华为云 NIST CSF 实践指南

文档版本 1.0

发布日期 2022-05-17

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中国站上开放的产品和服务，以及承载这些产品和服务的数据中心节点。

1.2 发布目的与目标读者

NIST CSF是由美国国家标准与技术研究所（National Institute of Standards and Technology，简称NIST）制定的网络安全框架（Cybersecurity Framework，简称CSF），旨在为寻求加强网络安全防御的组织提供指导，更好地管理网络安全风险。目前该框架已成为全球认可的安全评估体系，华为云在通过独立第三方机构的评估后获得了NIST CSF网络安全框架的认证。

本文档通过介绍华为云如何参照NIST CSF框架构建或提升网络安全、风险管理能力。帮助客户了解：

- 华为云如何基于NIST CSF构建网络安全体系；
- 华为云为客户提供了多种产品帮助其实施NIST CSF网络安全框架。

1.3 基本定义

- 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。
- 关键基础设施：对美国来说至关重要的系统和资产，此类系统和资产的失效或毁灭会对网络安全、国家经济安全、国家公共健康安全或者其中的任意组合造成破坏性影响。
- 移动代码：程序（例如：脚本、宏、或其他便携的指令集）可在不经修改的情况下移植至各类平台集合并可按照完全相同的语义被执行。
- 框架核心：是一系列在关键基础设施领域通用的网络安全活动、预期成果和适用性参考。框架核心包括四个元素：“功能”、“类别”、“子类别”和“参考性文献”。

- 框架实施层：折射出组织风险管理方法的特征，即组织如何看待网络安全风险和其现有的用以管理该类风险的流程。
- 框架轮廓：特定系统或组织选取的框架类别和子类别的成果展现。

2 NIST CSF 简介

2.1 NIST CSF 的发展历程

为了增强美国关键基础设施的韧性以应对网络安全风险，2014年《网络安全加强法案》（CEA）更新了国家标准与技术研究院（National Institute of Standards and Technology，简称NIST）的职责，包括制定和开发网络安全风险框架，供关键基础设施所有者和运营商自愿使用。这将NIST之前在13636号行政命令（Executive Order (EO) 13636）“改善关键基础设施网络安全”（2013年2月）下开发框架版本1.0的工作正式化,并为未来框架演变提供了指导。根据13636号行政命令制定并基于CEA持续演进的框架使用通用语言，以业务和组织需求为基础，以兼顾成本和收益的方式处理和管理网络安全风险，而无需对业务提出额外的监管要求。

2018年4月，NIST改进、澄清并完善了版本1.0，并综合版本1.1草案收到的意见，发布了NIST CSF 1.1版本。

2.2 NIST CSF 框架和主要内容

NIST CSF由框架核心、框架实施层和框架轮廓三部分组成，其框架核心包括五个功能，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（Respond）和安全恢复能力（Recover）。这个能力框架实现了网络安全“事前、事中、事后”的全过程覆盖，帮助企业主动识别、预防、发现、响应安全风险。

NIST CSF的框架核心的5个功能要素介绍如下：

- **识别（Identity）**：帮助组织理解进而管理系统、人员、资产、数据和能力的网络安全相关风险。“识别”功能中的活动是有效使用框架的基础。只有在理解组织业务、支持关键业务的资源以及相关的网络安全风险时，才能使组织根据其风险管理策略和业务需求将资源集中投入到优先级高的工作中。此功能中的类别（Categories）有“资产管理”、“业务环境”、“治理”、“风险评估”和“风险管理策略”等。
- **保护（Protect）**：制订并实施适当的保障措施，确保关键基础服务的交付。“保护”功能对于限制或遏制潜在网络安全事件的影响起到支持作用。此功能中的类别有“访问控制”、“意识和培训”、“数据安全”、“信息保护流程和程序”、“维护”和“保护性技术”。

- **检测（Detect）**：制订并采取适当措施识别网络安全事件的发生。“检测”功能能够及时发现网络安全事件。此功能中的类别有“异常和事件”、“安全持续监控”以及“检测流程”。
- **响应（Respond）**： 制订并实施适当的活动，以对检测的网络安全事件采取行动。“响应”功能支撑对潜在网络安全事件影响进行遏制的能力，此功能中的类别有 “响应计划”、“沟通”、“分析”、“缓解”和“改进”。
- **恢复（Recover）**：制订并实施适当的活动以保持计划的弹性，并恢复由于网络安全事件而受损的功能或服务。“恢复”功能可支持及时恢复至正常运行状态，以减轻网络安全事件的影响。此功能中的类别有“恢复计划”、“改进”和“沟通”。

2.3 框架适用群体

NIST CSF适用于所有依赖技术的组织，无论其网络安全关注点是信息技术（IT）、工业控制系统（ICS）、网络物理系统（CPS）、物联网（IoT）还是更普遍的连接设备。

3 华为云的认证情况

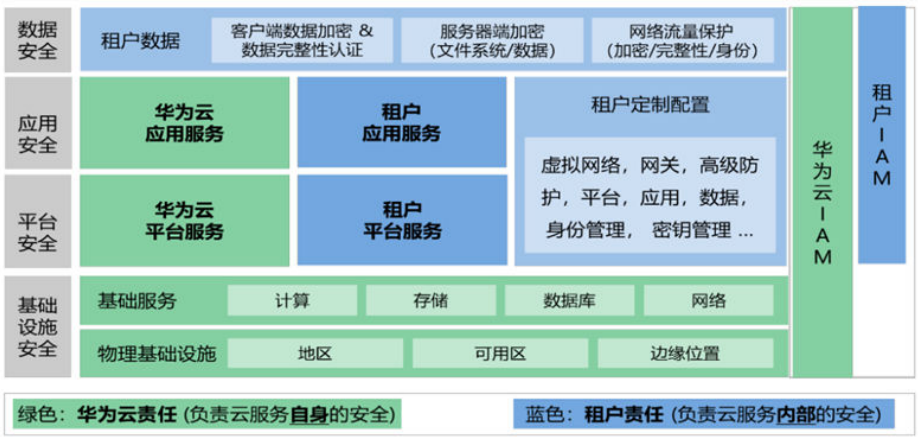
华为云获得了由全球公认的权威标准组织英国标准协会（BSI）颁发的NIST CSF Tier4最高等级认证，成为国内首个获得NIST CSF认证的云服务商，标识了华为云在风险检测、处置、响应、恢复等方面的能力成熟度，表明了华为云内具备为全球用户提供安全可信的云服务的能力。

认证范围覆盖了华为云在其官网发布的产品及服务，以及遍布全球多地的数据中心。如需了解NIST CSF认证详情，可在华为云**信任中心**申请下载NIST CSF评估报告。

4 华为云责任共担模型

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

图 4-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与租户的安全责任详情，可参考华为云已发布的**《华为云安全白皮书》**。

5 华为云如何基于 NIST CSF 框架构建网络安全体系

华为云基于NIST CSF框架对网络安全体系进行了优化，并在日常运营中遵循PDCA循环模型对其进行维护和持续改进，但这并不意味着客户使用华为云的服务就可以通过NIST CSF认证，客户与华为云基于上文的责任矩阵共同承担安全责任，客户应根据其自身的情况，采取相应的措施。

5.1 识别（Identify）

类别	子类别	参考信息	华为云采取的措施	建议客户采取的措施
资产管理（ID.AM）：根据组织对组织目标和组织风险策略的相对重要性，确定和管理使组织实现业务目的的数据、人员、设备、系统和设施	ID.AM-1：盘点组织内的物理设备和系统	ISO/IEC 27001:2013 A.8.1.1 A.8.1.2	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，并明确了资产所有者。	客户负责识别并记录在华为云之外的物理资产（例如，服务器、计算机、网络设备、移动设备、物联网设备、外围设备等）。 客户负责识别并记录软件平台和应用程序清单，并确保记录的信息能准确反映当前现状。
	ID.AM-2：盘点组织内的软件平台和应用程序	ISO/IEC 27001:2013 A.8.1.1 A.8.1.2 A.12.5.1	同ID.AM-1	

	ID.AM-3：组织通信和数据流相映射	ISO/IEC 27001:2013 A.13.2.1 A.13.2.2	华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分区自我保护和容错恢复能力。华为云会维护最新的网络拓扑结构图。 对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过虚拟专用网络（VPN）等方式实现。	客户负责控制其应用程序内以及应用程序与外部系统之间的通信和数据流。并负责授权与外部和内部信息系统的连接，并记录连接信息。
	ID.AM-4：外部信息系统已编入目录	ISO/IEC 27001:2013 A.11.2.6	华为云制定并实施办公计算机安全管理规定，明确办公资产使用人有义务确保所使用资产的安全，并对使用状况负责。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。原则上不使用从网络下载的自由/开源软件，若由于业务需要安装，将对其进行杀毒软件扫描。	客户负责识别和记录所有外部信息系统。
	ID.AM-5：资源（例如：硬件、设备、数据、时间、人员和软件）根据其分类、关键性和业务价值进行优先排序	ISO/IEC 27001:2013 A.8.2.1	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。	客户负责根据资产的分类、重要性和业务价值确定资产的优先级，并根据优先级制定安全保护措施。

	ID.AM-6：建立了所有员工和第三方利益相关者（供应商、消费者、合作伙伴）的网络安全角色和职责	ISO/IEC 27001:2013 A.6.1.1	华为云在各产品、服务的业务团队中明确规定了所有员工及第三方利益相关者对应角色的信息安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的信息安全管理职责。信息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。	客户负责确定公司及其第三方利益相关者的网络安全角色和职责，负责制定对第三方利益相关者的安全要求，并监控第三方服务提供商的合规性
商业环境（ID.BE）：理解并优先考虑组织的使命、目标、利益相关者和活动；此信息用于告知网络安全角色，职责和风险管理决策	ID.BE-1：识别和传达组织在供应链中的角色	ISO/IEC 27001:2013 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2	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要求。 华为云已制定综合采购变更管理规定及流程，按照管理规定严格管理供应商服务的变更。 华为云的灾备策略中规定对于同一服务须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。	客户负责识别、记录和传达他们在供应链中的角色。

	ID.BE-2：识别和传达组织在关键基础设施和其行业领域的地位	ISO/IEC 27001:2013 条款4.1	华为云根据ISO 27001的要求建立并实施信息安全管理体系，并在日常运营中遵循PDCA循环模型对其进行维护和持续改进，在体系建立初期确定内外部环境并识别相关方需求，以确定信息安全管理体系的范围。在组织方面，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。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。	客户负责确定、记录和传达在关键基础架构中的角色。
	ID.BE-3：建立和传达组织使命、目标和活动的优先级	N/A	同ID.BE-2	客户负责确定、记录和传达其组织使命和业务目标的优先级。

	ID.BE-4：建立关键服务交付的依赖关系和关键功能	ISO/IEC 27001:2013 A.11.2.2 A.11.2.3 A.12.1.3	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。 华为云对电气、消防安全执行严格管控。华为云数据中心采用多级保护方案保障业务7*24小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源(UPS)，提供短期备用电力供应。华为云数据中心建筑防火等级均按一级设计施工，使用了A级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统得以控制火情。 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资源进行容量规划，避免资源被过度使用，满足容量需求。同时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。	客户负责识别、记录和传达关键服务交付的依赖关系。

	ID.BE-5：建立所有运行状态的韧性要求，以支撑关键服务交付（例如：在恢复期间、正常操作期间的胁迫/攻击）	ISO/IEC 27001:2013 A.11.1.4 A.17.1.1 A.17.1.2 A.17.2.1	华为云在建设数据中心时会考虑在政治稳定、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。对于入侵、授权等风险，建立了监控机制及响应机制。 华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，排除单点故障的风险，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，应用在数据中心实现N+1部署，在一个数据中心故障的情况下可以将流量负载均衡到其他中心。 华为云已经通过ISO 22301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。	客户负责识别其系统的弹性要求，并根据要求选择服务所在的Region和AZ。
治理（ID.GV）：管理和监控组织的法规、法律、风险、环境和运营要求的政策、程序和流程都已	ID.GV-1：建立和传达组织网络安全策略	ISO/IEC 27001:2013 A.5.1.1	华为云实施文档化的信息安全政策和程序，为操作和信息安全管理提供指导。信息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。	客户负责制定其组织的信息安全政策和程序，为网络安全风险管理提供信息。

理解并告知网络安全风险的管理	ID.GV-2：协调网络安全角色和职责，并与内部角色和外部合作伙伴保持一致	ISO/IEC 27001:2013 A.6.1.1 A.7.2.1 A.15.1.1	华为云在各产品、服务的业务团队中明确规定了所有员工及第三方利益相关者对应角色的信息安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的信息安全管理职责。信息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。 华为云已制定针对公司各类人员的信息安全管理要求，对华为员工、机要岗位员工及外部人员提出分层分级的信息安全管理要求。 针对员工，在其与公司签署的聘用协议中包含保密条款，并明确员工的信息安全责任。 针对外部人员，华为云接口部门在与之签署的合同或协议条款中明确约定对外部人员及所属公司的信息安全管理要求，以及信息安全违规处罚措施。 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。	客户负责确定和记录信息安全角色和职责，并制定和实施网络安全计划，其中包括内部和外部利益相关者的角色和责任，以及沟通和协调方法。

	ID.GV-3：理解和管理关于网络安全的法律和法规要求，包括隐私和公民自由义务	ISO/IEC 27001:2013 A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5	华为云设立了专岗同外部各方保持积极的联系，以追踪法律、法规的相关要求变化。当识别到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。 华为云以全球隐私保护的法律法规为基石，参考业界广泛认可的优秀实践，建设了华为云的隐私保护体系，对隐私和个人可识别信息进行保护。	客户负责识别与网络安全相关的法律法规，并制定、记录和传播有关这些合规要求的政策。
	ID.GV-4：通过治理和风险管理流程解决网络安全风险	ISO/IEC 27001:2013 条款6	华为云制定了信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断，同时根据要求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等。风险评估的目的是识别华为云的威胁和漏洞，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。	客户负责制定、记录和传播网络安全风险管理政策。

风险评估（ID.RA）：组织理解组织运营（包括任务、功能、形象或声誉）、组织资产和个人的网络安全风险	ID.RA-1：识别并记录资产漏洞	ISO/IEC 27001:2013 A.12.6.1 A.18.2.3	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系统、应用、网络进行漏洞扫描。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。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。 华为云会在官网公布已经发现的产品或服务的漏洞并进行预警，客户可查看安全公告以了解漏洞影响的范围，处置方式及威胁级别。	客户负责制定漏洞管理机制，根漏洞扫描流程，以组织定义的频率对其信息系统（例如客户应用程序、数据库和操作系统）进行漏洞扫描，记录、分析漏洞扫描结果，并在定义的响应时间内完成漏洞修复。

	ID.RA-2：通过信息共享平台和来源接收网络威胁信息	ISO/IEC 27001:2013 A.6.1.4	华为PSIRT已建立完善的漏洞感知与收集渠道。在华为官网PSIRT公开了漏洞收集邮箱psirt@huawei.com及漏洞奖励计划https://bugbounty.huawei.com/hbp，鼓励全球漏洞协调组织、供应商、安全公司、组织、安全研究者和华为员工等提交华为产品或解决方案的漏洞。同时，华为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。同时，华为云设立了专有漏洞收集邮箱hws_security@huawei.com，华为云自己的安全运维团队通过自研及商业在线安全扫 描工具，定期执行漏洞扫描任务（扫描不包括租户实例），让华为云环境下的漏洞 “无处可躲”，实现漏洞的“可视化”。	客户负责从信息共享平台收集和分析网络威胁情报，必要时生成内部安全警报，并向相关人员传播。
	ID.RA-3：识别并记录内部和外部的威胁	ISO/IEC27001：2013 条款6.1.2	同ID.GV-4	客户负责制定、记录和传播网络安全风险（包含内部和外部的威胁）管理政策。

	ID.RA-4：识别潜在的业务影响和可能性	ISO/IEC27001：2013 A.16.1.6 条款6.1.2	华为云致力于客户数据的安全和隐私保护，以国际标准为蓝本建立了信息安全管理体系（ISMS）和隐私信息管理体系（PIMS），系统地开展信息安全风险评估和隐私影响评估PIA），充分识别和分析安全与隐私风险，制定并执行处置措施予以应对。 法律遵从是华为在全世界生存、服务、贡献的重要基础，华为云长期致力于严格遵守业务所在国的所有适用法律法规，从外规内化和合规红线的制定，对合规风险进行系统性的识别和管理，并建立突发事件应急预案，开展相关培训和演练，提升组织合规意识和应对突发事件的能力。 同时华为云建立了从供应商到华为云、从华为云到客户的端到端业务持续改进和优化管理，并通过建立政策、组织、制度、流程，基线和 IT 平台，开展业务影响分析和风险评估，提升组织对公司相关制度和流程要求的遵从，确保对日常业务风险的有效管理，保障华为云组织与云服务的业务连续，有效支撑客户系统的稳定运行及业务运作。	客户负责评估和记录潜在风险发生的可能性以及对业务的影响程度。

	ID.RA-5：通过威胁、漏洞、可能性和影响确定风险	ISO/IEC 27001:2013 A.12.6.1	华为云制定了信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断，同时根据要求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等。风险评估的目的是识别华为云的威胁和漏洞，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。	客户负责制定风险评估办法，通过威胁、漏洞、风险发生可能性和风险影响程度评估风险。
	ID.RA-6：确定风险应对措施并确定优先级	ISO/IEC 27001:2013 条款6.1.3	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。	客户负责分析识别的风险，并根据组织定义的风险承受能力确定风险的优先级。

风险管理策略（ID.RM）：确定组织优先事项、约束条件、风险承受能力和假设条件，并用于支持运营风险决策	ID.RM-1：风险管理流程由组织的利益相关者建立、管理和同意	ISO/IEC 27001:2013 条款6.1.3 条款8.3 条款9.3	华为云制定了信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断，同时根据要求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等。风险评估的目的是识别华为云的威胁和漏洞，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。 华为云每年定期开展管理评审，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。	客户负责制定与信息系统相关的风险管理策略。该策略需获得组织利益相关者的同意。
	ID.RM-2：确定并明确说明组织的风险承受能力	ISO/IEC 27001:2013 条款6.1.3 条款8.3	华为云基于风险、治理、控制框架，从数据安全与隐私保护、合规以及运营等层面展开全方位、多维度的风险管理，将华为云服务的风险控制到最小的可接受范围。同时定义了风险的可接受范围并规定了决策风险接受的流程和角色。	客户负责确定组织的风险承受能力级别并获得组织利益相关者的同意。
	ID.RM-3：组织的风险承受能力的决策取决于其在关键基础设施和行业特定风险分析中的角色	ISO/IEC 27001:2013 条款6.1.3 条款8.3	华为云在风险识别阶段会分析业务活动，将识别的固有风险及已有控制措施共同作为风险承受能力的决策因素。	客户负责根据行业标准以及其系统的重要性确定不同级别的风险承受能力。

供应链风险管理（ID.SC）：确定组织的优先事项、约束、风险承受能力和假设条件，并用于支持与管理供应链风险相关的风险决策。组织已建立并实施识别、评估和管理供应链风险的流程。	ID.SC-1：网络供应链风险管理流程由组织利益相关者识别、建立、评估、管理和同意	ISO/IEC 27001:2013 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2	同ID.BE-1	客户负责制定供应链风险管理流程，流程必须由组织利益相关者确定、建立、评估和管理。
	ID.SC-2：使用网络供应链风险评估流程，识别、评估和确定供应商和第三方合作伙伴信息系统、组件和服务的优先级	ISO/IEC 27001:2013 A.15.2.1 A.15.2.2	同ID.BE-1	客户负责根据供应链风险管理流程评估与关键信息系统相关的所有合作伙伴和供应商。
	ID.SC-3：与供应商和第三方合作伙伴签订的合同来用于实施组织网络安全计划和网络供应链风险管理计划目标的适当措施	ISO/IEC 27001:2013 A.15.1.1 A.15.1.2 A.15.1.3	同ID.BE-1 供应商安全和隐私要求包含在已签署的合同协议中。与第三方的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。华为云法务团队也会定期对合同的条款进行审查。	客户应要求其供应商和合作伙伴实施适当的管控措施，以实现供应链风险管理流程所定义的目标。
	ID.SC-4：通过审计、测试结果或其他评估方式对供应商和第三方合作伙伴进行评估，以确认他们正在履行合同义务	ISO/IEC 27001:2013 A.15.2.1 A.15.2.2	同ID.BE-1	客户负责监控和审查其供应商和合作伙伴，以确认他们已按要求履行义务。

	ID.SC-5：与供应商和第三方提供商进行响应和恢复的计划和测试	ISO/IEC 27001:2013 A.17.1.3	华为云安全演练团队定期制定针对不同产品（包含基础服务、运营中心、数据中心、组织整体、第三方供应商等）以及不同场景的演练，以维护业务连续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性计划进行测试。	客户负责制定其业务系统的应急响应和恢复计划，如涉及第三方提供的服务，需联合第三方进行测试。

5.2 保护（Protect）

类别	子类别	参考信息	华为云的回应	客户的责任

身份管理、认证和访问控制（PR.AC）：对物理和逻辑资产及相关设施的访问仅限于授权的用户、流程和设备，并且对授权活动和交易的未授权活动的评估风险一致性进行管理	PR.AC-1：为授权的设备、用户和流程颁发、管理、验证、撤销和审核身份和凭证	ISO/IEC 27001:2013 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3	华为云员工账号管理遵从公司用户账号权限管理规定。 针对云平台账号，华为云制定了公有云账号权限管理要求及流程。对账号进行分类管理并建立访问控制策略，相关文件均通过评审流程并发布。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。 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。 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。 针对外包合作人员账号/权限，管理负责人在外包合作人员离场或不再需要账号/权限时提交注销申请。 主管会审视下属的账号/权限持有情况是否合理，如下属岗位/角色变动，将审视其原有岗位账号/权限是否已注销。	客户负责开发、记录、维护、传播和实施访问控制策略和支持程序。客户负责正确使用华为云的身份和访问管理（IAM）创建和管理用户帐户。

	PR.AC-2：管理和保护资产的物理访问	ISO/IEC 27001:2013 A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8	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。 华为云对于生产及非生产环境使用物理和逻辑隔离手段。在数据中心设计施工和运营时，合理划分了机房物理区域（包括高度敏感区域），合理布置了信息系统的组件，以防范物理和环境潜在危险。 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。 华为云制定并实施办公场所安全管理规定，对员工的安全责任与行为规范提出要求，制定政策和程序并实施访问控制，确保无	不涉及。

			人值守的用户设备有适当的保护。 华为云制定并实施办公计算机安全管理规定，明确办公资产使用人有义务确保所使用资产的安全，并对使用状况负责。员工携带办公便携机外出时将其随身携带或妥善存放，确保便携机中所存储华为信息的安全。如办公计算机丢失或被盗，员工将及时报告。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。	

	PR.AC-3：管理远程访问	ISO/IEC 27001:2013 A.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1	华为云的员工在内部办公网络中使用唯一身份标识。当需要从外部网络接入华为内部办公网络时，需通过VPN接入。 华为云制定了移动设备管理规定，以实施对移动计算设备的统一管理。对移动设备使用的原则、职责、权限要求、设备管理安全要求、网络接入要求及违规处罚等均做出规定并实施。针对便携电脑，机要岗位不配备便携电脑，当便携电脑进入受控区域时需获得批准，同时对便携电脑采取措施以防止丢失后发生数据泄露。 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。为实现对华为云的远程管理，不论是从互联网还是办公网接入，都要首先访问资源池堡垒机，再从堡垒机访问相关资源。	客户负责开发、记录、维护、传播和实施访问控制策略，并根据其访问控制策略为组织控制的移动设备制定使用规范。

	PR.AC-4：管理访问权限和授权，包含最小权限原则和职责分离原则	ISO/IEC 27001:2013 A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5	华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段。华为云运维人员登入运维管理区时必须先通过虚拟专用网络（VPN – Virtual Private Network）接入，再通过堡垒机访问被管理节点。管理员可从此区域访问所有区域的运维接口，此区域不向其他区域开放接口。 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。	客户负责根据用户的工作职能为每个用户提供适当的访问级别，保持适当的职责分离和最低权限。

	PR.AC-5：保护网络完整性（如网络隔离，网络分段）	ISO/IEC 27001:2013 A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3	华为云数据中心节点众多、功能区域复杂。为了简化网络安全设计，阻止网络攻击在华为云中的扩散，最小化攻击影响，华为云参考安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域、业务层面的划分和隔离。安全区域内部的节点具有相同的安全等级。华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。 华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD– Point 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。 关于安全区域的详细介绍可参考《华为云安全白皮书》。	客户负责管理其在华为云上的应用程序的网络访问，通过使用网络分段、防火墙、防病毒和入侵检测来保护网络完整性。

	PR.AC-6：身份被证明并绑定到凭据，并在适当的时候在交互中断言	ISO/IEC 27001:2013 A.7.1.1 A.9.2.1	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。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。同时为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。	客户负责对应用程序采取身份鉴别措施，保证身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，用户身份鉴别信息丢失或失效时，采用技术措施保证鉴别信息重置过程的安全。
	PR.AC-7：用户、设备和其他资产已身份认证（例如：单因子、多因子）并与交易风险相一致（例如：个人的安全和隐私风险以及其他组织风险）	ISO/IEC 27001:2013 A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3 A.18.1.4	同PR.AC-1 华为云制定了密码策略及账号口令安全相关管理规范，对秘密鉴别信息的分配进行管理。新建系统中的账号缺省密码在首次使用前由用户进行更改，当用户需要重置密码时对其身份进行验证。 华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，严格纳管回收特权账号。使用IAM对访问进行管理，支持多因素认证用于登录验证和操作保护，员工每次登陆均需要使用多重身份验证确定身份。也提供会话超时策略、账号登陆和锁定策略。	客户负责制定身份鉴别信息的保护措施，确保具有登录失败处理功能，配置并启用结束会话、限制非法登录次数等相关措施。

意识及培训（PR.AT）：为组织的人员和合作伙伴提供网络安全意识教育，并进行培训，以履行符合相关政策、程序和协议的网络安全相关的义务和职责	PR.AT-1：告知并培训所有用户	ISO/IEC 27001:2013 A.7.2.2 A.12.2.1	在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。	客户负责对内部人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；针对不同岗位制定不同的培训提高计划。
	PR.AT-2：特权用户理解其角色和职责	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的信息安全责任。对于合 同方，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全责任。	客户负责在用户使用特权用户之前对其进行基于角色和职责的培训，并为其制定相应的培训计划。

	PR.AT-3：第三方利益相关者（例如供应商、客户、合作伙伴）理解其角色和责任	ISO/IEC 27001:2013 A.6.1.1 A.7.2.1 A.7.2.2	同PR.AT-2 华为云已制定针对公司各类人员的信息安全管理要求，对华为员工、机要岗位员工及外部人员提出分层分级的信息安全管理要求。针对员工，在其与公司签署的聘用协议中包含保密条款，并明确员工的信息安全责任。针对外部人员，华为云接口部门在与之签署的合同或协议条款中明确约定对外部人员及所属公司的信息安全管理要求，以及信息安全违规处罚措施。 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。供应商安全和隐私要求包含在已签署的合同协议中。与第三方的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。华为云法务团队也会定期对合同的条款进行审查。	客户负责建立第三方利益相关方的安全角色和要求，并就相关内容与第三方达成一致，形成正式文件，在与选定的服务供应商签订的相关协议中明确整个服务供应链各方需履行的信息安全相关义务。
	PR.AT-4：高级管理人员理解其角色和职责	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	同PR.AT-2	客户负责在高级管理人员使用特权用户之前对其进行基于角色和职责的培训，并为其制定相应的培训计划。
	PR.AT-5：物理和网络安全人员理解其角色和职责	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	同PR.AT-2	客户负责在物理和网络安全人员使用特权用户之前对其进行基于角色和职责的培训，并为其制定相应的培训计划。

数据安全（PR.DS）：信息和记录（数据）按照组织的风险策略进行管理，以保护信息机密性、可用性和完整性	PR.DS-1：保护静态数据	ISO/IEC 27001:2013 A.8.2.3	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。 华为云对在公共网络上提供的应用服务采用多种安全措施保护其中涉及的数据。包括使用IAM进行访问控制，对用户进行身份认证和鉴权。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。对应用服务中的操作留存日志以支持审计。对接口进行身份认证及鉴权、传输保护和边界防护，确保API应用安全。	客户负责采用密码技术保证重要数据在存储（如服务器、PC终端、或是系统重要组件等）中的完整性和机密性。
	PR.DS-2：保护传输中的数据	ISO/IEC 27001:2013 A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3	同PR.DS-1 华为云已制定相关安全管理规定，定义了信息传输策略和流程，并详细定义了控制要求。 华为云对包含在电子消息中发送的信息进行保护，保护措施包括使用办公计算机安全软件、网络接入管控、权限管理、访问控制、传输加密和内容加密等。	客户负责采用技术措施对传输过程中的数据进行保护，包括：采用密码技术或校验技术保证通信过程中数据的完整性，采用密码技术保证通信过程中重要数据或整个报文的保密性等。

	PR.DS-3：资产在整个删除、转移和处置过程中得到正式管理	ISO/IEC 27001:2013 A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.5 A.11.2.7	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。 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。	不涉及。
	PR.DS-4：维护足够的容量以确保可用性	ISO/IEC 27001:2013 A.12.1.3 A.17.2.1	华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，排除单点故障的风险，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，应用在数据中心实现N+1部署，在一个数据中心故障的情况下可以将流量负载均衡到其他中心。 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资源进行容量规划，避免资源被过度使用，满足容量需求。同时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。	客户负责监控和规划其应用程序和租户环境的容量需求。

	PR.DS-5：实施数据泄露保护	ISO/IEC 27001:2013 A.6.1.2 A.7.1.1 A.7.1.2 A.7.3.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5 A.10.1.1 A.11.1.4 A.11.1.5 A.11.2.1 A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3	同PR.DS-1 在人员管理方面，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。同时为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。 员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的信息安全责任。对于合同方，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全责任。 华为云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。对于外部人员，华为云接口部门根据业务需要与其所属组织签署保密协议。 在账号及权限管理方面，华为云员工账号管理遵从公司用户账号权限管理规定。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。对账号进行分类管理并建立访问控制策略，相关文件均通过评审流程并发布。 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、	客户负责采取技术手段对数据的泄漏进行保护，例如制定数据访问控制策略、对重要数据进行加密。

			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，员工每次登陆均需要使用多重身份验证确定身份。 在物理访问控制方面，华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段。华为云运维人员登入运维管理区时必须先通过虚拟专用网络（VPN – Virtual Private Network）接入，再通过堡垒机访问被管理节点。管理员可从此区域访问所有区域的运维接口，此区域不向其他区域开放接口。 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。 在存储介质管理方面，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。	

	PR.DS-6：使用完整性检查机制以确认软件、固件和信息的完整性	ISO/IEC 27001:2013 A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3 A.14.2.4	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、软件安装、软件退出等环节，均实施严格的管控。 华为云对在公共网络上提供的应用服务采用多种安全措施保护其中涉及的数据。包括使用IAM进行访问控制，对用户进行身份认证和鉴权。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。对应用服务中的操作留存日志以支持审计。对	客户负责使用完整性验证工具来监控和检测对软件、固件和信息的未授权更改。

			接口进行身份认证及鉴权、传输保护和边界防护，确保API应用安全。 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。	
	PR.DS-7：开发和测试环境与生产环境隔离	ISO/IEC 27001:2013 A.12.1.4	华为云对于生产及非生产环境使用物理和逻辑控制并用的隔离手段，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。 华为云所有云服务发布前都经过了多轮安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。详细内容可参考《华为云安全白皮书》。同时，华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如SecureCAT可以对业界主流的OS和DB的安全配置进行检查。华为云对测试数据的选择和保护制定了规范，并在测试工作中严格遵循。	客户负责将生产及非生产环境进行物理或逻辑隔离，并确保测试数据和测试结果受到控制。

	PR.DS-8：使用完整性检查机制以确认硬件的完整性	ISO/IEC 27001:2013 A.11.2.4	对于数据中心的维护，华为云建立了数据中心运维管理相关的制度与流程，其中包含设备的具体管控措施、例行的维护计划等。 华为云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。	客户负责管理云上运行的应用程序的生命周期，并调配和监控其控制下的硬件的运行状况。
信息保护流程和步骤（PR.IP）：维护安全策略（用于解决组织间目的、范围、角色、责任、管理承诺和协作）、流程、规程，并用于管理对信息系统和资产的保护	PR.IP-1：创建和维护信息技术/工业控制系统的基线配置，并包含安全原则（例如：最小功能概念）	ISO/IEC 27001:2013 A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4	华为云制定并实施桌面终端服务软件标准，办公计算机使用其中定义的标准操作系统和软件。 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。 华为云建立了系统的变更管理、服务上线流程，并将其要求传达给所有相关的开发人员（包含内部员工及外部合作伙伴），新上线或变更的服务应遵循华为云发布、变更管理流程的规定。 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。	客户负责制定配置管理计划，在整个生命周期中，建立并记录重要信息系统、产品、组件的配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等，与操作规程共同维护，并对其的机密性进行保护。

	PR.IP-2：实施管理系统的系统开发生命周期	ISO/IEC 27001:2013 A.6.1.5 A.14.1.1 A.14.2.1 A.14.2.5	华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。 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。 通过结合华为在安全上的长期积累和华为云的现状，华为云不仅积极推行快速迭代的全新DevOps流程，还将华为的安全生命周期SDL无缝嵌入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。	客户负责建设系统开发生命周期管理机制，并与网络安全风险管理相结合，实现安全技术措施同步规划、同步建设、同步使用。
	PR.IP-3：已制定配置变更管理流程	ISO/IEC 27001:2013 A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4	华为云建立了系统的变更管理、服务上线流程，并将其要求传达给所有相关的开发人员（包含内部员工及外部合作伙伴），新上线或变更的服务遵循华为云发布、变更管理流程的规定。 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。	客户负责将配置信息改变纳入系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 客户负责建立变更管理程序，依据程序控制系统所有的变更，记录变更实施过程；监控、评估变更的完整性，记录变更的变化，分析潜在影响，跟踪缺陷整改效果，并报告给相关人员。

	PR.IP-4：创建、维护并测试信息备份	ISO/IEC 27001:2013 A.12.3.1 A.17.1.2 A.17.1.3 A.18.1.3	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。 华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。	客户负责对重要系统和数据库进行容灾备份，备份须满足组织的RTO和RPO目标。对备份数据进行管理维护，根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

	PR.IP-5：符合有关组织资产的物理运营环境的政策和法规	ISO/IEC 27001:2013 A.11.1.4 A.11.2.1 A.11.2.2 A.11.2.3	在物理保护方面，华为云设立了分区防护。对于可能的自然灾害制定了选址策略以消减风险。对于入侵、授权等风险，建立了监控机制及响应机制。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。 华为云对电气、消防安全执行严格管控。华为云数据中心采用多级保护方案保障业务7*24小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源(UPS)，提供短期备用电力供应。华为云数据中心建筑防火等级均按一级设计施工，使用了A级防火材料，满足国家消防规范。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统得以控制火情。 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	不涉及。

			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。	
	PR.IP-6：根据政策销毁数据	ISO/IEC 27001:2013 A.8.2.3 A.8.3.1 A.8.3.2 A.11.2.7	同PR.DS-1 华为云制定并实施介质管理规定，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。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。	不涉及。
	PR.IP-7：改进保护流程	ISO/IEC 27001:2013 A.16.1.6 条款9 条款10	华为云根据ISO 27001的要求建立并实施信息安全管理体系，并在日常运营中遵循PDCA循环模型对其进行维护和持续改进，在体系建立初期确定内外部环境并识别相关方需求，以确定信息安全管理体系的范围。在组织方面，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。	客户负责对组织采取的安全保护措施制定相应的控制流程，包括：定期对安全目标、安全管理制度、安全计划的合理性和适用性进行论证和评审，对存在不足或需要改进的进行修订；定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

	PR.IP-8：共享保护技术的有效性	ISO/IEC 27001:2013 A.16.1.6	华为云致力于构建开放、协作、共赢的安全生态体系，与业界领先的安全产品与服务供应商一起，基于责任共担模式，为云租户提供易部署、易管理、完善的安全解决方案，应对已知、未知的安全威胁，保障租户的数据和业务安全。 面对未来智能社会的安全威胁，华为云将积极联合全球安全伙伴打造一个开放、协作、共赢的安全生态圈。在持续提供云安全增值服务，提升用户信任的同时，不遗余力地推动行业和社会进步。	客户负责在其认可的安全的环境下，将其权限范围内的信息与适当相关方进行共享。 客户可积极参与网络安全国家标准、行业标准的制定，和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

	PR.IP-9：制定并管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）	ISO/IEC 27001:2013 A.16.1.1 A.17.1.1 A.17.1.2 A.17.1.3	华为云已通过ISO 22301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。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。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。 华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程。并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。	客户负责制定事件响应和业务连续性计划，以及事件和灾难恢复计划。

	PR.IP-10：测试响应和恢复计划	ISO/IEC 27001:2013 A.17.1.3	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。 华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。	客户负责定期对系统相关的人员进行应急预案培训，并进行应急预案的演练，应根据可能面临的不同风险制定演练场景，充分评估对不同事件的响应能力。

	PR.IP-11：人力资源实践中（如：取消服务、人员筛选）包含网络安全	ISO/IEC 27001:2013 A.7.1.1 A.7.1.2 A.7.2.1 A.7.2.2 A.7.2.3 A.7.3.1 A.8.1.4	人员任用前，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。同时为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。 员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的信息安全责任。对于合同方，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全责任。 人员任用中，华为云已制定针对公司各类人员的信息安全管理要求，对华为员工、机要岗位员工及外部人员提出分层分级的信息安全管理要求。在员工与公司签署的聘用协议中包含了保密条款，并明确员工的信息安全责任。 针对外部人员，华为云接口部门在与之签署的合同或协议条款中明确约定对外部人员及所属公司的信息安全管理要求，以及信息安全违规处罚措施。 在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。 华为建立了严密的安全责任体系，贯彻违规问责机制。华为云以行为和结果为主要依据对员工进行问责。根据华为云员工安全违规的性质，以及造成的后果确定问责处理等级，分级处理。对触犯法律法	客户负责在人力资源管理中充分考虑网络安全，包括指定或授权专门的部门或人员负责人力资源管理，建立正式的人员安全策略， 明确定义目标、范围、角色、职责、管理承诺、组织关系。

			规的，移送司法机关处理。直接管理者和间接管理者存在管理不力或知情不作为的，须承担管理责任。违规事件处理根据违规个人态度与调查配合情况予以加重或减轻处理。华为云的违规政策供所有员工进行查看学习，并定期组织培训提升员工对违规行为、违规后果、惩罚措施的了解。 人员离职时，华为云规定员工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。对于外部人员，华为云接口部门根据业务需要与其所属组织签署保密协议。 华为云制定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。	

	PR.IP-12：制定并实施漏洞管理计划	ISO/IEC 27001:2013 A.12.6.1 A.14.2.3 A.16.1.3 A.18.2.2 A.18.2.3	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。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。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。 华为云在其官网公布已经发现的产品或服务的漏洞并进行预警，客户可查看安全公告以了解漏洞影响的范围，处置方式及威胁级别。	客户负责定期以及在系统上线、变更等重要时间节点采取必要的措施对安全漏洞和隐患进行识别，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补，并报告相关部门。应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。定期对风险评估和漏洞扫描的人员、流程、工具的有效性进行审查，并及时更新。
维护（PR.MA）：按照政策和流程维护和维修工业控制和信息系统组件	PR.MA-1：使用已批准和受控的工具维护和维修组织资产并记录	ISO/IEC 27001:2013 A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6	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。	客户负责维护其自己的基础架构，包括连接到华为云环境的基础架构。
	PR.MA-2：以防止未授权访问的方式，批准、记录和执行组织资产的远程维护	ISO/IEC 27001:2013 A.11.2.4 A.15.1.1 A.15.2.1	同PR.AC-3	客户负责确保非本地维护和诊断活动得到批准和记录，以防止未授权的访问。

保护技术（PR.PT）：按照相关政策、流程和协议管理技术安全解决方案，以确保系统和资产的安全性和韧性	PR.PT-1：根据政策来确定、记录、实施和审查审计/日志记录	ISO/IEC 27001:2013 A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1	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。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。	客户负责制定正式的审计策略并形成文件， 明确日志审计的目的、范围、角色、责任和追究制度。
	PR.PT-2：保护可移动媒体，并根据政策限制其使用	ISO/IEC 27001:2013 A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.8.3.3 A.11.2.9	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。	不涉及。
	PR.PT-3：通过配置系统融入最小功能原则，以提供基本功能	ISO/IEC 27001:2013 A.9.1.2	在人员权限管理方面，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。 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。	客户负责遵循最小功能原则，限制对重要信息系统、产品、组件的未授权访问，并对所有的非授权访问尝试进行记录，所有计算设备应遵循最小安装的原则，基于白名单技术，仅安装需要的组件和应用程序。

	PR.PT-4：保护通信和控制网络	ISO/IEC 27001:2013 A.13.1.1 A.13.2.1 A.14.1.3	华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分区自我保护和容错恢复能力。华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据 存储区（OBS – Object - Based Storage）、运维管理 区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在 互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。华为云高效的多维全栈防护体系也包括多种边界防护措施，华为云已将各项高级防护功能按需适配到华为云外网边界和内网的区域间的信任边界。 详细介绍可参考《华为云安全白皮书》。	客户负责制定网络和通信机制，保护应用程序内以及应用程序与外部系统之间的信息流。 客户负责建立和记录使用限制、配置和连接要求以及访问应用程序的实施指导。

	PR.PT-5：执行机制（例如故障安全、负载平衡、热插拔）以实现正常和不利情况下的韧性需求	ISO/IEC 27001:2013 A.17.1.2 A.17.2.1	华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，排除单点故障的风险，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，应用在数据中心实现N+1部署，在一个数据中心故障的情况下可以将流量负载均衡到其他中心。 华为云已经通过ISO 22301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。	不涉及。

5.3 检测（Detect）

类别	子类别	参考信息	华为云的回应	客户的责任
异常和事件（DE.AE）：检测到异常活动并理解事件的潜在影响	DE.AE-1：建立并管理用户和系统的网络操作和预期数据流的基线	ISO/IEC 27001:2013 A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2	华为云参考互联网安全中心（CIS – Center of Internet Security）安全基线并将其融入华为云服务 DevSecOps 流程，所有产品在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，产品的配置变更均须遵从变更管理流程。	针对信息系统内部各组件间、信息系统之间的信息流: 客户负责根据制定的信息流控制策略，保证信息流得到授权和批准。根据信息系统进行数据交互的安全协议，控制信息流，并定期更新数据交互协议。在网络和系统的配置管理方面， 客户应建立管理制度，对网络和系统的配置管理作出规定，制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置。

	DE.AE-2：分析检测到的事件以理解攻击目标和方法	ISO/IEC 27001:2013 A.12.4.1 A.16.1.1 A.16.1.4	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。该日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间超过180天，90天内可以实时查询。华为云有专门的内审部门，定期对运维流程各项活动进行审计。 华为云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。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。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。 华为云已建立安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件。	客户负责根据已制定的监控策略，开启信息系统（网络、主机、数据库、应用等）的审计记录，并定期查看和分析审计记录，以发现攻击行为。客户应采取技术措施对网络行为进行分析，当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间等。
	DE.AE-3：从多方来源和传感器收集事件数据并进行关联	ISO/IEC 27001:2013 A.12.4.1 A.16.1.7	同DE.AE-2 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。	客户负责关联和分析从多个来源收集的安全相关信息。采用自动化机制，以协助跟踪安全事件以及收集和分析事件信息。

	DE.AE-4：确定事件的影响	ISO/IEC 27001:2013 A.16.1.4	安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件。确定是安全事件后会根据已制定安全事件的定级原则和升级原则，考虑安全事件对客户业务的影响程度进行事件定级。 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。	当信息系统及系统所处理、存储或传输的信息遭遇未经授权的访问、使用、披露、中断、修改或破坏时，客户负责分析这些事件所带来的风险及影响。
	DE.AE-5：建立事件警报阈值	ISO/IEC 27001:2013 A.16.1.4	同DE.AE-2	客户负责预先对安全事件进行分类分级，并定义哪些安全事件需被报告。
安全连续监控（DE.CM）：监控信息系统和资产，以识别网络安全事件和验证保护措施的有效性	DE.CM-1：监控网络，以检测潜在的网络安全事件	N/A	同DE.AE-2	客户负责制定网络监控策略，包括确定监控指标、监控频率，并根据监控策略对网络的安全状况进行持续监控。
	DE.CM-2：监控物理环境，以检测潜在的网络安全事件	ISO/IEC 27001:2013 A.11.1.1 A.11.1.2	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。	不涉及。

	DE.CM-3：监控人员活动，以检测潜在的网络安全事件	ISO/IEC 27001:2013 A.12.4.1 A.12.4.3	同DE.AE-2	客户负责监控员工对环境的访问，以了解潜在的安全事件。
	DE.CM-4：检测恶意代码	ISO/IEC 27001:2013 A.12.2.1	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。	客户负责制定恶意代码防范规范，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。并提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码检查等。
	DE.CM-5：检测未经授权的移动代码	ISO/IEC 27001:2013 A.12.5.1 A.12.6.2	同DE.CM-4	客户负责定义可接受和不可接受的移动代码和移动代码技术，为可接受的移动代码和移动代码技术建立使用限制和实施指南。

	DE.CM-6：监控外部供应商行为，以检测潜在的网络安全事件	ISO/IEC 27001:2013 A.14.2.7 A.15.2.1	华为云对研发外包管理提出明确要求，并将外包人员及外包项目的监督纳入员工及项目日常职责中。 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。	客户负责制定供应商监控策略，包括确定监控指标、监控频率，根据监控策略开展持续监控。 根据组织对供应商提出的信息安全要求，监控其对组织安全流程和程序的遵守程度。若组织使用外部信息系统，同样应对外部信息系统的服务供应商提出信息安全要求，并加以监控。 客户负责定期监视、评审和审核服务供应商提供的服务。
	DE.CM-7：对未经授权的人员、连接、设备和软件进行监控	ISO/IEC 27001:2013 A.12.4.1 A.14.2.7 A.15.2.1	同DE.AE-2 同DE.CM-6	客户负责监控其系统中是否有未经授权的人员、连接、设备和软件。
	DE.CM-8：实施脆弱性扫描	ISO/IEC 27001:2013 A.12.6.1	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。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。	客户负责制定漏洞扫描流程，规定扫描对象、扫描频率等信息。根据制定的漏洞扫描流程，使用漏洞扫描工具和技术对系统进行漏洞扫描。漏洞扫描需包括识别平台和软件漏洞以及错误配置，评估所发现漏洞的影响，将漏洞扫描结果形成漏洞扫描报告，对发现的漏洞进行风险评估，并在规定的时间内修补漏洞等活动。

检测流程（DE.DP）：维护和测试检测流程和程序，以确保意识到异常事件	DE.DP-1：合理定义检测的角色和职责，以确保问责制	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2	华为云在各产品、服务的业务团队中明确规定了所有员工及第三方利益相关者对应角色的信息安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的信息安全管理职责。信息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。	客户负责制定检测流程，并明确定义检测的角色和责任，以确保问责制。
	DE.DP-2：检测活动符合所有适用要求	ISO/IEC 27001:2013 A.18.1.4 A.18.2.2 A.18.2.3	华为云以全球隐私保护的法律法规为基石，参考业界广泛认可的优秀实践，建设了华为云的隐私保护体系，对隐私和个人可识别信息进行保护。 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。 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。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。 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。	客户负责确保其制定的检测流程符合组织的内部要求和外部要求。

	DE.DP-3：测试检测流程	ISO/IEC 27001:2013 A.14.2.8	华为云所有云服务发布前都经过了多轮安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。详细内容可参考《华为云安全白皮书》。同时，华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如SecureCat可以对业界主流的OS和DB的安全配置进行检查。	客户负责开展安全评估，以验证安全检测措施的有效性。组织可定期开展渗透测试，在事先未通知的情况下，绕过或避开物理设施出入口安全控制企图侵入设施内部，以验证安全监控是否有效。组织可定期验证防范恶意代码攻击的技术措施的有效性。
	DE.DP-4：沟通事件检测信息	ISO/IEC 27001:2013 A.16.1.2 A.16.1.3	华为云已建立安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件，并根据事件响应流程对事件进行定级并处理。 华为云已制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。 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,要求包括员工应报告发现的信息安全弱点。对于其他外部相关人员，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全事件报告责任。华为云向员工提供了报告信息安全事件的渠道及注意事项。	客户负责向内部和外部的相关方传达事件检测的结果。

	DE.DP-5：不断改进检测流程	ISO/IEC 27001:2013 A.16.1.6	同DE.AE-4	客户负责持续维护和评审安全测试、培训和监控计划，确保计划符合组织的风险管理策略及风险应对活动的优先排序。

5.4 响应（Respond）

类别	子类别	参考信息	华为云的回应	客户的责任
响应计划（RS.RP）：执行和维护响应流程和程序，以确保对检测到的网络安全事件进行响应	RS.RP-1：在事件发生期间或之后执行响应计划	ISO/IEC 27001:2013 A.16.1.5	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程。并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。 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。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。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。 华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。	客户负责制定应急预案，规定在信息系统发生中断、入侵或故障事件的响应策略和流程，并在发生信息系统中断、入侵或故障事件时，启动应急预案，进行事件响应。 客户负责制定安全事件响应计划，明确不同安全事件的报告和响应流程，在安全事件发生时，根据已制定的流程对安全事件进行响应。

沟通（RS.CO）：响应活动应与内部和外部利益相关方协调一致（例如：执法机构的外部支持）	RS.CO-1：当需要响应时，人员知道他们的角色和操作顺序	ISO/IEC 27001:2013 A.6.1.1 A.7.2.2 A.16.1.1	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信息安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的信息安全 管理职责。在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。 华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。	客户负责对相关人员进行培训，保证他们了解对应的职责和在事件响应中的正确操作。
	RS.CO-2：报告的事件符合既定标准	ISO/IEC 27001:2013 A.6.1.3 A.16.1.2	华为云已制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。 同时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，根据要求在必要时向监管机构报告事件。	客户负责根据既定的标准向内部和外部利益相关者报告事件。此外，客户应酌情支持相关执法机构的调查。

	RS.CO-3：信息共享符合响应计划	ISO/IEC 27001:2013 A.16.1.2 条款7.4	同RS.CO-2 华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程。并持续优化该机制。安全事件响应流程中根据不同类型及级别的安全事件定义了通报机制，包括通报方式、通报时间点、通报对象、通报内容模板等。	客户负责制定安全事件报告机制，定义需被报告的安全事件类型，明确不同安全事件的报告流程，并规定安全事件报告的管理职责，对造成系统中断和造成信息泄露的重大安全事件应采用不同的报告程序。
	RS.CO-4：与利益相关方的协同符合响应计划	ISO/IEC 27001:2013 条款7.4	同RS.CO-3	客户负责在制定应急预案和安全事件响应计划时，应识别应急响应和安全事件响应活动所依赖的内外部相关方，并规定与各相关方的协作方式和协作流程。
	RS.CO-5：与外部利益相关者共享漏洞信息，以实现更广泛的网络安全态势感知	ISO/IEC 27001:2013 A.6.1.4	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，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。	客户应加强与网络安全管理部门、各类供应商、业界专家与安全组织的合作与沟通，以不断加强对组织人员的安全教育和培训，保持对优秀安全实践和技术的了解，分享关于新的威胁、脆弱性和事件等相关安全信息。并建立网络安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络安全的投诉和举报。

分析（RS.AN）：执行分析，以确保有效响应和支持恢复活动	RS.AN-1：调查来自检测系统的通知	ISO/IEC 27001:2013 A.12.4.1 A.12.4.3 A.16.1.5	同RS.RP-1 华为云已建立安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件。	客户负责对日志、检测和报警数据进行分析、统计，发现可能的安全事件并获取事件信息，以便快速对事件进行响应。
	RS.AN-2：理解事件的影响	ISO/IEC 27001:2013 A.16.1.4 A.16.1.6	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。	在发生突发事件时，客户负责根据组织已制定的安全事件分类分级标准，在发生安全事件时，判断事件的影响及级别。
	RS.AN-3：进行取证	ISO/IEC 27001:2013 A.16.1.7	华为云制定了安全事件应急处置流程及响应流程，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。	客户负责在安全事件报告和响应处理过程中收集证据，记录处理过程。信息系统应提供审计报告生成能力，以支持对安全事件的事后调查，且保证审计记录的内容及时间戳不可篡改。
	RS.AN-4：事件分类符合响应计划	ISO/IEC 27001:2013 A.16.1.4	华为云已建立安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件，并根据事件响应流程对事件进行定级并处理。	客户负责制定信息安全事件分类分级的标准，并针对不同级别的事件规定相应的响应流程。在发生信息安全事件时，应根据预先定义的标准判断事件的类别和级别，以便启动相应的应对措施。

	RS.AN-5：建立流程，以接收、分析和响应源自内部和外部向组织披露的漏洞（例如：内部测试、安全公告或安全研究员）	N/A	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。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。 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。	客户负责不断从组织指定的外部组织处接收信息安全警报，生成合适的内部安全警报，并向组织指定的外部组织、内部人员或角色发布。客户应与业界相关安全组织和协会建立和保持联系，以分享最新安全威胁、漏洞和事件以及其它安全信息。

缓解（RS.MI）：执行活动，以防止事件扩展，减轻其影响并解决事件	RS.MI-1：遏制事件	ISO/IEC 27001:2013 A.12.2.1 A.16.1.5	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。 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。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。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。 华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程。并持续优化该机制。安全事件响应流程中清晰定义了在事件	信息安全事件发生时，客户应根据制定的事件处置机制和流程，采取紧急措施遏制事件的恶化。 在发现组织提供的应用软件设有恶意程序时，组织应当停止提供服务，采取消除等处置措施。

			响应过程中负责各个活动的角色和职责。 华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。	
	RS.MI-2：缓解事件	ISO/IEC 27001:2013 A.12.2.1 A.16.1.5	同RS.MI-1	信息安全事件发生时，客户应根据制定的事件处置机制和流程处置安全事件，最大可能地降低事件的影响。
	RS.MI-3：缓解新识别的漏洞，或记录为可接受的风险	ISO/IEC 27001:2013 A.12.6.1	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。 华为云在其官网公布已经发现的产品或服务的漏洞并进行预警，客户可查看安全公告以了解漏洞影响的范围，处置方式及威胁级别。	客户负责及时修补发现的安全漏洞和隐患，包括对安全控制措施评估和监控过程中发现的安全问题采取处置措施，对风险评估中已识别的风险，应进行记录并采取风险处置措施，对系统漏洞扫描中发现的漏洞进行风险评估，并在规定的时间内修补漏洞。
改进（RS.IM）：通过整合当前和以前的检测/响应活动的经验教训，改进组织的响应活动	RS.IM-1：响应计划吸取了经验教训	ISO/IEC 27001:2013 A.16.1.6 条款10	同RS.AN-2	客户负责在应急预案框架中包括经验总结的内容，以对应急预案中响应程序实施或测试期间遇到的问题进行总结，并将总结的经验教训纳入应急预案的响应程序中。

	RS.IM-2：更新响应策略	ISO/IEC 27001:2013 A.16.1.6 条款10	华为云至少每年审查一次信息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。	客户负责更新应急预案响应程序，以适应组织、信息系统或操作环境的变化或解决应急预案响应程序实施或测试期间遇到的问题.

5.5 恢复（Recover）

类别	子类别	参考信息	华为云的回应	客户的责任
恢复计划（RC.RP）：执行和维护恢复流程和程序，以确保恢复受网络安全事件影响的系统或资产	RC.RP-1：在网络安全事件发生期间或之后执行恢复计划	ISO/IEC 27001:2013 A.16.1.5	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云有专业的安全事件管理统，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。	客户负责制定应急预案和安全事件响应流程，应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
改进（RC.IM）：通过将经验教训纳入未来活动，改进恢复计划和流程	RC.IM-1：恢复计划吸取了经验教训	ISO/IEC 27001:2013 A.16.1.6 条款10	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。	客户负责在应急预案框架中包括经验总结的内容，以对应急预案中响应程序实施或测试期间遇到的问题进行总结，并将总结的经验教训纳入应急预案的响应程序中。

	RC.IM-2：更新恢复策略	ISO/IEC 27001:2013 A.16.1.6 条款10	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。 华为云至少每年审查一次信息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。	客户负责更新应急预案中恢复流程的更新，以适应组织、信息系统或操作环境的变化或解决应急预案中恢复流程实施或测试期间遇到的问题。
沟通（RC.CO）：恢复活动与内部和外部各方协调一致（例如：协调中心、互联网服务提供商、攻击系统的所有者、受害者、其他CSIRT和供应商）	RC.CO-1：管理公共关系	ISO/IEC 27001:2013 A.6.1.4 条款7.4	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。 华为云已制定并执行主动通知客户流程，将影响客户业务的服务通知及时发送给客户，以便客户及时调整业务策略、降低业务影响、提升客户服务感知。	客户负责建立危机处理机制，加强与客户、媒体、社会公众的沟通，并制定针对社会公众、媒体等相关各方的预案，在发生突发事件时及时、准确披露信息。
	RC.CO-2：事件发生后修复声誉	ISO/IEC 27001:2013 条款7.4	在1、2级事件发生后，安全事件接口人将与舆情接口人同步，由其启动危机公关处理。	客户负责事先制定与重要利益相关方的沟通策略、方式、原则和计划，在事件发生时，根据沟通策略和计划，对不同的对象进行沟通，以降低或消除事件对组织品牌声誉负面影响的目标。

	RC.CO-3：与内部和外部利益相关者以及执行和管理团队沟通恢复活动	ISO/IEC 27001:2013 条款7.4	同RC.CO-1	客户负责建立危机处理机制，加强与客户、媒体、社会公众的沟通，并制定针对社会公众、媒体等相关各方的预案，在发生突发事件时及时、准确披露信息。

6 华为云如何协助客户构建基于 NIST CSF 框架的网络安全体系

华为云已通过NIST CSF网络安全框架的最高等级认证，能够在全球范围内提供安全可信的云服务。华为云提供的产品和服务可以针对NIST CSF框架核心中五项功能中的部分类别提供帮助，协助解决客户管理网络安全风险时遇到的问题,如需了解产品详情，请前往华为云官网中的**产品页面**。

功能	华为云提供的产品	功能介绍
识别（Identify）	数据安全中心服务（DSC）	数据安全中心服务（DSC - Data Security Center）是新一代的云原生数据安全平台，可以为客户提供数据分级分类、数据安全风险识别、数据水印溯源、数据脱敏等基础数据安全能力，并通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。
	安全治理云图（Compass）	安全治理云图（Compliance Compass）是一个自动化合规评估和安全治理的平台，以华为内部“云服务网络安全与合规标准”（Cloud Service Cybersecurity & Compliance Standard，3CS）为基座，将华为积累的全球安全合规经验服务化，开放PCI DSS、ISO27701、ISO27001等安全治理模板，将合规语言IT化实现自动化扫描，可视化呈现合规状态，一键生成合规遵从性报告，帮助租户快速实现云上业务的安全遵从，提升租户获得法规及行业标准认证的效率。
	企业主机安全服务（HSS）	通过采用企业主机安全服务（HSS - Host Security Service）全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，构建服务器安全体系，以降低当前服务器面临的主要安全风险。客户可通过HSS服务的提供可视化界面统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

	漏洞扫描服务（VSS）	客户可通过华为云提供漏洞扫描服务（VSS - Vulnerability Scan Service）。实现对Web应用、操作系统、配置基线的扫描，以及对资产内容合规检测和弱密码检测，以识别网站或服务器暴露在网络中的安全风险。华为云会第一时间针对紧急爆发的通用漏洞CVE进行分析并更新规则，提供快速、专业的CVE漏洞扫描。
保护（Protect）	统一身份认证服务（IAM）	华为云提供的统一身份认证服务（IAM – Identity and Access Management）。提供适合企业级组织结构的用户账号管理服务，为用户分配不同的资源及操作权限。用户通过使用访问密钥获得基于统一身份认证服务的认证和鉴权后，以调用API的方式访问华为云资源。统一身份认证服务可以按层次和细粒度授权，保证同一企业客户的不同用户在使用云资源上得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保客户业务的持续性。
	云堡垒机（CBH）	云堡垒机（CBH - Cloud Bastion Host）是华为云的一款4A统一安全管控平台，可帮助客户实现集中的帐号、授权、认证和审计管理。云堡垒机提供云计算安全管控的系统和组件，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。客户可以通过统一运维登录入口实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。客户员工登录公司系统、运维人员访问运维网络区域、员工从企业外部网络远程接入相关资源以及管理员接入管理平台等场景都可以使用云堡垒机实现访问控制及统一操作日志审计，确保网络和网络服务仅由已获授权的用户访问。
	虚拟私有云（VPC）	华为云为客户提供的虚拟私有云（VPC - Virtual Private Cloud）服务可为客户构建隔离且私密的虚拟网络环境，在流畅访问的同时隔离客户，在此基础上支持灵活配置虚拟私有云之间的互联互通。客户可以完全掌控自己的虚拟网络构建与配置，包括虚拟私有云内的IP地址段、子网、安全组等子服务，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，满足客户更细粒度的网络隔离需求。客户可将虚拟私有云用于划分网络区域、在云上建立隔离的生产与测试环境等。
	应用信任中心（ATC）	华为云的应用信任中心（ATC）可实现依据用户身份、访问行为、应用健康度进行细粒度的动态授权控制。

	虚拟专用网络（VPN）	对于需要将已有数据中心扩展到华为云上的场景，客户可以使用虚拟专用网络（VPN - Virtual Private Network）。该服务可用于在传统数据中心与华为云提供的虚拟私有云之间建立安全加密通信隧道，便于客户使用云平台中的云服务器、块存储等资源，将应用程序转移到云中、启动额外的Web服务器、增加网络的计算容量等，实现企业的混合云架构。
	密钥管理服务（KMS）	客户可以使用密钥管理服务（KMS）为可识别的所有者绑定密钥。密钥管理服务中所有密钥均由云硬件安全模块的硬件真随机数生成器生成，保证密钥的随机性。密钥管理服务的根密钥保存在云硬件安全模块中，确保根密钥不泄露。密钥管理服务主机均使用标准的加密传输模式与密钥管理服务服务节点建立安全通信链接，保证密钥管理服务相关数据在节点间的传输安全。密钥管理服务基于统一身份认证服务（IAM – Identity and Access Management）中角色统一进行RBAC访问控制。对于用户，只有通过身份验证及密钥管理服务鉴权并拥有密钥操作权限，才能操作密钥管理服务中存储的主密钥。仅设置了只读权限的用户只能查询主密钥信息，不能对主密钥进行操作。密钥管理服务对主密钥进行了客户隔离，每一个租户只能访问与管理属于自己的主密钥，无法操作其他租户的主密钥。此外，系统管理员仅有设备管理权限，没有任何访问主密钥的权限。
	SSL证书服务（SCM）	华为云的SSL证书管理(SCM - SSL Certificate Manager)服务可以向客户提供一站式证书的全生命周期管理，实现网站的可信身份认证与安全数据传输。平台联合全球知名数字证书服务机构为用户提供购买SSL证书的功能，用户也可以将本地的外部SSL证书上传到平台，实现用户对内部和外部SSL证书的统一管理。客户在部署该服务后，可以将服务使用的HTTP协议替换成HTTPS协议以消除HTTP协议的安全隐患。该服务可应用于网站可信认证、应用可信认证以及应用数据传输保护
	Anti-DDoS流量清洗（Anti-DDoS）	客户可通过Anti-DDoS流量清洗服务实现对网络层和应用层的DDoS攻击防护，Anti-DDoS为客户提供精细化的防护服务，客户可以根据业务的应用类型，配置流量阈值参数，并通过实时告警功能查看攻击和防御状态。客户如需更大流量攻击的检测和清洗服务，可通过华为云的DDoS高防（AAD - Advanced Anti-DDoS）服务来实现。

	对象存储服务（OBS）	对象存储服务（OBS – Object Storage Service）可存储客户信息资产中的非结构化数据，对象存储服务支持存储对象的生命周期管理，可以协助客户管理其信息资产。此外，对象存储服务中的多重安全防护如SSL传输加密、服务端加密、身份鉴权均可提供对所存储信息的安全保护。
	API网关（APIG）	API网关（API Gateway）是为企业开发者及合作伙伴提供的高性能、高可用、高安全的API托管服务，能快速将企业服务能力包装成标准API服务，帮助您轻松构建、管理和部署任意规模的API，并上架API市场进行售卖。借助API网关，可以简单、快速、低成本、低风险地实现内部系统集成、业务能力开放及业务能力变现。
	软件开发平台（DevCloud）	为客户提供端到端的研发工具服务，实现 全生命周期覆盖，实现开发测试环 境、类生产环境、生产环境的一致 性。全方位系统安全加固，核心研 发数据加密传输和存储，基于角色 的企业级安全管控，全面保障企业研发数据的安全。
	云审计服务（CTS）	华为云的云审计服务 (CTS - Cloud Trace Service)可以实时、系统地记录用户通过云账户登录管理控制台执行的操作。客户可根据企业对日志保留期限的要求购买不同规格的对象存储服务服务以实现日志的备份。
检测（Detect）	Web应用防火墙（WAF）	客户可通过部署Web应用防火墙（WAF - Web Application Firewall）对网站业务流量进行多维度检测和防护。Web应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁，通过对HTTP(S)请求进行检测，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，全面避免网站被黑客恶意攻击和入侵，保护Web服务安全稳定。
	威胁检测服务（MTD）	威胁检测服务（MTD - Managed Threat Detection）是一种持续监控访客对客户使用的全局服务的帐号/域名的恶意活动和未经授权行为的服务。此服务集成了AI智能引擎、威胁情报、规则基线三种检测方式，智能检测来自多个云服务日志数据中的访问行为以发现是否存在潜在威胁，对可能存在威胁的访问行为生成告警信息，输出告警结果。帮助客户在威胁未形成巨大风险之前及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护客户的帐户安全，保障服务稳定运行，提升运维效率。

	态势感知（SA）	态势感知（SA - Situation Awareness）是华为云为客户提供的安全管理与态势分析平台。能够检测出包括DDoS攻击、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等多种云上安全风险。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为客户呈现出全局安全攻击态势，帮助客户识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联DDoS高防、企业主机安全服务、Web应用防火墙和数据库安全服务等，集中呈现安全防护状态。
	云日志服务（LTS）	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。
	云监控服务（CES）	客户可通过华为云提供的云监控服务（CES - Cloud Eye Service）实现对弹性云服务器（ECS - Elastic Cloud Server）的使用量以及网络带宽的立体化监控，云监控服务支持通过Open API、SDK、Agent方式上报租户自定义的指标，并通过邮件、短信等方式进行通知，以保证客户第一时间知悉业务运行情况。
响应（Respond）	管理检测与响应（MDR）	管理检测与响应（MDR - Managed Detection and Response）服务，该服务可以帮助客户建立由管理、技术与运维构成的安全风险管控体系，结合企业与机构业务的安全需求反馈和防控效果对安全防护进行持续改进，帮助企业与机构实现对安全风险与安全事件的有效监控，并及时采取有效措施持续降低安全风险并消除安全事件带来的损失。
	消息通知服务（SMN）	消息通知服务（SMN – Simple Message Notification）是一个简单、灵活、海量、托管的消息推送服务。通过该服务，用户可以高效且经济的方式将消息推送给电子邮箱、手机号码、HTTPS 应用程序以及移动推送。通过SMN，用户可以单独发送消息也可群发消息。用户还可以轻松地集成其它云服务(例如CES、OBS、AS 等)，并接受它们的事件通知。

恢复（Recover）	云服务器备份（CSBS）	客户如需创建在线备份，可以使用云服务器备份（CSBS - Cloud Server Backup Service）服务，它可以为云服务器下所有云硬盘创建一致性在线备份，当发生病毒入侵、人为误删除、软硬件故障时将数据恢复到任意备份点。云服务器备份提供对弹性云服务器和裸金属服务器的备份保护服务，支持基于多云硬盘一致性快照技术的备份服务，并支持利用备份数据恢复服务器数据，最大限度保障用户数据的安全性和正确性，确保业务安全
	云备份（CBR）	客户可以使用华为云提供的云备份（CBR – Cloud Backup and Recovery）服务实现对云硬盘（EVS - Elastic Volume Service）、弹性云服务器（ECS - Elastic Cloud Server）和裸金属服务器（BMS - Bare Metal Server）的备份保护。云备份支持基于快照技术的备份服务以及利用备份数据恢复服务器和云硬盘的数据。同时云备份支持同步线下备份软件BCManager中的备份数据以及对备份数据的完整性校验。

7 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。

8 版本历史

日期	版本	描述
2022年2月	1.0	首次发布