务提供商等渠道获取威胁情报，评估其对自身关键系统的影响，并采取技术和管理措施应对已知威胁。 2. 客户应将威胁狩猎结果纳入自身的风险	华为云PSIRT会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。 华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。

	CIIO 应对威胁狩猎发现的所有威胁进行分析，以判定是否存在或曾发生涉及 CII 的网络安全事件。如确认存在或曾发生网络安全事件，应立即启动相应的事件报告、响应和恢复预案。	管理，确保发现的威胁得到评估、缓解和跟踪，必要时启动事件响应，保护业务安全。	
6.4 网络威胁情报与信息共享	关键信息基础设施所有者（CIIO）应当建立并实施威胁情报获取机制及处理流程，用于分析评估威胁情报与关键信息基础设施（CII）的关联性及潜在影响。 CIIO应当建立并实施网络安全威胁与漏洞信息共享机制，与专员共享网络安全威胁和漏洞相关信息，以及针对此类威胁和漏洞可采取的应对措施，用于威胁监控和分析。 CIIO 应当制定控制措施，以缓解从威胁情报识别的网络安全威胁，并及时处置已发现的系统漏洞。	1. 客户应建立机制收集、分析来自云服务提供商和其他渠道的威胁情报，判断其对关键系统的相关性与影响，并据此更新风险应对措施。 2. 客户应责任将相关的网络安全威胁和漏洞信息共享给监管机构，并采取应对行动，包括报告、处置和恢复计划。	华为云按照政策要求，在公司内部与外部间建立了多条信息沟通渠道，以确保华为云在内部员工之间，以及华为云内外部云服务客户间的有效沟通。华为云确保网络安全保障体系在各体系、各区域、全流程的实施，积极推动与政府、客户、合作伙伴、员工等各利益相关方的沟通，以确保利益相关方能及时有效地接收到的华为云网络安全有关信息。为促进与外部的顺畅沟通，华为云配备专人与行政机构、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。与外部利益相关者紧密合作，共享信息，以期推动网络安全领域的进步。 客户应在规定时间内向监管机构通报安全事件相关情况。为配合客户满足网络安全事件上报，华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响 华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。

6.6 响应与恢复要求

编号	具体控制要求	客户关注点	华为云的内部实践
7.1 事件管理	关键信息基础设施所有者（CIIO）应当制定网络安全事件响应计划，明确CIIO应对网	1. 客户应制定完整的事件响应计划，涵	华为云每年对信息安全事件管理程序和流程进行培训和测试，所有的安全事件响应人员，包括后备人员均需参与。此外，华

	络安全事件的处置流程。 CIIO应确保CIRT成员接受专业培训并配备必要的应急响应资源。 对于采用Kerberos认证协议的CII资产，CIIO应建立域控制器Kerberos票据授予票据账户重置规程，并在域控制器遭受入侵时执行该账户的重置。 CIIO应建立并实施流程，识别、调查并解决导致每起网络安全事件的根本原因，包括结构性、行为性、管理性、技术性或系统性因素，以防止类似事件再次发生。 CIIO应向所有CII使用、运营和管理人员（含外部供应商及其人员）传达响应计划，并在计划更新时及时通知。 CIIO应至少每12个月对《网络安全事件响应计划》进行一次审查，以确保其保持更新并具有适用性。首次审查应在计划建立后的12个月内完成。 当 CII 网络运行环境或事件响应要求发生重大变化时，CIIO 应及时审查响应计划。	盖事件报告、沟通机制、网络安全事件响应团队职责、恢复流程及取证程序，并确保外部供应商知情并能配合执行。 2. 在使用 Kerberos 认证的关键资产上，客户应有可操作的账户重置机制，用于在入侵事件中降低进一步风险。 3. 客户应定期审查和更新该计划，培训相关人员，并确保供应商也同步更新和参与。	为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案，定期做应急演练和测试，持续优化应急响应机制。 华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划和流程，作为流程的一环节，在安全事件得到遏制后，华为云会做根本原因分析，并制定应对和预防措施。同时，华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。 华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云设置 7*24 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。
7.2 危机沟通计划	关键信息基础设施所有者（CIIO）应当建立危机沟通计划，用于应对网络安全事件引发的危机情况。 CIIO应确保危机沟通计划包含以下内容： (a) 设立危机沟通团队，在危机发生时启动运作； (b) 识别可能的网络安全事件场景及相应的应对措施； (c) 针对每类网络安全事件场景，明确目标受众和利益相关方（包括员工、客户及公众等）； (d) 指定媒体应对发言人和技	1. 客户应制定危机沟通计划，明确危机事件下的沟通流程、角色分工（包括与云服务提供商的配合机制）、发言人、目标受众、沟通渠道等，并确保外部合作方知情并能协同执行。	华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。

	术专家代表； (e) 确定向相关目标受众和利益相关方传递信息的主要及备用通信渠道； (f) 建立危机沟通团队、发言人、技术专家及其他相关人员之间的协调机制，确保危机期间响应行动协调一致； (g) 制定危机沟通计划，确保相关人员能够履行既定职责。 CIIO应向所有相关人员（包括危机沟通团队成员、发言人和技术专家等）传达危机通信预案，并在预案更新时及时通知。 CIIO 应至少每 12 个月审查一次危机通信预案以确保其有效性，首次审查应在计划建立后 12 个月内完成。	2. 客户应至少每年审查一次危机沟通计划并为相关人员提供培训。	
7.3 网络安全演练	关键信息基础设施所有者（CIIO）应当开展基于场景的网络安全演练。 CIIO应至少每12个月开展一次第7.3.1款所述的情景式网络安全演练。首次演练应在合规日期后12个月内完成。 在设计网络安全演练的事件响应场景时，CIIO应包含以下测试验证要素： (a) 针对威胁情报所识别威胁和漏洞的应对措施； (b) 与合作伙伴及供应商的协调方案； (c) 事件响应期间对后续网络安全威胁和事件的持续监测能力； (d) CIIO应对网络安全事件的资源和能力充足性。 CIIO应确保以下利益相关方参与网络安全演练： (a) 高级管理层； (b) 危机管理团队； (c) 企业通信和业务运营人员； (d) 网络安全事件响应团队（CIRT）； (e) 服务提供商。	客户需每年至少开展一次基于真实情景的演练，测试其事件响应、业务连续性、灾难恢复和危机沟通计划是否有效，并确保包括供应商、管理层、传播团队等相关方参与，同时记录演练情况并准备好在监管要求下提交报告。	华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。同时，华为云使用eBackup系统对备份数据进行循环冗余校验以确保备份数据的完整性和可用性，校验失败则无法成功进行备份。此外，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。 华为云每年对信息安全事件管理程序和流程进行培训和测试，所有的安全事件响应人员，包括后备人员均需参与。此外，华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案，定期做应急演练和测试，持续优化应急响应机制。

	若专员提出要求，CIIO应在收到请求后30个工作日内，提交已完成的网络安全演练报告副本及整改方案。 对于专员依据第 16 条开展的网络安全演练，CIIO 应按要求提供与 CII 相关的信息（包括相关网络安全事件响应计划和危机沟通计划），以支持此类演练的规划和实施。		

6.7 网络弹性要求

编号	具体控制要求	客户关注点	华为云的内部实践
8.1 备份与恢复计划	关键信息基础设施所有者（CIIO）应制定完备的备份与恢复计划，以确保在发生系统中断或数据损坏事件时，能够完整恢复其关键信息基础设施（CII）资产。 CIIO应根据其运营需求定期执行备份，并确保备份成功完成。备份频率应与运营要求相匹配。 CIIO应确保备份存储于未连接任何计算机或互联网的独立设备中，且与对应的CII资产分离，并防止未经授权的访问、修改和删除。 CIIO应定期开展备份恢复测试，测试频率需根据CII的网络安全风险特征确定，以确保在需要时能够成功完成数据恢复。 CIIO 应至少每 12 个月对备份与恢复计划进行一次全面审查，确保计划的持续适用性。首次审查应在计划建立后 12 个月内完成。	1. 客户应根据业务需求设定备份与恢复计划，定期执行备份并验证恢复效果，确保所有关键数据可恢复。 2. 客户应至少每12个月审查一次备份与恢复计划，并确保符合监管要求，特别是防止未授权访问和修改备份数据。 3. 华为云的云备份（CBR）服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。此外，华为云还规范了业务恢复策略的制定，确保业务能在恢复时间目标内恢复到可接受水平。华为云建立了节点数据定期备份机制，通过eBackup系统实现对节点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。 华为云每年会对建立的备份与恢复和业务连续性相关规范和策略流程进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

		导致数据不可用的场景前可将数据恢复到任意备份点。	
8.2 业务连续性计划与灾难恢复计划	关键信息基础设施所有者（CIIO）应制定业务连续性计划（"BCP"）和灾难恢复计划（"DRP"），以确保在因网络安全事件导致服务中断时，能够持续提供基本服务。 CIIO应确保BCP和DRP包含针对不同网络安全威胁场景的应对方案。 CIIO应在BCP中明确定义恢复时间目标（RTO）和恢复点目标（RPO）。 对于使用Kerberos认证协议作为域控制器的CII资产，CIIO应将Kerberos票据授予票据（TGT）泄露的恢复程序纳入灾难恢复演练内容。 CIIO 应至少每 12 个月对 BCP 和 DRP 进行一次审查，以确保其持续有效性。首次审查应在计划建立后 12 个月内完成。	1. 客户应制定完整的业务连续性与灾难恢复计划，明确各类网络安全事件下的应对方案，设定合理的恢复时间目标（RTO）和恢复点目标（RPO），并定期演练恢复流程，特别是涉及使用Kerberos协议的关键系统。 2. 客户应至少每年审查一次业务连续性与灾难恢复计划，确保其始终有效和实用。	华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。同时，华为云使用eBackup系统对备份数据进行循环冗余校验以确保备份数据的完整性和可用性，校验失败则无法成功进行备份。此外，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。 客户应建立业务连续性机制，并保障RTO与RPO的实现。华为云遵循 ISO22301业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。在该体系框架的要求下，华为云会定期开展业务影响分析，识别关键业务，确定关键业务的恢复时间目标与恢复点目标以及最小恢复水平。在识别关键业务的过程中，华为云将业务中断对客户的影响程度作为判断关键业务的一个重要标准。 华为云每年会对建立的备份与恢复和业务连续性相关规范和策略流程进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

6.8 网络安全培训与意识

编号	具体控制要求	客户关注点	华为云的内部实践
9.1 网络安全意识计划	关键信息基础设施所有者（CIIO）应制定并实施网络安全意识培养计划，对所有使用、操作和管理关键信息基础设施（CII）的人员（包括外部供应商及其人员）开展网络安全教育培训。 CIIO应至少每12个月通过测试	1. 客户应建立全面的网络安全意识计划，对所有使用和管理关键信息基础设施的人员（包括供应商）开展定期培训和测	华为云为确保员工的信息安全意识能够符合公司要求建立了一系列的网络安全培训及学习机制，要求员工持续学习网络安全知识，了解相关的政策和制度，会涵盖安全处理钓鱼邮件、移动设备和存储介质的安全处理、安全的互联网浏览及安全使用社交媒体等主题。面向全员开展形式多样的网络安全宣传活动，包括网络安全社区运营、网络安全典型案例宣传、网络安全

	问卷和调查等方式，评估网络安全意识培养计划在实现以上目标方面的有效性。首次评估应在计划实施后12个月内完成。 CIIO 应至少每 12 个月对网络安全意识培养计划进行一次审查，以确保计划的时效性和适用性。首次审查应在计划制定后 12 个月内完成。	评，培训内容应包括法律法规、行为守则、安全政策和程序，以及当前常见威胁和防范措施。 2. 客户还应至少每 12 个月采用问卷或测验方式对该计划进行评估和修订，确保安全知识传达有效、内容及时更新。	活动周、网络安全动画宣传片等，以提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营。 华为云每年会对建立的人员意识培训计划进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
9.2 网络安全培训与技能	关键信息基础设施所有者（CIIO）应确保所有负责操作和管理关键信息基础设施（CII）的员工接受网络安全技能培训，使其能够有效履行与CII相关的职责。 CIIO应确保非员工身份的操作和管理CII人员（包括外部供应商及其人员）具备必要的网络安全技能，以有效履行其与CII相关的职责。 CIIO应确保为CII开展网络安全风险评估的工作组，由持有行业公认认证（如风险与信息系统控制认证（CRISC）或同等资质）的专业人员监督指导。 CIIO 应确保为 CII 开展网络安全审计的工作组，由持有行业公认认证（如信息系统审计师认证（CISA）或同等资质）的专业人员监督指导。	1. 客户应确保所有操作和管理其关键信息基础设施的人员，包括自身员工和外部供应商，均经过必要的网络安全技能培训，能有效履职。 2. 对于负责网络安全风险评估和审计的团队，客户应确保相关监督人员持有行业认可的专业资质证书，如 CRISC 或 CISA。 3. 客户应建立管理和监督机制，定期核查培训成效及资质，确保网络安全能力符合业务需求和合规要求。	华为云建立了自己的培训机制，根据不同的角色、岗位为员工设计合适的培训方案。其中一般员工的培训频率为至少每年一次，核心岗位员工培训频率更高。华为云对开发人员、运维工程师及网络安全管理人员等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。新员工转正前必须通过有关网络安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试，管理者需参加网络安全必须的培训和研讨。

7 华为云如何遵从及协助客户满足《数据中心韧性和安全性咨询指南》

IMDA 于 2025 年 2 月 25 日发布了《数据中心韧性和安全性的咨询指南》，该指南为数据中心为运营商提供了框架，旨在建立一个强大的业务连续性管理系统，包括制定业务连续性政策，以最大限度地减少服务中断并确保客户的高可用性。这包括实施业务连续性政策和流程的指导，实施持续改进机制等

当客户遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

7.1 数据中心韧性与安全风险的管理

编号	具体控制要求	客户关注点	华为云的内部实践
3.1	数据中心运营商（DCOs）应： a. 制定明确的业务连续性政策，阐明目标、范围和责任。该政策应与数据中心运营商的组织目标和监管要求保持一致； b. 确定业务连续性管理体系（BCMS）的范围。数据中心运营商应识别关键业务产品和服务（如电力、制冷、网络连接等），明确BCMS的覆盖范围、使命、目标及内外部义务； c. 获得高层管理人员对业务连续性政策的支持与参与，确保为BCMS提供必要资源，分配并传达相关职责。数据中心运营商应确保BCMS实现预期成果，并推动其持续改进； d. 当业务引入变更（如新产品（例如锂离子电池）、供	若客户作为数据中心运营商，应建立并持续优化业务连续性管理体系（BCMS），制定清晰的业务连续性政策，明确BCMS范围，确保政策与监管要求一致。需争取高层支持，分配资源、明确职责，并在业务发生变化时及时更新BCMS内容。同时，确保相关人员接受培训，熟悉在中断前、中、后各阶段的职责，并建	华为云制定了业务连续性管理规定，以规范业务连续性相关管理框架、目的和范围、管理目标、角色和职责等内容。华为云已经通过ISO22301业务连续性管理体系标准的认证，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。 为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得IS0 22301认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。

	应商或商业模式等）时，相应更新BCMS。更新内容应包括变更目的及其潜在影响； e. 确保分配足够资源以支持BCMS的建立、实施、维护和持续改进。相关人员应具备支持BCMS所需的专业能力和培训； f. 确保参与 BCMS 的人员了解相关政策，以及业务中断前、中、后期各自的角色和职责。数据中心运营商还应确定内外部沟通的内容、时机、对象、方式和负责人。	立有效的沟通机制以应对突发事件。 若客户作为在数据中心托管业务方，应了解并配合供应商的 BCMS 要求，识别自身关键业务需求并协同确保整体韧性。	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，保证灾难恢复时能及时获取外部支持。
3.2	数据中心运营商（DCOs）应： a. 开展业务影响分析，识别关键业务功能及服务中断可能造成的影响。数据中心运营商应确定服务中断对客户造成不可接受影响的最大可容忍时间范围； b. 开展全面的风险评估，识别内部和外部潜在威胁与漏洞。数据中心运营商应评估这些风险发生的可能性及其后果，并为每个已识别的风险采取适当的风险处置措施； c. 实施一系列业务连续性策略和解决方案，以降低服务中断的可能性或缩短中断持续时间。相关措施包括但不限于：冗余电源、防雷系统、火灾探测与灭火系统、防范勒索软件等网络安全措施； d. 制定详细的响应和恢复计划，明确规定服务中断期间及之后为快速恢复正常运营所需采取的行动。数据中心运营商可建立并维护事件响应架构（评估、启动、行动），以便在事件发生时提供有效响应；以及 e. 确保参与业务连续性管	若客户作为数据中心运营商，应执行业务影响分析和全面风险评估，识别关键基础服务的中断风险与影响，设定服务中断可容忍时长，并制定相应的控制措施。同时，应建立清晰的响应和恢复计划，构建“评估-启动-行动”机制，对内部员工与关键供应商定期开展业务连续性培训和演练。 若客户作为在数据中心托管业务方，应识别自身业务在数据中心中断时的影响，分析潜在风险并设定可容忍时间。	为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得ISO 22301认证。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。 华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案，定期做应急演练和测试，持续优化应急响应机制。此外，华为云制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。 华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。

	理体系（BCMS）的员工（和/或供应商）经过培训并做好有效响应事件的准备。数据中心运营商应定期开展测试和演练，确保业务连续性计划的有效性和适用性。这些演练有助于发现计划中的不足、提升准备水平，并确保员工（和/或供应商）熟悉其在服务中断期间的职责。		
3.3	数据中心运营商（DCOs）应： a. 建立关键绩效指标（KPIs），以评估业务连续性策略的实施效果，并确保其持续符合组织目标； b. 定期开展内部审计、审查及反馈会议，识别业务连续性管理体系（BCMS）中的不足和改进空间； c. 确保高层管理人员定期评审组织的 BCMS，以保证其适用性、充分性和有效性。	1. 若客户作为数据中心运营商，应设定用于衡量业务连续性管理体系（BCMS）有效性的关键绩效指标，并定期开展内部审计、管理评审，并收集相关反馈，识别改进点。同时，推动高层管理者定期参与评估，确保 BCMS 的适用性、充分性与有效性不断优化。 2. 华为云的云监控（CES）服务可实现对客户自身云资源的使用情况和绩效的监控。华为云可以根据客户的需求按照 SLA 向客户提供服务报告。	华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立完善的信息安全管理体系、IT 服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。

3.4	数据中心运营商（DCOs）应： a. 通过整改不符合项及实施纠正措施，建立持续改进的企业文化； b. 评估所采取纠正措施的有效性，必要时对业务连续性管理体系（BCMS）进行调整；以及 c. 持续关注可能导致服务中断的新威胁和技术发展动态，及时更新 BCMS。	若客户作为数据中心运营商，应应建立持续改进机制，针对评审或审计中发现的问题采取及时的整改措施。评估每项纠正措施的实际效果，如有不足及时调整 BCMS。同时，应密切关注新兴威胁与新技术的变化，动态更新业务连续性管理体系。	华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立完善的信息安全管理体系、IT 服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。
3.5	运营商可参考 ISO 22301、ISO 27001/2、ISO 31000、ISO 22237 及 TIA-942 等国际标准完善 BCMS 措施。	若客户作为数据中心运营商，应在完善 BCMS 措施时可参考 ISO 等国际标准。	华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立完善的信息安全管理体系、IT 服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。

7.2 网络安全风险的补充管理措施

编号	具体控制要求	客户关注点	华为云的内部实践
4.1.a	数据中心运营商（DCOs）应当根据各数据中心的业务和运营需求，针对关键风险领域有效防范和管理网络威胁风险（如供应链攻击、恶意软件攻击、勒索软件等），并确保其网络和系统部署了充分的网络安全控制措施。 数据中心运营商应当： 建立、维护并持续改进经管理层批准的信息安全管理体系，明确界定角色、	若客户作为数据中心运营商，应建立并持续优化信息安全管理体系，明确角色与职责，确保安全审计机制完善，设置安全联络人对接监管和客户，制定并传达新技术与设备的使用政策，并强化关键网络安全控制措施。 若客户作为在数据中心托管业务方，应指定安全联系人与数据中心运营商保持沟通性。	华为云参照 ISO 27001 构建了信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性等。 另外，对于数据中心的维护，华为云建立了数据中心运维管理相关的制度与流程，其中包含设备的具体管控措施、例行的维护计划等。

	职责以及信息安全政策和标准的协调机制。DCO 应确保可审计实体的建立和定期更新（例如审查审计范围、确定审计范围的有效性等）。应指定主要和备用的信息安全联络人员，作为与当地主管部门的联络点，并可供客户联系。DCO 还应依据行业标准，建立并记录针对关键和新兴技术、服务及终端设备（例如无线技术、笔记本电脑、移动设备）的可接受使用政策，并向所有相关员工和第三方传达		
4.1.b	确保所有员工和第三方人员在聘用或签订合同前均符合岗位要求，并充分理解其职责、雇佣及合同条款（包括终止条款），以降低盗窃、欺诈或设施滥用风险。数据中心运营商应按照适用的道德准则和合同义务进行背景审查，确保组织所有的资产均被妥善登记并由员工和相关第三方在离职或合同终止时予以归还。同时，应建立并实施信息安全培训和意识提升计划，要求新入职员工和相关第三方人员必须完成培训，并至少每年对培训内容进行一次复审更新。	若客户作为数据中心运营商，应确保员工和第三方入职前背景审查，明确职责和合约要求，落实资产归还管理；开展入职及年度信息安全培训。	人员任用前，华为云通过既定的新员工背景调查机制对满足特定条件的拟聘员工进行背景审查，同时，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，在聘用员工或外部人员前对其进行背景调查。 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，此外华为云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。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。 为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为云从意识教育普及、宣传活动开展、华为员工商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育，有专门的信息安全意识培训计划，并每年至少执行一次针对全员的安全意识培训，意识教育的形式包括但不限于现场演讲、视频网课等。

			此外，华为云重点关注员工以及外包人员的安全意识培养，制定了可落地的安全意识培训计划并定期执行。
4.1.c	建立针对第三方服务提供商的有效管控框架，该框架应包括：对第三方服务商的尽职调查、协议签订、交付管理、服务绩效保证以及内部控制合规性审查。同时应制定并维护风险管理流程，持续监督第三方服务可能带来的风险及影响。此外，还需确保所使用的开源组件安全可靠，防范通过软件供应链发起的网络攻击。	1. 若客户作为数据中心运营商，应建立并执行第三方管理框架，包括尽职调查、合约管理、绩效监控和内部控制审查；制定第三方风险管理流程；确保开源软件使用安全，防范软件供应链攻击。 2. 华为云的云监控（CES）服务可实现对客户自身云资源的使用情况和绩效的监控。华为云可以根据客户的需求按照 SLA 向客户提供服务报告。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。在华为云内部，华为云已建立供应商选择和监督体系，并规范了研发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。 在华为云内部，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，管理其访问权限不应超过其服务所必须。供应商的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。 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。在上线前，引入的开源软件均遵从华为公司发布的安全配置规范要求进行加固后才能应用到生产环境。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。

4.1.d	确保自身及其第三方服务提供商通过定期审查，符合数据中心运营商（DCOs）制定的信息安全与风险管理政策、标准、程序及合同义务。数据中心运营商应建立相关程序、培训或意识提升措施，以及相应的政策执行机制，以防止员工进行未经授权的访问，并通过可接受使用政策或协议来执行与相关第三方及终端用户的商业协议。同时，应确保密码控制措施的使用符合相关协议、适用法律法规的要求。	若客户作为数据中心运营商，应定期审查自身及第三方的合规情况，防止未经授权访问，实施员工与第三方的可接受使用政策，开展培训提升安全意识，并确保加密措施符合合同及法规要求。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。在华为云内部，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。 华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。 在华为云内部，华为云在引入供应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，管理其访问权限不应超过其服务所必须。供应商的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。
4.1.e	确保对其网络和系统中执行的活动及发生的事件进行持续跟踪和记录保存，保存期限应足以检测任何未经授权的活动，并在发生安全事件（如访问违规）时便于调查和解决。数据中心运营商应确保网络和系统活动的审计跟踪被完整记录、妥善保护并定期审查。	1. 若客户作为数据中心运营商，应记录并保护网络和系统活动日志，保留足够时间用于追踪异常，定期审查审计记录，支持安全事件的检测与调查。 2. 若客户作为在数据中心托管业务方，在发生安全事件应配合数据中心运营商调查。 3.华为云的云日志（LTS）服务，用于收集来自主机和云服务的日志服务，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为	在日志保存过程中采取安全措施防止日志被篡改，以确保支撑网络安全事件回溯和合规。为确保日志数据安全，安全日志会进行统一备份或归档，并依照数据安全管理的要求，限制安全日志使用的申请及权限，仅允许授权人员因必要原因进行安全日志的查询，确保受控使用。华为云遵从法律法规要求，具备集中、完整的日志审计系统，具备强大的数据保存及查询能力，确保所有日志内容保存时间超过 6 个月。

		客户提供实时、高效、安全的日志处理能力。 4. 华为云的云审计服务（CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。	
4.1.f	确保其网络和系统采用安全设计和配置，防止因系统配置薄弱而产生未授权入口点或遭受恶意活动攻击。数据中心运营商应当：制定配置标准；实施针对恶意代码威胁的防护措施；确保及时应用安全补丁；限制并管控实用程序的使用；实施控制措施以限制使用未经批准或未授权的软件等。	1. 若客户作为数据中心运营商，应制定安全配置标准，防止系统配置漏洞；部署防恶意代码措施，及时更新补丁，控制工具和软件使用，避免未经授权的软件运行。 2. 客户可使用华为云的企业主机安全（HSS）服务对主机进行基线检查，包括检测系统口令复杂度策略、经典弱口令、风险账号，以及常用系统与中间件的配置，以识别不安全项目，预防安全风险。	华为云对支撑业务运营的服务器操作系统、数据库管理系统及网络设备建立了统一的基线配置标准，以实现对服务基线配置的统一管理，明确华为云生产环境中各系统/组件的安全配置要求，并确保安全配置的有效执行和持续改进。华为云参考互联网安全中心（CIS - Center of InternetSecurity）安全基线并将融入华为云 DevSecOps 流程中并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。华为云的运维团队根据内部的安全基线管理规范，定期检查并更新网络设备安全参数设置。华为云对主机操作系统、虚拟机、数据库、web 应用组件等均进行安全配置加固并进行定期检查。
4.1.g	开展安全测试并实施全网监控措施，以主动及时地检测网络和系统中的漏洞及恶意软件。数据中心运营商应当：在基础设施、应用程序发生重大变更或定期开展时，执行内外漏洞扫描及来自互联网的网络层和应用层渗透测试；同时确保第三方开源组件的使用安全，防范通过软件供应链发起的网络攻击。	1. 若客户作为数据中心运营商，应定期开展安全测试和漏洞扫描，实施网络与系统监控，进行渗透测试，确保开源组件安全，防范软件供应链攻击。 2. 客户可使用华为云的企业主机安全（HSS）服务提供的资产管理、漏洞管理、基线检查、入侵检测等功能，帮助客户更方便地管理主机安全风险，实时发现并阻止黑客入侵行为，以及满足等保合规的要求。	华为云建立了漏洞定期扫描机制，每月对报告范围内的产品执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，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。华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。 华为云使用IPS入侵防御系统、Web 应用防火墙（WAF -Web Application Firewall）、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。 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。在上线前，引入的开源软件均遵从华为公司发布的安全配置规范要求进行加固后才能应用到生产环境。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。
4.1.h	制定新应用程序、系统、数据库、基础设施、服务、运营及设施的开发或获取政策和流程，确保安全成为信息系统及相关业务流程的组成部分。	若客户作为数据中心运营商，应制定并实施开发或引入新系统、服务、设施等的安全政策与流程，确保安全要求融入设计和业务流程中。	华为云已制定开发安全管理相关制度，对华为云服务在规划、设计、开发、部署、运维和用户支撑环境应遵循的安全编程规范及应用安全开发规范进行了定义。同时，华为云规范了采用 DevOps 开发模式的产品/服务在部署和发布阶段流程，当中规范了对环境隔离的相关要求，提高生产环境稳定性。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。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。

4.1.i	实施加密及安全的加密密钥管理措施，确保电子传输或存储的敏感信息免遭未经授权的使用或泄露。数据中心运营商应建立密钥管理程序，涵盖密钥管理生命周期的所有环节（包括密钥材料的生成、分发、使用、存储、归档、更换和销毁）。	1.若客户作为数据中心运营商，应实施加密和完整的密钥管理流程，覆盖密钥的生成、使用、存储、更换和销毁，确保敏感数据在传输和存储中受到保护。 2. 华为云的数据加密（DEW）服务是一款综合的云上数据加密服务。为客户提供专属加密、密钥管理、凭据管理、密钥对管理等服务，使用 DEW 可以解决数据安全、密钥安全、密钥管理复杂等问题。	华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。
4.1.j	实施管理控制措施，确保特权账户创建、维护和删除相关策略、标准及程序的执行。数据中心运营商应建立正式的审查和撤销流程，定期评估权限和访问级别的适当性，并及时取消或移除访问权限；实行职责分离和工作范围划分，减少信息资产遭到未经授权或无意修改及滥用的机会；对所有服务和应用程序账户实施控制措施（如每年至少两次更换服务认证凭证）；系统配置变更（特别是重大或敏感变更）需设置多重审批。	若客户作为数据中心运营商，应实施特权账户管理制度，定期审查权限，及时撤销无效账户，控制服务账号的使用，定期更换凭证，关键配置变更须多重审批，确保职责分离防止滥用。	华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求。华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，特权账号被严格纳管回收。特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。仅在员工职责所需时，对其授予特权或应急账号。所有特权或应急账号的申请需要经过多级的评审和批准。华为云仅会在得到客户授权后登录租户的控制台或者资源实例协助客户进行维护。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。 华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。 华为云制定了密码策略及账号口令安全相关管理规范，包括规定密码长度、复杂度、更改周期，密码中不允许包含用户ID，不可使用易被破解的常用口令

			以及最近5次使用过的密码等。对秘密鉴别信息的分配进行管理。新建系统中的账号密码在首次使用前由用户进行更改，当用户需要重置密码时对其身份进行验证。 华为云制定了变更管理的管理规定和变更流程，定义了涵盖变更实施前、实施中及实施后应遵循的网络安全要求，以防止未授权变更。例如，变更前，各项变更均需通过多个环节的审核；变更实施中，会通过日志记录、操作监控及双人操作等方式确保变更安全实施，并确保变更过程可追溯；变更后，对变更实施专人验证，确保变更达到预期效果，不会造成网络安全风险。
4.1.k	实施网络分段和安全控制措施，将其网络和系统划分为独立的网络域并与公共网络（即互联网）隔离。数据中心运营商应基于业务需求和安全要求，在网络域之间实施适当的访问控制，并部署网络入侵检测或防御系统以检测/阻止异常网络活动。	1. 若客户作为数据中心运营商，应实施网络分段，将内部系统与互联网隔离；按业务与安全需求设定访问控制，并部署入侵检测/防御系统，防止异常网络行为。 2. 华为云的Web应用防火墙（WAF）服务，通过对HTTP(S)请求进行检测，为客户提供识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击的服务，保护Web服务安全稳定。3. 客户可以使用华为云提供的虚拟私有云（VPC）服务，实现不同区域之间网络隔离。VPC可为租户构建出私有网络环境，实现不同租户间在三层网络的	华为云基于业务功能及风险等级将生产及非生产环境划分为多个安全区域，DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS –Object - Based Storage）、运维管理区（OM – Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。 华为云使用IPS入侵防御系统、Web应用防火墙（WAF -Web Application Firewall）、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。

		完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络ACL和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。	

8 华为云如何遵从及协助客户满足《云服务韧性和安全性咨询管理》

IMDA 于 2025 年 2 月 25 日发布了《云服务韧性和安全性咨询指南》，为云服务提供商提供框架，涵盖 7 类措施以提升云服务的安全性和韧性。该指南建议云服务提供商实施的措施涉及安全测试、用户访问控制、数据治理以及灾难恢复规划等领域。

当客户遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

8.1 云治理

编号	具体控制要求	华为云的内部实践
2.2	云服务提供商（CSPs）应确保在其整体管理架构中落实信息安全管理。	华为云参照ISO 27001构建了信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性等。 华为云遵循已建立的信息安全管理体系，包括资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性得等多个安全领域，全方位保护客户系统和数据的保密性、完整性和可用性。华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
2.3	云服务提供商（CSPs）应确保所有员工和第三方人员在聘用或签约前符合岗位要求，并充分理解其职责、雇佣及合同条款（包括终止条款），以降低盗窃、欺诈或设施滥用的风险。	人员任用前，华为云通过既定的新员工背景调查机制对满足特定条件的拟聘员工进行背景审查，同时，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，在聘用员工或外部人员前对其进行背景调查。 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，此外华为云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。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。 为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为云从意识教育普及、宣传活动开展、华为员工商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育，有专门的信息安全意识培训计划，并每年至少执行一次针对全员的安全意识培训，意识教育的形式包括但不限于现场演讲、视频网课等。 此外，华为云重点关注员工以及外包人员的安全意识培养，制定了可落地的安全意识培训计划并定期执行。
2.4	云服务提供商（CSPs）应建立并维护针对云服务的专项风险管理计划，以识别、量化、优先排序并缓解或解决影响云服务运营及信息资产的风险。	华为云各业务团队根据要求定期执行信息安全风险评估，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审，确保符合公司风险管理要求。风险评估报告完成后由高级管理层进行审批。风险评估的主要流程如下： ● 风险管理人员识别各业务场景中所涉及的固有风险，基于华为云面临的威胁和脆弱性进行风险评估； ● 基于固有风险清单，结合已有的风险管控措施，输出残余风险清单，并将风险及时录入风险管理平台，包括风险描述、所属领域、风险等级、风险来源等； 基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。风险评估报告完成后由高级管理层进行审批。
2.5	云服务提供商（CSPs）应建立有效的管控框架，对支持云环境的第三方服务提供商进行管理。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。在华为云内部，华为云已建立供应商选择和监督体系，并规范了研发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。 在华为云内部，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，管理其访问权限不应超过其服务所必须。供应商的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。 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。在上线前，引入的开源软件均遵从华为

		公司发布的安全配置规范要求进行加固后才能应用到生产环境。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。
2.6	云服务提供商（CSPs）应确保自身及第三方服务提供商遵守其信息安全与风险管理政策、标准、程序及合同义务。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。在华为云内部，华为云已建立供应商选择和监督体系，并规范了研发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。 华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。 在华为云内部，华为云在引入供应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，管理其访问权限不应超过其服务所必须。供应商的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。
2.7	云服务提供商（CSPs）应实施事件管理控制措施，确保及时通报影响云环境中信息资产和系统的信息安全事件及漏洞。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划和流程，作为流程的一环节，在安全事件得到遏制后，华为云会做根本原因分析，并制定应对和预防措施。同时，华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。
2.8	云服务提供商（CSPs）应确保仅授权用户可随时访问云环境中存储的数据。	华为云制定了数据安全策略及数据安全保护管理规定，对数据资产的分级分类标准进行了定义，同时明确了数据匿名化及标签化处理标准，对数据在整个生命周期中须遵循的安全措施进行了规范。同时，华为云制定了云服务安全与隐私活动操作指导，规范云服务在产品生命周期中应遵循的隐私保护要求。 华为云作为云服务提供商，定义了华为云数据安全责任共担模型。在与客户签订的用户协议中明确划分了客户与华为云数据的所有权、安全责任和义务。对于客户内容数据，华为云承诺不触碰客户的内容数据。对于客户的采购相关的信息，华为云将依照数据保留条款、隐私声明等协议予以保护，在处理过程中，遵循数据最小化原则收集、存储和使用客户的信息，并通过全面的数据保护措施确保客户的账户信息安全。 如果客户的业务数据中涉及敏感个人数据，云服务将默认加密存储该等数据，在非信任网络之间的传输的数据都是被加密的。在信息传输过程中使用安全加密信道（如HTTPS），对存储的静态数据使用安全加密算法进行加密保护，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。 华为云遵循华为公司的管理要求，制定了数据留存规范，其中

		对各类数据的留存期限进行了规定。在存储个人数据时不超过实现数据处理目的所必要的期限。华为云定期对收集、使用、披露个人数据的目的进行审核，对不再需要的个人数据进行匿名化或删除等安全处理。 华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。此外，华为云还规范了业务恢复策略的制定，确保业务能在恢复时间目标内恢复到可接受水平。 华为云制定并实施移动介质管理规定，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。 华为云提供的云数据迁移服务（CDM），支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。

8.2 云基础设施安全

编号	具体控制要求	华为云的内部实践
2.9	云服务提供商（CSPs）应确保对云环境中执行的活动和发生的事件进行持续跟踪和记录保存，保存期限应足以检测任何未经授权的活动，并在发生安全事件（如访问违规）时便于调查和解决。	在日志保存过程中采取安全措施防止日志被篡改，以确保支撑网络安全事件回溯和合规。为确保日志数据安全，安全日志会进行统一备份或归档，并依照数据安全管理的要求，限制安全日志使用的申请及权限，仅允许授权人员因必要原因进行安全日志的查询，确保受控使用。华为云遵从法律法规要求，具备集中、完整的日志审计系统，具备强大的数据保存及查询能力，确保所有日志内容保存时间超过 6 个月。
2.10	云服务提供商（CSPs）应确保云基础设施中的系统及支撑网络采用安全设计和配置，防止因系统配置薄弱而产生未授权入口点或遭受恶意活动攻击。	华为云对支撑业务运营的服务器操作系统、数据库管理系统及网络设备建立了统一的基线配置标准，以实现对服务基线配置的统一管理，明确华为云生产环境中各系统/组件的安全配置要求，并确保安全配置的有效执行和持续改进。华为云参考互联网安全中心（CIS － Center of InternetSecurity）安全基线并将融入华为云 DevSecOps 流程中并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。华为云的运维团队根据内部的安全基线管理规范，定期检查并更新网络设备安全参数设置。华为云对主机操作系统、虚拟机、数据库、web 应用组件等均进行安全配置加固并进行定期检查。

2.11	云服务提供商（CSPs）应对云基础设施（包括服务、虚拟机及物理基础设施）开展安全测试并实施监控措施，以主动及时地检测漏洞和恶意软件。	华为云建立了漏洞定期扫描机制，每月对报告范围内的产品执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，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。华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。 华为云使用 IPS 入侵防御系统、Web 应用防火墙（WAF -Web Application Firewall）、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。
2.12	云服务提供商（CSPs）应实施系统获取和开发安全控制措施，确保安全成为信息系统及相关业务流程的有机组成部分。云服务提供商应针对新应用程序、系统、数据库、基础设施、服务、运营及设施的开发或获取制定政策和程序。	华为云已制定开发安全管理相关制度，对华为云服务在规划、设计、开发、部署、运维和用户支撑环境应遵循的安全编程规范及应用安全开发规范进行了定义。同时，华为云规范了采用 DevOps 开发模式的产品/服务在部署和发布阶段流程，当中规范了对环境隔离的相关要求，提高生产环境稳定性。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。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。
2.13	云服务提供商（CSPs）应实施加密及安全的加密密钥管理措施，确保电子传输或存储的敏感信息免遭未经授权的使用或泄露。	华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。 华为云会限制未经授权的基于 Web 的电子邮件服务的访问，防止电子邮件地址免受欺骗、垃圾邮件和网络钓鱼之类的恶意活动的侵害。

8.3 云运营管理

编号	具体控制要求	华为云的内部实践
2.14	云服务提供商（CSPs）应实施运营安全控制措施，确保云服务的运营具备文档化、安全性、可靠性、韧性和可恢复	华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采

	性。	取进一步解决方法，避免对租户云服务的系统性能造成影响。 华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。华为云作为云服务提供商，确保各项云技术的安全开发、配置和部署以及所提供云服务的运维运营安全。
2.15	云服务提供商（CSPs）应实施变更管理控制措施，确保云基础设施的变更按计划且经授权执行。	华为云制定了变更管理的管理规定和变更流程，对不同变更类型应遵循的不同的变更管理流程，包括申请、评审及实施相关变更进行了定义，各项变更均需通过多个环节的审核，并依据变更的紧急程度等因素对变更进行分类。 变更申请必须提交变更方案，其中须提供回退方案和回退的方式，对现网产生影响第一时间按照变更方案启动问题，如果变更失败会执行变更回退。 华为云研发环境采取分级管理，对开发环境进行包括物理隔离、逻辑隔离、接入访问控制、数据传输通道审批及审计等保护措施。华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。 华为云建立安全补丁管理的流程，保证安全补丁在 IT 安全标准规定的期限内完成安装。同时，华为云制定了漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，不断优化云平台及云产品默认安全配置、及时在规定的期限内应用修补措施或补丁、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等。

8.4 云服务管理

编号	具体控制要求	华为云的内部实践
2.16	云服务提供商（CSPs）应实施云服务管理控制措施，确保与云服务及支撑网络特权账户创建、维护和删除相关的政策、标准及程序得到执行。	华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求。华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，特权账号被严格纳管回收。特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。仅在员工职责所需时，对其授予特权或应急账号。所有特权或应急账号的申请需要经过多级的评审和批准。华为云仅会在得到客户授权后登录租户的控制台或者资源实例协助客户进行维护。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。 华为云的相关人员遵循华为公司的IT安全标准，其中明确不允许以明文形式通过Internet、无线设备传送密码，密码存储在华为公司系统中时须使用业内认可的加密技术对密码进行加密。

		此外，华为云要求为用户建立安全的密码重置流程，密码重置应验证用户身份，比如公司邮箱验证码、预留手机号验证码等。 华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。 华为云制定了密码策略及账号口令安全相关管理规范，包括规定密码长度、复杂度、更改周期，密码中不允许包含用户 ID，不可使用易被破解的常用口令以及最近5次使用过的密码等。对秘密鉴别信息的分配进行管理。新建系统中的账号密码在首次使用前由用户进行更改，当用户需要重置密码时对其身份进行验证。 华为云制定了会话超时策略、账号登陆和锁定策略。其中明确系统支持根据账号、角色、IP等多种特征组合来确定是否允许通过认证建立认证后的会话，同时必须使用会话 Token 对敏感和关键的操作进行校验以确保会话的真实性。此外管理员在进行系统维护时，查看或检测到非法用户会话时，可通过管理界面强制该用户下线，并清除用户的会话信息。同时设置会话超时机制，在一段时间未收到消息后，可进行会话锁定或返回登录页面，目前超时页面会话为30分钟。 华为云自身使用行业广泛使用的AES强效加密法对平台内的数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。 在华为云内部，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，管理其访问权限不应超过其服务所必须。供应商的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。 华为云制定了变更管理的管理规定和变更流程，定义了涵盖变更实施前、实施中及实施后应遵循的网络安全要求，以防止未授权变更。例如，变更前，各项变更均需通过多个环节的审核；变更实施中，会通过日志记录、操作监控及双人操作等方式确保变更安全实施，并确保变更过程可追溯；变更后，对变更实施专人验证，确保变更达到预期效果，不会造成网络安全风险。

8.5 云服务客户访问

编号	具体控制要求	华为云的内部实践
2.17	云服务提供商（CSPs）应实施云用户访问控制措施，确保建立并执行相关政策、标准及程序，以管理用户账户的创建、维护和删除，限制访问并保护用户凭证，防止对信息和信息系统的未授权访问。	华为云制定了公司用户账号权限管理的要求，规范华为云员工在申请、维护和注销权限时应遵循的流程。同时，华为云制定了运维账号的生命周期管理，包括帐号的开销户管理、帐号责任人/使用人管理、口令管理、开销户监控管理等，帐号一旦建立，立即纳入帐号管理员的日常维护管理工作。所有运维帐号，所有设备及应用的帐号均实现统一管理，并通过统一审计平台集中监控，并且进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。此外，针对华为云云平台账号，华为云制定了公有云账号权限管理要求及流程，明确了对账号的分类管理和访问控制策略。对云服务的访问通过统一身份认证服务（IAM）对用户进行访问控制和权限管理。 华为云设置了不成功的登录尝试阈值以预防无限制的非法密码登录尝试，目前最大的密码登录尝试次数5次。对于系统、中间件和网络基础设施的成功和失败的登录尝试均保留日志记录，通过定期的日志审查和日志告警，对非法登录或非法登陆未遂事件进行报告。 华为云制定了密码策略及账号口令安全相关管理规范，包括规定密码长度、复杂度、更改周期，密码中不允许包含用户 ID，不可使用易被破解的常用口令以及最近5次使用过的密码等。对秘密鉴别信息的分配进行管理。新建系统中的账号密码在首次使用前由用户进行更改，当用户需要重置密码时对其身份进行验证。 华为云自身使用行业广泛使用的AES强效加密法对平台内的数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。 华为云制定了会话超时策略、账号登陆和锁定策略。其中明确系统支持根据账号、角色、IP等多种特征组合来确定是否允许通过认证建立认证后的会话，同时必须使用会话 Token 对敏感和关键的操作进行校验以确保会话的真实性。此外管理员在进行系统维护时，查看或检测到非法用户会话时，可通过管理界面强制该用户下线，并清除用户的会话信息。同时设置会话超时机制，在一段时间未收到消息后，可进行会话锁定或返回登录页面，目前超时页面会话为30分钟 身份认证及鉴权：华为云对每个 API 请求通过与华为云 IAM 的集成进行身份验证，确保只有经过身份验证的用户才能访问和管理云监控信息，且传输通道通过 TLS 加密。华为云 API 网关对用户命令支持二级权限管理。用户发出命令时，不仅需要通过

		IAM 的身份登录和鉴权，而且命令也需要经过 API 网关的检查鉴权。平台层或应用层接到命令后，会再次对用户的权限进行检查判断，只有用户确实拥有当前 API 命令的执行权限，命令才允许执行。所有的访问请求可以通过令牌和访问密钥两种方式认证。

8.6 租户与客户隔离

编号	具体控制要求	华为云的内部实践
2.18	云服务提供商（CSPs）应实施租户和客户隔离控制措施，限制同一物理资源内的用户访问，并隔离网络和系统环境，确保客户之间不会因数据丢失、滥用和隐私侵犯而相互构成风险。	华为云基于业务功能及风险等级将生产及非生产环境划分为多个安全区域，DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS –Object - Based Storage ）、运维管理区（OM –Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能， 确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制。 作为华为云平台操作系统，华为统一虚拟化平台(UVP)通过对服务器物理资源的抽象，将CPU、内存、I/O等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑源， 在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。主机内由Hypervisor提供的虚拟交换机（vSwitch）通过设置VLAN、VXLAN、ACL等属性确保虚拟机在网络层的逻辑隔离。同时，UVP支撑的CPU、内存、I/O隔离进一步实现虚拟机在平台层的逻辑隔离。UVP还提供安全组功能，用于多台虚拟机之间的分组隔离。多台虚拟机之间如果要相互访问，可以建立安全组。同一个安全组内的多台虚拟机默认可相互访问，处于不同安全组的任何两台虚拟机默认禁止相互通信，但可定制配置为允许通信。 虚拟私有云服务（VPC – Virtual Private Cloud）为弹性云服务器构建隔离的、用户自 主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。华为云对云端数据的隔离是通过虚拟 私有云（VPC – Virtual Private Cloud）实施的，VPC 采用网络隔离技术，实现不同租户间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，满足租户更细颗粒度的网络隔离需要。

8.7 云韧性

编号	具体控制要求	华为云的内部实践
2.19	云服务提供商（CSPs）应实施物理和环境安全控制措施，通过适当的程序和评估，防止对云环境和基础设施的未授权物理访问、破坏或干扰。	华为云定期对华为云的硬件、软件、数据、人员和服务进行识别。华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。华为云并使用IPAM对IP资源进行统一的管理。同时，华为云平台部署了HSP主机安全平台套件，对平台资产进行网络安全防护。 华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流程。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。 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。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。 华为云每年会对建立的物理与环境安全相关规范和策略流程进行审阅和更新，同时华为云安全管理部门定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
2.20	云服务提供商（CSPs）应实施业务连续性和灾难恢复控制措施，确保在信息系统故障和灾难导致业务活动中断时能够及时恢复，并尽可能预防此类中断。	华为云制定了业务连续性管理规定，以规范业务连续性相关管理框架、目的和范围、管理目标、角色和职责等内容。华为云已经通过ISO22301业务连续性管理体系标准的认证，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。此外，华为云还制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故

		障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。 华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可以充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。

9 华为云如何遵从及协助客户满足《事件响应检查清单》

CSA 于 2021 年 4 月 11 日发布了《事件响应检查表》，该表是围绕美国国家标准与技术研究院 （NIST） 开发的 IPDRR（识别、保护、检测、响应、恢复）框架构建，旨在指导组织对网络事件的准备、响应和恢复。

当客户遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

编号	具体控制要求	客户关注点	华为云的内部实践
1. 准备阶段	事件准备不仅涉及应急响应准备，还包括通过确保系统、网络和应用程序安全来预防事件。 应急准备： ☐ 指定内部事件响应负责人 ☐ 委任第三方事件响应服务商 ☐ 记录产品/服务供应商联系方式 ☐ 监管机构联系方式 ☐ 执法机关联系方式 ☐ 新加坡网络安全应急响应中心(SingCERT) ☐ 客户联系方式 ☐ 其他：_____ 调查资源准备： ☐ 关键资产及数据清单与存储位置 ☐ 网络拓扑图 ☐ IT系统活动当前基准 ☐ IT系统及软件版本	1. 客户应: ● 指定企业内事件响应负责人，并留存供应商及关键外部机构联系方式； ● 明确所使用的云资源； ● 制定自身的事件响应计划、备份方案、危机沟通及业务连续性策略； ● 分析常见威胁并制定应对措施； ● 向员工和关键人员传达计划内容，定期组织培训与演练。 2. 华为云的云监控（CES）服务可实现对客户自身云资源的使用情况和绩	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 华为云建立了集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现，以确保支撑网络安全事件回溯。

	文档 ☐ 重要数据备份 ☐ 其他：_____ 制定相关计划： ☐ 预防与检测计划 ☐ 遏制、清除与恢复计划 ☐ 危机管理与沟通计划 ☐ 业务连续性计划 ☐ 其他：_____ 事件预防： 识别可能影响组织的攻击类型并制定应对方案： ☐ 恶意软件 ☐ 网络钓鱼 ☐ 分布式拒绝服务攻击 ☐ 勒索软件 ☐ 数据泄露 ☐ 数据损坏 ☐ 其他：_____ 计划沟通与演练： ☐ 向员工及关键利益相关方传达计划 ☐ 用户意识培训 ☐ 定期审查更新计划(如系统上线、新员工入职时或定期) ☐ 计划走查/演练 ☐ 其他：_____	效的监控。华为云可以根据客户的需求按照SLA 向客户提供服务报告。同时华为云为客户提供了Anti-DDoS流量清洗服务，客户可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。 3. 客户可以使用华为云提供的云备份（CBR）服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware 虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致数据不可用的场景前可将数据恢复到任意备份点。客户可使用云硬盘（EVS）中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。华为云还为客户提供了镜像（IMS)服务，客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。客户可以使用对象存储（OBS）服务的版本控制功能，将云上的文档、硬盘、服务器进行备份。	华为云还制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。 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。华为云支持与第三方安全信息和事件管理（SIEM–Security Information and Event Management）系统如 ArcSight、Splunk 对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。 华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案。同时，华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。
2. 检测与分	事件检测与分析是识别事件并评估其影响与严重程度的第一步。	1. 客户应: • 开启并监控自身云服务日志；	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度

析阶段	识别潜在攻击向量： 重点关注常见攻击途径： ☐ 设计缺陷的Web应用 ☐ 系统配置错误 ☐ 互联网下载 ☐ 不良网络安全习惯(如弱密码、使用默认密码、软件过期等) ☐ 人为失误 ☐ 授权第三方 ☐ 其他：_____ 审查事件征兆与指标来源： ☐ 安全软件(如入侵检测系统、SIEM系统、杀毒软件等) ☐ 各类日志(操作系统、服务应用、网络设备等) ☐ 公开信息(如SingCERT警报、厂商漏洞通告等) ☐ 内部人员反馈 ☐ 其他：_____ 初步评估与优先级排序： ☐ 对照基准分析事件 ☐ 核查已知威胁征兆 ☐ 评估事件范围与性质(恶意行为或技术故障) ☐ 确定响应优先级(是否启动危机管理) ☐ 其他：_____ 证据收集： ☐ 事件摘要 ☐ 事件指标 ☐ 系统事件记录 ☐ 响应行动记录 ☐ 受影响系统日志 ☐ 系统取证副本 ☐ 其他：_____	• 使用自身安全工具检测异常活动，或集成供应商提供的监控服务； • 根据事件迹象评估影响并判断是否需通知供应商； • 保存自身相关的事件证据； • 启动客户内部通报流程并视情况通知供应商、监管、客户。 2. 华为云的云日志（LTS）服务，用于收集来自主机和云服务的日志服务，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为客户提供实时、高效、安全的日志处理能力。 3. 客户可使用华为云的企业主机安全（HSS）服务提供的资产管理、漏洞管理、基线检查、入侵检测等功能，帮助客户更方便地管理主机安全风险，实时发现并阻止黑客入侵行为，以及满足等保合规的要求。	和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 华为云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。华为云支持与第三方安全信息和事件管理（SIEM–Security Information and Event Management）系统如 ArcSight、Splunk 对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。 华为云建立了统一的事件分析处理平台实现对安全事件的统一收集，并针对收集上来的安全事件进行统一的跟踪管理，确保安全事件得以被及时处理及修复。

	利益相关方通知： ☐ 董事会 ☐ 监管机构与政府部门(警方、PDPC、CSA、新交所等) ☐ 客户 ☐ 媒体 ☐ 其他：_____		
3. 遏制、清除与恢复阶段	制定遏制策略： ☐ 隔离受影响系统 ☐ 重路由/过滤网络流量 ☐ 防火墙过滤 ☐ 关闭脆弱端口和邮件服务器 ☐ 阻断未授权访问 ☐ 其他：_____ 威胁清除： ☐ 清除恶意软件 ☐ 禁用被入侵账户 ☐ 修补所有受影响主机的漏洞 ☐ 其他：_____ 恢复措施： ☐ 备份恢复 ☐ 系统重建 ☐ 重置密码(管理员与用户) ☐ 加强边界安全 ☐ 验证业务系统完整性 ☐ 其他：_____ 持续监控： ☐ 监测异常活动 ☐ 增强日志记录与监控 ☐ 其他：_____	1. 客户应: ● 如控制权限允许，可自行隔离问题实例、账户或资源； ● 与供应商协同，进行受影响服务的恢复与账号清理； ● 恢复重要业务前，确保已清除威胁并进行完整性验证； ● 开启增强监控，防止后续攻击。 2. 华为云的云备份（CBR）服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware 虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致数据不可用的场景前可将数据恢复到任意备份点。	华为云拥有7*24的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。 华为云建立了统一的事件分析处理平台实现对安全事件的统一收集，并针对收集上来的安全事件进行统一的跟踪管理，确保安全事件得以被及时处理及修复。 华为云建立了集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现，以确保支撑网络安全事件回溯。
4. 事后审查阶段	事后审查阶段 ☐ 分析系统与流程缺陷 ☐ 评估响应计划执行情况 ☐ 制定强化措施	客户应: • 梳理事件发生原因，总结响应得失； • 更新自身事件响应计划；	华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯并形成事件报告总结经验教训，在报告中告知事件的

	□ 经验总结与分享 □ 其他：_____	根据事件影响程度，向客户或业务相关方通报并说明改进措施。	描述、起因、影响、华为云已采取的措施等内容。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。

10 华为云如何遵从及协助客户满足《TR 62: 2018 云中断事件响应指南》

ITSC 于 2018 年 4 月 20 日发布了《TR 62: 2018 云中断事件响应指南》，通过规范云服务中断事件的响应流程，进一步强化新加坡在业务连续性管理与灾难恢复计划方面的实施要求。旨在提升智能国家中云服务提供商的透明度、信任和弹性。该指南侧重于基础设施或系统故障以及环境问题直接相关的云中断，但不包括网络安全和恶意行为。

当客户遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

10.1 云服务客户（CSC）指南

编号	具体控制要求	客户关注点	华为云的内部实践
5.1.2.2 云服务客户（CSC）职责	云服务客户（CSC）应明确以下职责（部分职责需与云服务提供商（CSC）共同承担），并配置适当资源用于管理云服务中断事件全生命周期： —确保向CSP提供明确、可联络的对接人信息； —识别关键数据需求并与CSP协商纳入实施方案，保障业务在云服务中断（特别是长时间中断）期间持续运行； —设计实施必要的弹性架构，与CSP架构形成互补并满足业务目标； —评估CSP支持方案，必要时获取增强支持	1. 客户应主动了解服务商提供的增值服务，设计符合业务需求的弹性架构，设定明确对接人，准备业务连续性计划，及时上报和升级中断事件，配合事件响应与修复，并在中断期间获取关键信息用于后续改进。 2. 客户可以使用华为云提供的云备份（CBR）服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致	华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。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，保证恢复时能及时获取外部支持。

	以满足业务需求； —通过双方约定的渠道提交事件报告； —当服务等级即将或已无法达标时向CSP升级事件； —向CSP确认预计中断时长及恢复时间节点； —启动业务连续性计划/IT灾备计划/危机管理计划，降低中断造成的业务影响；明确需CSP向监管机构通报受监管业务运营情况的要求； —与CSP协同分析其网络事件响应计划（COIR）及承诺，确保符合CSC的数据泄露响应流程/要求，有效管控云中断涉及数据泄露/丢失时的影响； —指派具备资质的技术和业务人员参与中断处置及验证工作。 CSC的积极参与（如向CSP准确提供事件诱因详情、验证问题修复情况）可有效加速云服务恢复进程。 CSC 应在中断事件处置期间及事后向 CSP 获取全部必要信息，为后续可能的中断事件做好预案准备。	数据不可用的场景前可将数据恢复到任意备份点。客户可使用云硬盘（EVS）中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。华为云还为客户提供了镜像（IMS)服务，客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。客户可以使用对象存储（OBS）服务的版本控制功能，将云上的文档、硬盘、服务器进行备份。	
5.1.3 云服务评估	云服务客户（CSC）在采购云服务前应完成以下工作： —开展业务影响分析，识别通过云服务采购实现自动化的业务流程需求； —评估分析云服务不可用期间的潜在业务	客户应根据自身业务影响分析，选择适合的中断保护等级和责任共担模式，评估云中断带来的风险，制定缓解措施，并综合考察服务商的声誉、资质、灾备能力、	商业声誉：华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现大突破。 截至目前，华为云已获得众多全球性、区域性和行业特定的安全合规的

	影响，以及中断期间需采取的风险缓释措施（由CSC和/或CSP执行）； —参照网络事件响应（COIR）框架，评审并选定符合业务需求、能降低云服务中断影响的适用类别。 此外，CSC评估云服务提供商（CSP）时还应考量以下因素： —市场声誉与历史记录； —服务年限； —与云服务客户业务需求相关的认证清单及其适用性； —满足CSC未来需求的扩展能力； —是否具备全面的灾难恢复计划； —第三方对内部控制、风险管理、安全及数据隐私的保证措施； —合同条款。	扩展性和合同条款等因素。	权威认证，全力保障客户部署业务的安全。关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网“信任中心-合规中心”。 业务连续性和灾难恢复计划：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。 风险管理和内部控制（包括IT和网络安全）的有效性：华为云内部制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。 华为云线上的《华为云用户协议》对客户和华为云的安全职责进行划分，华为云《华为云服务等级协议》规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中包含华为云对其分包商的安全承诺。
5.1.4 业务级政策 5.1.5 关键性能指标	在云服务提供商（CSP）选择过程中，云服务客户（CSC）应评估其与客户之间的合同、法律及监管要求，并确认CSP能否满足这些要求且已在合同中明确体现。 基于选定的COIR框架类别（见第4章），CSC应将以下框架参数作为关键性能标准，并确定CSP需达成的具体指标值。这些参数用于评估CSP应对云中断事件的准备程度与承诺水平： —服务可用性（或中	1. 客户应根据自身法律和监管要求，评估并确认合同条款中包含关键性能指标（如服务可用性、通知机制、健康监测和响应计划），并与云服务提供商深入沟通，确保所选服务架构满足业务需求和中断响应目标。 2.华为云的云监控（CES）服务可实现对客户自身云资源的使用情况和绩效的监控。华为云可以根据客户的需求	华为云可以根据客户的需求按照SLA向客户提供服务报告，华为云也会安排专人负责客户方发起的尽职调查。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。 华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。华为云配备了专人与行业机构、风险和

	断时长） —可用性历史记录 —计划性维护通知要求：可用通信渠道、最低提前通知时长 —CSP对云服务健康状态的监测范围：硬件/软件/网络健康状态、硬件/软件/网络容量、合同约定的SLA/KPI指标 —可供CSC使用的健康监测机制 —CSP的COIR计划共享机制 —CSP的COIR计划演练要求 上述参数应纳入 CSC 与 CSP 的合同 SLA 条款。关键性能指标可结合以上所述服务模式及部署模式进行定制化调整。此外，CSC 应与潜在 CSP 就所订阅云服务的架构设计进行深入讨论，确保关键性能目标的实现。	按照 SLA 向客户提供服务报告。	合规组织、地方当局和监管机构保持联系并建立联络点，保证恢复时能及时获取外部支持。 华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对租户云服务的系统性能造成影响。
5.1.6 事件管理要求	在评估过程中选定云服务中断影响类别后，云服务客户（CSC）应依据网络事件响应（COIR）框架，将以下参数作为云服务提供商（CSP）必须满足的中断期间要求进行考量： —CSP的云服务中断事件通知机制，且其通知承诺需满足CSC要求（特别是监管合规要求）； —CSP向CSC通报中断事件的可用通信渠道； —CSC向CSP上报中断事件的可用通信渠道；	1. 客户应明确自身对中断事件通知、沟通渠道、响应时效、恢复目标（RTO/RPO）及支持服务的具体需求，并确保这些要求在合同中明确体现，同时评估多级支持、SLA惩罚机制、数据所有权等条款。 2. 华为云的云审计服务（CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资	华为云拥有7*24的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。 为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的

	—CSP提供的支持服务时段； —CSP的响应时间； —CSP的恢复时间目标（RTO）； —CSP的恢复点目标（RPO）； —CSP提供中断修复进展状态更新的频率； —CSP用于状态更新的可用通信渠道。 此外，CSC评估事件管理要求时还应考虑以下要素： —可用的多样化支持选项； —CSP在未达标情况下的补救措施与违约责任； —服务等级协议（SLA）除外条款，包括各项假设（特别是CSP对CSC角色责任的预设）； —SLA变更的通知机制； —服务接入与退出政策； —软件许可及数据所有权（含衍生数据如审计日志）； —现场访问权限； —获取第三方审计及灾备性能报告的权利； —第三方独立保证的定期提供； —满足事件管理目标的支持方案。 CSC 应与 CSP 明确确认上述要求是否满足，并确保相关条款纳入合同约定。	源跟踪和问题定位等常见应用场景。	程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 在《华为云服务等级协议》中，约定了各项产品/服务的服务等级，包括对服务可用性的承诺，以及未达到承诺的服务补偿。同时，华为云制定线下合同模板，根据不同客户的需求进行定制化。 华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。 华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT 服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。同时，华为云每年定期接受专业第三方审计机构的审核。如有必要，客户可以通过官方渠道向华为云申请获取证书以及审计报告的副本。

5.1.7 灾难恢复计划	作为供应商评估环节，云服务客户（CSC）应充分理解并分析云服务提供商（CSP）IT灾备计划所覆盖的关键业务中断风险。 基于自身风险承受能力与成本效益分析，CSC应制定业务连续性计划及流程，以缓解CSP灾备计划未涵盖的业务中断风险。	客户应深入了解服务商的灾难恢复计划覆盖范围，评估自身的风险承受能力和成本效益，制定补充的业务连续性计划来应对服务商未涵盖的风险。服务商应提供详尽的灾难恢复计划，确保关键业务风险得到覆盖，并支持客户的业务连续性需求。	业务连续性和灾难恢复计划：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。
5.1.8 第三方依赖分析	作为供应商评估环节，云服务客户（CSC）应充分理解并分析CSP对第三方服务的依赖关系，特别是其间的合同安排。CSC应识别和评估CSP所用第三方可能带来的风险，并通过合同与CSP协商制定风险缓解方案。 CSC 的业务连续性计划、IT 灾备计划和危机管理计划应基于自身风险偏好和成本效益分析，对第三方风险进行针对性管控。	客户应重点识别和评估云服务提供商所依赖的第三方合作伙伴及其合同安排，识别潜在风险，并通过合同谈判制定风险缓释措施，同时将这些风险纳入自身的业务连续性、灾难恢复和危机管理计划。服务商应透明披露其第三方依赖关系，配合客户风险评估和风险缓解需求。	华为云也会安排专人积极配合客户对对合同的审查，提供相应的材料。 此外，华为云内部也制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。华为云遵从公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。
5.1.9 云中断准备	当云服务客户（CSC）通过网络事件响应（COIR）框架采购云服务时，应确保所有相关外包风险均得到有效管控或缓解。 在某些情况下，CSC可能可能需要高于COIR框架建议参数的中断保护。此时CSC应选择能提供最佳参数匹配的云服务提供商（CSP），明确其可实施的控制措施，并	客户应确保与云服务提供商签订的合同中涵盖所有外包风险的解决方案，并根据自身风险偏好选择合适的服务等级和保护措施。同时，应制定、测试并维护完整的业务连续性、灾难恢复和危机管理计划，以有效应对可能的云中断事件。	为配合客户满足合规要求并行使对 CSP 的监管，华为云线上的《华为云用户协议》对客户和华为云的安全职责进行划分，华为云《华为云服务等级协议》规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中与客户共同约定相应要求。华为云在一定程度上会遵从客户的合同流程。如有必要，华为云会积极配合客户方发起的尽职调查。

	通过协商达成特定的中断保护要求。 基于风险偏好和成本效益分析，CSC 应实施、测试并维护健全的业务连续性计划、IT 灾备计划及危机管理计划，以补充 COIR 框架建议的防护等级。		
5.2.1 中断管理、监控与处置	当云服务提供商（CSP）确认并通报安全事件后，受影响的云服务客户（CSC）应收集事件关键信息，以便召集具备相关专业能力的利益相关方共同处置。CSC 应确保事件获得充分关注并及时响应。 CSC应基于影响分析和分类开展风险评估，明确事件对自身业务、客户及监管合规的影响程度。 根据影响分析结果，CSC 应制定方案以管控云服务中断事件。	客户在云中断事件发生后应及时收集事件的关键信息，召集相关专业人员参与处置，评估事件对业务和合规的影响，并制定相应的行动方案来控制和管理中断风险。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。
5.2.2 危机管理	云服务客户（CSC）的危机管理团队应在事件升级为危机前及时响应。 该团队应通过电子邮件、热线电话、社交媒体、官方网站及新闻等渠道与受影响客户保持沟通。信息更新的透明度与频次对有效实施危机管理至关重要。 需向受影响客户提供事件报告。 为保障大规模中断事件期间的沟通效率，CSC 应配置充足资源并选择合适的媒介，向客户及其他利益	客户应建立并激活危机管理流程，及时响应潜在危机，确保通过多种渠道透明、及时地向受影响客户和利益相关方通报事件详情、影响及恢复进展，保护组织声誉和客户利益。	华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。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，保证恢复时能及时获取外部支持。

	相关方传达事件报告与处置进展。		
5.2.3 数据泄露/丢失管理	云服务客户（CSC）还应制定并启动行动计划，以减轻数据泄露/丢失带来的监管和法律影响，并履行向相关监管机构的报告义务。必要时，CSC应通知其客户。 完成所有准备工作后，CSC可向数据主体、媒体及监管机构发出通知。 如云服务中断持续超出SLA约定期限，CSC应要求云服务提供商（CSP）提供数据访问权限，以便启动业务运营恢复工作。	1. 客户应制定完善的数据泄露应对方案，确保依法及时通知受影响的数据主体、监管机构及公众，准备好沟通材料和保护措施，降低法律与监管风险，并在中断超时情况下要求服务商提供数据访问支持，保障业务恢复。 2. 客户可以使用华为云提供的云备份（CBR）服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致数据不可用的场景前可将数据恢复到任意备份点。客户可使用云硬盘（EVS）中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。华为云还为客户提供了镜像（IMS)服务，客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。客户可以使用对象存储（OBS）服务的版本控制功能，将云上	客户对其内容数据拥有完全控制权。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。此外，华为云各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。 华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。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，保证恢复时能及时获取外部支持。

		的文档、硬盘、服务器进行备份。	
5.3.1 根本原因分析	云服务客户（CSC）应要求云服务提供商（CSP）在中断事件直接或间接归责于其管控范围时提供根本原因分析报告。此举有助于CSC理解导致中断的关键因素并获取经验教训。同时，CSC应自行开展根本原因分析，识别需缓解的风险以避免未来业务影响。 此外，CSC至少应考虑采取以下步骤： —判定CSP是否存在服务等级协议（SLA）违约及应提供的补偿方案； —评估是否有必要对CSP采取法律行动； —制定应对合规问题的监管措施； —评估数据泄露处置措施的充分性； —组织"经验总结"会议； —启动整改措施（包括培训宣导、业务流程优化、系统改造及第三方合同修订等）； —判断是否需要与受影响客户开展关系修复工作。	客户应要求服务商提供中断根本原因分析报告，进行自身的风险复盘和整改，评估 SLA 违约及补偿，考虑法律和合规措施，完善数据泄露应对，并开展内部培训和客户关系修复。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 在《华为云服务等级协议》中（具体请参见欧洲站的服务等级协议），约定了各项产品/服务的服务等级，包括对服务可用性的承诺，以及未达到承诺的服务补偿。同时，华为云制定线下合同模板，根据不同客户的需求进行定制化。
5.3.2 恢复计划更新	云服务客户（CSC）应启动 IT 灾难恢复（DR）计划、业务连续性计划及危机管理计划的更新流程。相关更新应基于事件经验总结和根本原因分析结果进行完善。	客户应根据中断的根本原因和经验，及时更新和完善 IT 灾难恢复、业务连续性及危机管理计划，提升未来应对能力。	如果需要华为云协助执行客户的灾难恢复计划，华为云会积极配合。同时，华为云在提供高可用基础设施、冗余数据备份、可用区灾备等服务外，还制定了自身的业务连续性计划。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安

			全。如果华为云的灾难测试过程中需要客户的参与，华为云会提前通知。 若测试结果表明业务连续性计划、恢复策略或应急预案等存在不足之处，将对相关文件进行更新。 华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。
5.3.3 政策与程序修订	基于根本原因分析结论及经验总结，CSC 需对相关政策和操作程序进行系统性更新。	客户应根据根本原因分析和经验教训，及时修订相关政策和操作程序。	华为云至少每年审查一次网络安全管理策略和网络安全计划，并根据需要予以更新，以反映业务目标或风险环境的变更情况。政策及流程的变更需要获得高级管理层的审批。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议。

10.2 云服务提供商（CSP）指南

编号	具体控制要求	华为云的内部实践
6.1.2 评估与分析	云服务提供商（CSP）可开展业务影响分析，从财务、声誉及法律层面评估云服务中断对自身及云服务客户（CSC）的影响。 CSP应通过风险评估识别设施、IT系统、流程、数据及第三方服务中可能导致云中断的单点故障。同时应与CSC协同识别并评估云服务所托管数据的类型与重要性。 作为风险评估的组成部分，CSP需特别分析云服务对第三方的依赖关系，尤其是相关合同安排。应全面评估第三方服务带来的风险，并通	华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。如果客户在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。 在华为云内部，华为云建立了正式的采购审核流程，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。协议中包含对于双方的责任和义务、服务内容以及供应商的网络安全和隐私数据处理的要求，同时通过保密协议对违反保密性的条款进行了约束。此外，华为云已建立供应商选择和监督体系，并规范了研发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。

	过合同协商制定风险缓解方案。 CSP应基于其风险容忍度及成本效益分析，制定针对第三方风险的风险管理计划。 CSP应根据风险评估中识别的单点故障和业务影响分析中确定的恢复优先级，制定连续性策略以降低风险。 CSP 应利用本阶段关键分析成果，最终形成事件响应计划。	
6.1.3.1 COIR 计划范围	云事件响应（COIR）计划至少应包含以下云服务中断事件管理要素： —云中断事件识别与通知； —中断事件管理、监控与控制； —危机管理； —根本原因分析； —数据抢救方案； —事后报告与整改； —弹性恢复计划； —政策与流程。 该计划应记录现有的事件检测触发机制（手动或自动），包含基于风险的评估标准以判定事件影响程度，并建立根据事件影响等级启动的内部/外部升级流程（含联系人信息）。计划还需通过关联IT灾备和/或业务连续性计划，制定中断时长预估及恢复流程。评估标准应明确界定事件升级为灾难和/或危机的临界条件。	事件检测和响应：华为云内部制定了完善的安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。在事件解决后，会根据具体情况向客户提供事件报告。 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。

	CSP应制定应对"压力场景"的行动方案，覆盖影响大量CSC及云服务的大规模中断事件。 CSP应规划额外容量及通讯机制以应对大规模客户沟通需求。 COIR 计划应规范内外部沟通流程，明确利益相关方的信息需求、角色职责及更新频率要求。CSP 需为 COIR 计划的制定、维护、演练和执行设立角色及职责。	
6.1.3.2 COIR 计划的演练与更新	云服务提供商（CSP）应建立事件响应计划更新机制，确保其时效性和适用性。 CSP应制定涵盖演练类型、角色职责、范围、频率及参与方（包括第三方和CSC）。演练类型应包含CSP对CSC的合同、法律及监管义务的履行情况。 在演练计划中，CSP需设计针对大规模中断的压力测试场景，覆盖影响大量CSC和云服务的极端情况。 CSP应在每次演练后编制报告，记录发现的问题及管理层限期整改方案，并采用基于风险的优先级排序标准。报告应共享给相关利益方。 CSP应根据商定的整改方案（包括演练发现问题的处置措施）修订事件响应计划。	华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。 华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。 华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯，并形成事件报告总结经验教训，在报告中告知事件的描述、起因、影响、华为云已采取的措施等内容。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。

	CSP 需书面明确角色职责，并建立 COIR 计划定期更新机制。当组织机构发生重大变更时，也应及时执行计划更新。	
6.2.2 云中断管理、监控与控制	若事件无法确认为云服务中断事故，云服务提供商（CSP）应将其记录为普通事件并停止处置流程。 对于已确认的中断事件，CSP应开展基于风险的影响分析与分级评估。 基于影响分析结果，CSP应启动行动方案管控云中断事件，并根据事件性质与影响范围调配额外人员。	事件检测和响应：华为云内部制定了完善的安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。在事件解决后，会根据具体情况向客户提供事件报告。 为向客户提供持续、稳定的云服务，华为云遵循 ISO22301 业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。
6.2.3 危机管理	危机管理团队应通过电子邮件、热线电话、社交媒体、官方网站及新闻公告等渠道，与云服务客户（CSC）及其他相关方保持沟通。 应向CSC提供包含以下（但不限于）内容的事件报告： —事件性质与范围的概述； —事件相关细节说明； —事件潜在影响的评估； —预计停机时长； —服务中断原因； —CSP已采取的处置措施； —需CSC配合的行动；以及 —受影响的基础设施。 发生大规模中断时，CSP应配置充足资源并	华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。 事件检测和响应：华为云内部制定了完善的安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。在事件解决后，会根据具体情况向客户提供事件报告。 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，保证恢复时能及时获取外部支持。 华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。华为云，建立了节点数据备份机制，通过 eBackup 系统实现对节

	选择合适的媒介（如邮件、官网），快速有效地向CSC及其他利益相关方通报事件报告及恢复进展。此举有助于提升沟通效率并履行对CSC的合约义务。 若云服务中断超出协议服务等级（SLA）约定期限，CSP应按CSC要求，以双方约定的安全存储格式提供数据或备份访问权限，以支持CSC开展业务恢复工作。	点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。
6.3.1 根本原因分析	建议云服务提供商（CSP）发布根本原因分析报告，此举有助于增强客户信心。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划和流程，作为流程的一环节，在安全事件得到遏制后，华为云会做根本原因分析，并制定应对和预防措施。同时，华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。 华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯，并形成事件报告总结经验教训，在报告中告知事件的描述、起因、影响、华为云已采取的措施等内容。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。
6.3.2 补救计划	根据云服务中断的影响和严重程度，云服务提供商（CSP）应考虑制定抢救计划，以尽可能快速地重建或抢救记录/数据、设备及基础设施，使服务恢复至全面运行状态（与中断前状态一致）。	华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联（DCI－Data Center Interconnect），满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划，并定期对其进行测试，该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。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。此外，华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。此外，华

		为云还规范了业务恢复策略的制定，确保业务能在恢复时间目标内恢复到可接受水平。华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面。
6.3.3 事后报告与整改	事件关闭流程应包含（但不限于）以下步骤： —评估可能需要采取的法律行动； —判定服务等级协议（SLA）违约情况及应向CSC提供的补偿方案； —召开"经验总结"会议； —启动整改措施（包括培训宣导、业务流程优化、系统改造及第三方合同修订等）； —更新云事件响应（COIR）程序；以及 —判断是否需与受影响客户/CSC开展关系修复工作。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。
6.3.4 弹性计划	云服务提供商（CSP）应启动更新流程，对其 IT 灾难恢复计划、业务连续性计划及危机管理计划进行修订。相关更新应基于事件经验教训及根本原因分析结果。	若测试结果表明业务连续性计划、恢复策略或应急预案等存在不足之处，将对相关文件进行更新。 华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。
6.3.5 政策与流程	云服务提供商（CSP）应启动更新流程，对相关政策和流程进行修订。相关更新应基于事件经验教训及根本原因分析结果。	华为云线上的《华为云用户协议》对客户和华为云的安全职责进行划分，华为云《华为云服务等级协议》规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中规定华为云若聘用分包商，需通知客户，并对分包的服务负责等要求。

10.3 使用云中断事件响应（COIR）框架

编号	具体控制要求	客户关注点	华为云的内部实践
7.1 COIR 需求识别	云服务客户（CSC）可参照云事件响应（COIR）框架确定其云服务中断防护需求。	客户应利用 COIR 框架和附录工作表，明确自身云中断保护的关键和可选需求，结	华为云线上的《华为云用户协议》对客户和华为云的安全职责进行划分，华为云《华为云服务等级协议》规定了华为云提供的服务水平。同时，华为云也制定了线

		合服务影响评估，选择适合的保护参数，并将其纳入服务等级协议中以保障权益。	下合同模板，可根据客户的要求，在其中规定华为云若聘用分包商，需通知客户，并对分包的服务负责等要求。
7.2 COIR 实践披露	为提升透明度，鼓励云服务提供商（CSP）运用云事件响应（COIR）框架，就其每项云服务的中断防护能力向客户进行披露。	客户在选择云服务供应商时，应了解评估其公开披露的 COIR 实践信息，结合自身需求和合同条款，确保所选供应商具备符合业务连续性要求的中断应对能力。	华为云已基于 COIR 框架对其云服务中断应对能力进行披露。具体披露内容，可参阅《华为云 COIR 披露表单》。

11 结语

本文描述了华为云如何为客户提供遵从新加坡网络安全监管要求的云服务，并表明华为云遵守新加坡国会，新加坡网络安全局（CSA）以及新加坡资讯通信媒体发展局（IMDA）发布的包括《计算机滥用法》在内的重点监管要求，有助于客户详细了解华为云对新加坡网络安全监管要求的遵从性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合新加坡网络安全监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本文仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对相关新加坡网络安全监管要求的遵从性。

12 版本历史

日期	版本	描述
2025 年 9 月	1.0	首次发布

