华为云中华人民共和国香港特别行政区 C-RAF 2.0 遵从性指南

文档版本 1.0

发布日期 2022-09-12

HUAWEI

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 背景与发布目的

随着信息科技的迅速发展，为中华人民共和国香港特别行政区（下文简称“中国香港”）金融机构带来了显著的效益，但同时网络攻击的复杂程度及潜在影响逐渐增加。为加强中国香港金融体系应对网络安全风险的能力，中国香港金融管理局（Hong Kong Monetary Authority，下文简称“金管局”或“HKMA”）推出了网络防卫计划（Cybersecurity Fortification Initiative，下文简称“CFI”），要求中国香港金融机构（认可机构，Authorized Institution，下文简称“AI”）实施网络防卫评估框架（Cyber Resilience Assessment Framework，下文简称“C-RAF”）。

华为云作为云服务提供商，致力于协助金融客户满足这些监管要求，持续为金融客户提供遵从金融行业监管要求的云服务及业务运行环境。本文旨在关注C-RAF 2.0的成熟度评估，并针对中国香港金融机构使用云服务的场景，详细阐述华为云将如何协助其满足C-RAF 2.0成熟度评估矩阵中规定的相关控制原则。

1.2 C-RAF 2.0 简介

HKMA是中国香港金融行业的主要监管机构，为进一步加强中国香港金融机构的网络安全能力，HKMA于2016年5月24日推出网络防卫计划（CFI），并于2016年12月21日发布CFI的实施细则。CFI包括以下三大支柱：

- 网络防卫评估框架（C-RAF）：是一套基于风险的框架，旨在让AI以此为依据，评估自身的网络安全风险状况，并制定和实施适当地防范网络攻击的防御措施。
- 专业发展计划（Professional Development Programme，简称PDP）：推出网络安全从业人员的认证计划及专业培训课程，为金融行业乃至信息科技界培养专业的网络安全从业人员。
- 网络情报共享平台（Cyber Intelligence Sharing Platform，简称CISP）：旨在提供分享有关网络攻击信息的有效基建。AI能够从网络情报共享平台及时收到提示或警告，以对金融行业可能出现的网络攻击进行应对。

其中，C-RAF包含三个部分：

- 固有风险评估（Inherent Risk Assessment）：AI可通过包含5个类别（技术、交付渠道、产品和技术服务、企业规模和组织特征、网络威胁的跟踪记录）的评估矩阵，评估自身的固有网络安全风险级别，并确定自身预期的成熟度级别。

- 成熟度评估（Maturity Assessment）：AI可通过包括7个领域26个组件的成熟度矩阵，评估自身当前的网络安全成熟度级别，并确定是否于预期的成熟度级别存在差距。若存在差距，AI将制定计划以提升其成熟度级别。
- 情报主导的网络攻击模拟测试（intelligence-led cyber attack simulation testing，简称“iCAST”）：对AI网络安全能力的测试，通过使用相关网络情报模拟来自对手的真实网络攻击。固有风险水平被评估为“中等”或“高”的AI应在在合理时间内进行iCAST。

到2019年末，AI基本上完成了一轮C-RAF评估，即C-RAF 1.0。鉴于C-RAF 1.0的推行以及网络安全的发展，金管局对CFI进行了全面的审查。考虑到过去几年的经验、行业咨询获得的反馈、以及海外发展和新实践，HKMA对CFI进行修订，并于2020年11月3日发布（2021年1月1日生效）的CFI 2.0和C-RAF 2.0。

C-RAF 2.0是□个结构化的评估框架，通过该框架，AI可以根据□组“控制原则”评估其固有风险和网络安全措施的成熟度。通过这个过程，AI应该能够更好地理解、评估、加强并不断提高他们的网络弹性。

为了遵循C-RAF 2.0，AI需要通过执行固有风险评估来确定其固有风险级别和预期的成熟度级别，然后执行成熟度评估来确定其网络安全的实际成熟度水平。对于预期成熟度级别和实际成熟度级别之间的任何差距，应标记为有待改进，以便AI能够进一步增强其网络安全，达到金管局预期的成熟度。对于旨在达到“中级”或“高级”成熟度水平的AI，需要进行iCAST，其中AI需要应用基于风险的方法来识别与其机构相关的攻击场景，并确保在iCAST演习中对其进行测试，以模拟有能力的对手进行的真实攻击。

根据HKMA的要求，C-RAF的评估通常每三年应进行□次。考虑到其固有风险评级、AI业务性质的变化或采用的技术等因素，AI应主动评估是否需要更频繁的评估。通过使用基于风险的方法，被评为□固有风险的AI应考虑评估审查周期不超过三年。

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。

- **服务提供商**

根据外包安排向金融机构提供服务的实体以及实体的分支机构。

- **云计算**

  根据美国国家标准技术研究院（NIST）的定义，是指一种基于互联网，能够按需提供共享计算机处理资源和数据的计算模式。

- **网络弹性**

  组织通过预测和适应网络威胁和环境中的其他相关变化，以及通过承受、遏制和快速从网络事件中恢复来继续执行其使命的能力。

2 华为云的认证情况

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，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全，主要包括：

全球性标准类认证

认证	描述
ISO20000-1:2011	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。
ISO27001:2013	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。
ISO22301:2012	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。
SOC审计	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。
PCI DSS认证	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。

认证	描述
CSA STAR金牌认证	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。
国际通用准则CCEAL3+	CC(Common Criteria)认证是一种信息技术产品和系统安全性的评估标准，它提供了一组通用的安全功能要求和安全保证要求，并在这些保证要求的基础上提供衡量IT安全性的尺度（即评估保证级EAL），使得独立的安全评估结果可以互相比较。
ISO27018:2014	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。
ISO29151:2017	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。
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。
BS10012:2017	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。
M&O认证	Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。
NIST网络安全框架(CSF)	NIST CSF由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
PCI 3DS认证	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。

地区性标准类认证

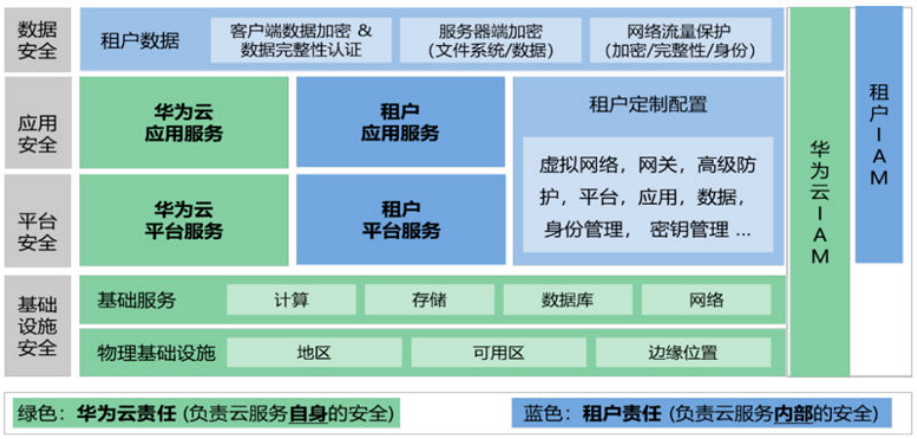
认证	描述
网络安全等级保护	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡MTCS Level3认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level3等级认证。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
云服务用户数据保护能力认证	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。
工信部云计算服务能力评估	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为获得云计算服务能力“一级”符合性证书。
可信云评估	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。
网信办网络安全审查	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。

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**”。

3 华为云安全责任共担模型

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 3-1 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》**。

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。关于更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。

5 华为云如何遵从及协助客户满 C-RAF 2.0 的要求

C-RAF 2.0的建立旨在最大限度地减少重复性和破坏性行动，并协助AI识别控制差距，制定网络弹性补救和增强行动，以降低网络安全风险。C-RAF 2.0的成熟度评估矩阵提供了AI要达到相应网络安全成熟度级别的控制目标和原则，包括治理、识别、保护、检测、响应和恢复、态势感知、第三方风险管理共7个领域。

金融机构在遵循C-RAF 2.0成熟度评估矩阵相关领域的要求时，华为云作为云服务提供商，可能会参与到要求所涉及的部分活动中。以下内容将总结C-RAF 2.0成熟度评估矩阵中与云服务提供商相关的要求，并阐述华为云作为云服务提供商，将如何帮助客户满足这些控制要求。

注：本章节的“对客户的提示”分别阐述AI客户在低（Baseline）、中（Intermediate）、高（Advanced）的成熟度级别下需要实施的控制。

5.1 识别

5.1.1 信息资产管理

控制原则编号	控制原则主题	对客户的提示	华为云的应答

2.1.1	信息资产管理	低：客户应建立准确和完整的操作环境视图，从而提供整体攻击面的可见性，促进审查网络控制的充分性和有效性。 中：除上述控制外，客户应建立流程以更新信息资产清单并防止在未经适当审查和批准的情况下发生偏差。 高：除上述控制外，客户应建立控制以防止对信息资产基线的未经授权的添加、更改或偏差，从而限制对攻击面进行意外或恶意增加的可能性。	作为云服务提供商，为配合客户满足监管要求： 华为云的**企业主机安全（Host Security Service, 简称HSS）**为客户提供统一的管理界面，供客户查询并管理云服务，是服务器的贴身安全管家，为客户提供资产管理功能，包括提供账号、端口、进程、Web目录和软件等安全资产信息的管理和分析。 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。此外，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。

5.2 保护

5.2.1 访问控制

控制原则编号	控制原则主题	对客户的提示	华为云的应答

3.1.1	用户账户管理	低：客户应建立用户账户管理机制，根据最小权限和职责分离原则管理员工访问系统和机密数据的权限，实施适当的密码策略及加密功能、账户锁定策略、权限申请审批和复核机制。 中：除上述控制之外，客户应建立用户权限变更的监控告警机制，以及密码生成和修改时与常用密码库的校验机制。 高：除上述控制之外，客户应基于风险考虑对本地访问的非特权账户实施多因素身份验证，并建立为协作计算设备和应用程序的访问控制机制。	客户可以使用华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**对使用云资源的用户账号进行管理。IAM除了支持密码认证之外还支持多因子认证，客户可自主选择是否启用。如果租户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的华为云资源。IAM可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。同时，客户应建立用户访问管理机制，基于最小权限原则进行访问系统权限限制和监督。 华为云制定了内部运维账户的生命周期管理，包括账户的开销户管理、账户责任人/使用人管理、口令管理、开销户监控管理等，账户一旦建立，立即纳入账户管理员的日常维护管理工作。所有运维账户，所有设备及应用的账户均实现统一管理，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。如果运维人员要使用账号，账号管理员可启动授权流程，通过事件单、告警单、变更单等完成授权；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。 在身份认证方面，当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。员工账号用于登录VPN、堡垒机，实现用户登录的深度审计。

3.1.2	特权用户账户管理	低：客户应建立特权账户的严格管理机制，对特权账户实施多因素身份验证。 中：除上述控制之外，客户应建立特权用户的审查机制，将多因素身份验证用于高风险系统，强制执行最小特权原则。 高：除上述控制之外，客户应基于风险考虑建立为协作计算设备和应用程序的访问控制机制（如适用），限制特定特权命令的使用。	在特权账号管理方面，华为云的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。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。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。
3.1.4	物理访问管理	低：客户应实施物理访问管理，对IT硬件、通信系统等高风险或机密信息的物理访问进行限制和记录，对物理访问进行持续监控，定期审查物理访问日志。 中：N/A。 高：N/A。	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了全天候（一天 24 小时、一周 7 天，即 7*24 小时）保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略，严格审核人员出入权限。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。

3.1.5	远程访问管理	低：客户应对员工、承包商和第三方的远程访问使用加密连接和多因素身份验证，为具有网络访问权限的非特权账户实施多因素身份验证。 中：除上述控制外，客户应实施加密机制来保护远程访问的机密性和完整性，通过集中管理的网络访问控制点路由所有远程访问，以便监控远程访问会话和审计用户活动。 高：除上述控制外，客户应按需授权通过远程访问方式执行特权命令等敏感操作，记录并定期审查访问的理由。	华为云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。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。
3.1.8	加密密钥管理	低：客户应建立涵盖密钥生成、分发、安装、更新、撤销和到期的加密密钥管理策略、程序和控制措施，以防止未经授权访问加密密钥。 中：N/A。 高：N/A。	华为云提供了**密钥管理服务（Key Management Service，简称KMS）** **密钥管理服务（Key Management Service，简称KMS）**。它帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM–Hardware Security Module），为租户创建和管理密钥，防止密钥明文暴漏在HSM之外，从而防止密钥泄露。目前已对接KMS服务的华为云服务包括：**云硬盘（Elastic Volume Service，简称EVS）**、**对象存储（Object Storage Service，简称OBS）**、**云备份（Cloud Backup and Recovery，简称CBR）**及**镜像服务（Image Management Service，简称IMS）**等。 华为云制定并实施密码算法应用规范，规定了密码算法的选择规则及应用规则，同时给出了常见应用实例指导。华为云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。

5.2.2 基础设施保护

控制原则编号	控制原则主题	对客户的提示	华为云的应答

3.2.1	网络保护	低：客户应使用网络外围防御工具，对高风险网络端口进行持续监控，通过无线网络进行身份验证和数据传输需要强加密（如适用），在互联网接入点以及DMZ区与内网之间部署防火墙，建立防火墙规则变更和定期审计的机制，部署入侵检测/防御系统，实施技术控制防止未经授权的网络连接。 中：除上述控制外，客户应将企业网络分区，采用纵深防御策略。为远程访问管理控制台实施安全控制。对无线网络部署外围防火墙，使用高强度加密密钥。将访客无线网络与内网进行物理隔离。采用反欺骗措施来检测和阻止伪造的源IP地址进入网络。 高：除上述控制，客户应部署工具和/或制定流程阻止不安全的员工自有设备或未经授权的设备的访问，限制和监控受信任和不受信任区域之间的流量，并定期或按需评估和审查环境变化，已识别差距并采取补救计划。	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、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。 在网络分区分域方面，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，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。 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（PublicService）、资源交付区（POD–PointofDelivery）、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。 华为云对云端数据的隔离是通过**虚拟私有云（Virtual Private Cloud，简称VPC）**实施的，VPC采用网络隔离技术，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合**虚拟专用网络（Virtual Private Network，简称VPN）**或**云专线（Direct Connect，简称DC）**，将VPC与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用VPC的ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。

			在网络边界防护方面，华为云建立了稳固、完善的边界和多层立体的安全防护系统，部署了Anti-DDoS、IDS/IPS、WAF等防护机制。Anti-DDoS快速发现和防护DDoS攻击，实时对流量型攻击和应用层攻击进行全面防护；WAF实时检测和防御Web攻击，对高危攻击进行告警并立刻自动阻断；IDS/IPS实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。
3.2.2	系统配置	低：客户应建立并实施系统安全配置基线，对系统配置变更进行监控。 中：除上述控制外，客户应定期审查关键系统，以识别潜在的漏洞、升级机会或新的防御层，并对不受支持的系统实施控制并定期测试以验证其有效性。 高：除上述控制外，客户应建立适当的控制措施防止设备或系统组件执行未经授权的代码，主动识别漏洞。	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，同时支持客户根据自身业务需求选择适合于自身的安全配置。如在主机安全方面，主机操作系统使用华为统一虚拟化平台（UVP），对CPU，内存和I/O资源隔离管理，主机操作系统已进行最小化裁剪并对服务做安全加固；在虚拟机安全方面，华为云提供镜像加固、网络与平台隔离、IP/MAC仿冒控制、安全组等安全配置。

3.2.3	虚拟化安全	低：客户应制定管理虚拟机映像和快照的安全性、创建、分发、存储、使用、报废和销毁的策略，实施对管理程序和主机操作系统的管理访问的控制措施。 中：N/A。 高：N/A。	华为云对虚拟机采取了一系列安全机制以应对网络安全风险： 华为云的虚拟机安全对网络与平台进行了隔离。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。 此外，华为云的虚拟机安全还有安全组。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。 华为云的虚拟机安全有镜像加固。华为云通过镜像工厂，由专业安全团队对虚拟机操作系统公共镜像进行安全加固，并及时修复系统安全漏洞，最终生成安全更新了的公共镜像，并通过**镜像服务（Image Management Service，简称IMS）**持续提供给租户。 同时提供相关加固和补丁信息以供用户对镜像进行测试、排除故障及其他运维活动时参考。由客户根据相关应用运行及安全运维策略，选择直接使用最新的公共镜像重新创建虚拟机或自行创建已安装安全补丁的私有镜像。

5.2.3 数据保护

控制原则编号	控制原则主题	对客户的提示	华为云的应答

3.3.2	数据保护	低：客户应明确数据加密的标准和要求，对在公共或不受信息的网络传输的机密数据进行加密，对存在在移动设备上的机密数据进行加密，在非生产环境中对客户数据进行脱敏，并制定数据处置和销毁的政策和流程。 中：除上述控制外，客户应采用工具来防止和/或检测未经授权访问或泄露机密数据。 高：除上述控制外，客户应对在专线和受信任区域传输时的机密数据进行加密。	针对于静态数据，华为云为保护租户数据的存储安全采取了一系列的保护机制。 首先，华为云提供了**密钥管理服务（Key Management Service，简称KMS）**。它帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM–Hardware Security Module），为租户创建和管理密钥，防止密钥明文暴漏在HSM之外，从而防止密钥泄露。目前已对接KMS服务的华为云服务包括：**云硬盘（Elastic Volume Service，简称EVS）**、**对象存储（Object Storage Service，简称OBS）**、**云备份（Cloud Backup and Recovery，简称CBR）**及**镜像服务（Image Management Service，简称IMS）**等。 其次，华为云提供的存储和数据库服务均具备高可靠保证。例如EVS云硬盘使用多副本的数据冗余保护机制，采用副本同步写、读修复等措施保证数据一致性，当检测到硬件故障能够自动后台修复，数据快速自动重建，数据持久性可达99.9999999%。；OBS对象存储服务通过支持对象数据的高可靠性，并通过业务节点的高可靠性网络和节点的多冗余设计，使系统设计可用性达99.995%，完全满足对象存储服务高可用的需求，通过提供对象数据多份冗余和保证多份对象的数据一致性自动修复技术，来提供对象数据的高可靠性，系统设计数据持久性高达99.9999999999%；RDS关系型数据库服务采用热备架构，故障系统1分钟自动切换。每天自动备份数据，上传到OBS桶，备份文件保留732天，支持一键式恢复。 针对于传输中的数据，华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过**虚拟专用网络（VPN）**和应用层TLS与证书管理，华为云服务为客户提供控制台和API两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。 针对于数据安全删除，华为云在客户确认删除数据后，会对指定的数据及

			其所有副本进行全面的清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。

5.2.4 安全开发

控制原则编号	控制原则主题	对客户的提示	华为云的应答

3.4.1	安全开发	低：客户应建立系统开发生命周期（SDLC）的管理框架和政策，将访问控制、身份验证、授权、数据完整性、日志记录等安全要求嵌入SDLC的各个阶段中。 中：除上述控制外，客户应制定并实施各阶段的安全标准，建立缺陷管理流程，并对连接互联网的应用程序进行安全测试。 高：除上述控制外，客户应建立并严格实施变更和发布管理流程，对应用与服务间的依赖关系进行充分审查，通过代码审查和/或静态代码分析识别漏洞，并对应用程序进行安全测试。	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。 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。 华为云严格遵从华为对内发布的安全编码规范。华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（CI/CD–Continuous Integration，Continuous Deployment）工具链，通过质量门限进行控制，以评估云服务产品的质量。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。

5.2.5 补丁和变更管理

控制原则编号	控制原则主题	对客户的提示	华为云的应答

3.5.1	补丁管理程序	低：客户应实施补丁管理程序，应确保软件和硬件补丁及时应用。 中：除上述控制外，客户通过工具和/或流程来识别缺少的安全补丁以及补丁的生效天数。 高：除上述控制外，客户应安装覆盖所有服务器的补丁监控软件，审查补丁管理报告以及时进行安全补丁的测试和安装。	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。
3.5.2	补丁评估和测试	低：客户应建立获取、测试和部署基于关键性软件补丁的正式流程，在将补丁应用于系统/软件之前应进行测试。 中：除上述控制外，客户应在部署安全补丁前进行影响评估，维护并定期审查现存漏洞，并定期向管理层报告。 高：除上述控制外，客户应利用自动化和分类技术措施促进大规模和快速的补丁修补。	华为云使用OSM工单系统平台进行OS的配置，补丁发布及升级，在云服务产品上线发布前，云服务团队需对服务发布包（包含补丁包）进行病毒扫描和完整性校验。同时，华为云建立了安全漏洞管理流程，设置了漏洞管理员及相关安全角色为漏洞的评估负责，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。此外，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。

3.5.3	变更管理流程	低：客户应制定变更管理流程，实施变更的申请和审批机制。 中：除上述控制外，客户应在实施变更期间评估网络安全风险，指派适当的人员负责变更审批，对IT基线配置的变更需要正式的变更请求、书面批准和安全影响评估。 高：除上述控制外，客户应实施变更管理系统，并利用工具检测和阻止未经授权的变更。	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。 所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。

5.2.6 修复管理

控制原则编号	控制原则主题	对客户的提示	华为云的应答

3.6.1	修复管理	低：客户应建立修复管理流程，对已识别的问题及时进行修复。 中：除上述控制外，客户应建立重复模拟测试机制以确保中高风险和漏洞得到解决。 高：除上述控制外，客户应建立资产维护和维修的授权审批机制，并及时记录和审查组织资产的维护和维修。针对所不能及时解决的关键和高风险问题，并采取适当缓解措施，并上报管理层。	客户可通过华为云提供**漏洞扫描服务（Vulnerability Scan Service，简称VSS）**，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。同时，客户可使用华为云的**企业主机安全（Host Security Service，简称HSS）**,检测Windows/Linux操作系统与SSH、OpenSSL、Apache、Mysql等软件存在的漏洞，并给出修复建议。此外，华为云可为客户提供**容器安全服务（Container Guard Service，简称CGS）**能够扫描镜像中的漏洞与配置信息，发现镜像中的漏洞并给出修复建议，帮助企业解决传统安全软件无法感知容器环境的问题。 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。 此外，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。

5.3 检测

5.3.1 脆弱性检测

控制原则编号	控制原则主题	对客户的提示	华为云的应答
4.1.1	防病毒和防恶意软件	低：客户应部署自动更新的防病毒和防恶意攻击软件工具，并实施电子邮件保护机制过滤常见的网络威胁。 中：除上述控制外，客户实施的流程和工具（例如沙盒）进行的行为分析，以检测并阻止存在的恶意软件。 高：除上述控制外，客户应建立集中的、自动更新的终端保护机制。	客户可使用华为云的**企业主机安全（Host Security Service, 简称HSS）**，通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，并提供一键隔离查杀能力。同时，客户可部署华为云**Web应用防火墙（Web Application Firewall，简称WAF）**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。 在物理主机层面，通过部署防病毒软件，以实现对恶意软件的攻击防御。华为云桌面终端标准镜像内默认提供防病毒软件，员工默认无法对防病毒软件进行禁用操作。此外，华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。

4.1.2	渗透/模拟测试	低：客户应定期进行渗透测试测试和漏洞扫描。 中：除上述控制外，客户应定期或在发生重大变更之后进行模拟测试。客户应持续进行漏洞扫描，确保全年覆盖所有高风险系统。 高：除上述控制外，客户建立覆盖所有终端的漏洞扫描流程。	华为云建立了漏洞定期扫描机制，每月对DDoS流量清洗服务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。此外，华为云会定期对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。

5.3.2 异常活动检测

控制原则编号	控制原则主题	对客户的提示	华为云的应答

4.2.1	日志监控和分析	低：客户建立流程和控制措施，以及时准确地检测异常安全行为。 中：除上述控制外，客户应将审计日志备份到集中式日志服务器，以防止日志未经授权的更改。 高：N/A。	华为云提供的**云日志服务（Log Tank Service，简称LTS）**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（Cloud Eye Service，简称CES）云监控服务（Cloud Eye Service，简称CES）**，为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。客户可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。 华为云有集中、完整的日志大数据分析系统安全云脑。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源ID(如：源IP、主机ID、用户ID等)、事件类型、日期时间、受影响的数据/组件/资源的ID（如目的IP、主机ID、服务ID等）、成功或失败等信息，以确保支撑网络安全事件回溯和合规。该日志分析系统有强大的数据保存及查询能力，确保所有安全日志保存时间超过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。 华为云安全云脑具备海量日志快速收集、处理、实时分析的能力，采用自研分析引擎，结合AI模型，实现安全日志自动化分析、识别、告警和处置。
4.2.2	安全信息和事件管理	低：客户应建立安全事件管理流程以检测异常活动。 中：除上述控制外，客户应部署检测未授权数据挖掘的工具，以及对安全日志进行主动监控的工具。 高：除上述控制外，客户应使用系统监控和分析员工行为，实施监控敏感数据或文件的措施，利用纵深防御技术来检测和及时响应网络攻击。	鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。

5.3.3 网络事件检测

控制原则编号	控制原则主题	对客户的提示	华为云的应答
4.3.1	事件监控	低：客户应建立事件监控机制，分配监控和报告事件的职责。 中：除上述控制外，客户应建立正常的网络活动基线，对关键资产进行安全监控。 高：除上述控制外，客户应实施评估恶意行为/软件的流程和解决方案。	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。此外，华为云会定期对事件的相关指标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。
4.3.2	检测和警报	低：客户应建立事件检测和告警机制，部署工具并设置适当的告警参数和风险指标，以检测、警告和触发事件响应程序。 中：除上述控制外，客户应通过自动化流程实时检测事件，提供充足的资源以实现持续检测、调查分析和响应。 高：除上述控制外，客户应安装自动化工具以检测对关键系统文件和安全设备的未经授权的变更，实施实时网络监控和检测工具。	

5.3.4 威胁监控与分析

控制原则编号	控制原则主题	对客户的提示	华为云的应答

4.4.1	威胁监控与分析	低：客户应制定针对威胁情报的监控流程。 中：除上述控制外，客户应明确威胁情报监控和分析的职责，建立安全运营中心，对威胁情况进行持续监控。 高：除上述控制外，客户应进行威胁情报分析和报告制定，以确定后续行动措施。将威胁情报用于更新机构的IT安全架构和IT配置标准，预测潜在的攻击和攻击趋势。	作为云服务提供商，为配合客户满足监管要求： 华为云的**威胁检测服务（Managed Threat Detection，简称MTD）**，通过接入目标区域中用户在华为云操作所产生的的IAM日志、DNS日志、CTS日志、OBS日志、VPC日志，持续检测日志中访问者的IP或域名是否存在潜在的恶意活动和未经授权行为，发现异常将及时告警。此服务集成了AI智能引擎、威胁情报、规则基线三种能力检测云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中隐含的异常访问行为，主动发现潜在威胁，对可能存在威胁的访问行为生成告警信息。用户可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护用户的帐户安全、保障服务稳定运行。 **态势感知（Situation Awareness，简称SA）**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。 华为云使用态势感知分析系统安全云脑，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，包括最常见的云攻击威胁：暴力破解、端口扫描、肉鸡、Web 攻击、Web 未授权访问、APT 攻击等。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。

5.4 响应与恢复

5.4.1 对事件响应和恢复的治理与准备

控制原则编号	控制原则主题	对客户的提示	华为云的应答
5.1.1	事件响应和恢复的治理	低：客户应就网络事件响应和恢复在整个机构建立明确的责任分工。 中：除上述控制外，客户应制定可操作的计划来对检测到的网络事件进行响应和恢复。 高：除上述控制外，客户应制定企业范围内整体协同的计划，来对检测到的网络事件进行响应和恢复。	华为云内部制定了安全事件管理机制，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。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。 为配合客户满足监管要求，华为云会在规定的时限内向客户报告安全事件，报告的内容包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。 同时华为云会针对安全事件进行根因分析，制定预防规避措施。此外，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。 华为云遵循ISO22301业务连续性管理国际标准，建立了一套完善的业务连续性管理体系，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。同时，在该体系框架下，定期进行业务影响分析和风险评估，识别关键活动及依赖、评估风险等级，并对识别出的可造成云服务资源中断的威胁制定应对策略，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，测试结果将被注释并记录归档，用以持续改进该计划。此外，华为云可根据客户需要，协助其制定并测试业务连续性计划。 华为云提供高可用基础设施、冗余数据备份、可用区灾备等，客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通

5.1.2	事件响应和恢复准备	低：客户应建立流程和具备能力，以有效地响应和恢复可能因网络事件而受损的关键功能、流程、系统和活动。 中：除上述控制外，客户应制定计划，以恢复和维护可能因网络事件而受损的任何能力或服务。 高：客户应准备计划和财力，以实时地恢复和维护可能因网络事件而受损的任何能力或服务，并将运营损失降至最低。	过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。

5.4.2 分析，缓解与恢复

控制原则编号	控制原则主题	对客户的提示	华为云的应答
5.2.1	分析	低：客户应建立网络事件分析和分类的流程。 中：客户应建立以内部知识和资产为基础的分析和分类网络事件的流程。 高：除上述控制外，客户应建立企业范围的事件意识和管理视角，尽可能利用自动化。	华为云的**威胁检测服务（Managed Threat Detection，简称MTD）**，通过接入目标区域中用户在华为云操作所产生的的IAM日志、DNS日志、CTS日志、OBS日志、VPC日志，持续检测日志中访问者的IP或域名是否存在潜在的恶意活动和未经授权行为，发现异常将及时告警。此服务集成了AI智能引擎、威胁情报、规则基线三种能力检测云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中隐含的异常访问行为，主动发现潜在威胁，对可能存在威胁的访问行为生成告警信息。用户可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护用户的帐户安全、保障服务稳定运行。 **态势感知（Situation Awareness，简称SA）**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

5.2.2	缓解	低：客户应制定降低网络事件影响的流程，包括第三方发生的网络事件。 中：除上述控制外，客户应制定有效和迅速执行根除计划的流程，针对不同类型的重大网络攻击制定单独的遏制策略；制定共享有关网络事件和网络最佳实践的流程。 高：除上述控制外，在适用的情况下，客户应部署自动化机制以支持事件管理、遏制、根除和恢复流程，确保负责事件管理的员工在事件期间与负责网络威胁情报的员工有效协作。	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。 华为云制定安全事件的定级原则和升级原则，根据安全事件对金融机构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金融机构通知流程，将事件通知金融机构。当发生严重的安全事件，已经或可能对大量金融机构造成严重影响时，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金融机构。至少包括事件的描述、起因、影响、华为云已采取的措施、建议金融机构采取的措施等。在事件解决后，会根据具体情况向金融机构提供事件报告。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，以确保能够及时处理重大事件。 此外，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。

5.2.3	恢复和质量保证测试	低：客户应建立并验证以及时、安全的方式恢复受影响的功能、服务和数据方面的流程。 中：客户应建立并验证以及时、安全、弹性的方式恢复受影响的功能、服务和数据方面的流程。 高：客户应建立并验证以及时、安全、有弹性和成本优化的方式恢复整个机构受影响的功能、服务和数据方面的流程。	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–DataCenterInterconnect），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。

5.4.3 网络取证

控制原则编号	控制原则主题	对客户的提示	华为云的应答

5.3.5	证据的保留和存储	低：客户应定义了证据保留期限。 中：客户应建立适当的流程以根据需要存储或归档证据。 高：N/A。	华为云通过集中的日志大数据分析系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志保留时间超过180天。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。此外，**云审计服务（CTS）**为租户提供云服务资源的操作记录,众多产品和服务也均有日志记录功能，且租户可根据自身需求自主选择日志保留时间，以有效支撑异常活动分析。 华为云制定安全事件的定级原则和升级原则，根据安全事件对金融机构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金融机构通知流程，将事件通知金融机构。当发生严重的安全事件，已经或可能对大量金融机构造成严重影响时，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金融机构。至少包括事件的描述、起因、影响、华为云已采取的措施、建议金融机构采取的措施等。在事件解决后，会根据具体情况向金融机构提供事件报告。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，以确保能够及时处理重大事件。 此外，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。

5.4.4 沟通与改进

控制原则编号	控制原则主题	对客户的提示	华为云的应答

5.4.1	上报	低：客户应建立流程以通知潜在网络事件的适当利益相关者。 中：除上述控制外，客户制定的沟通程序应包含通知其他组织可能影响他们或其客户的事件和通知媒体有关事件的程序。 高：N/A	华为云制定安全事件的定级原则和升级原则，根据安全事件对金融机构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金融机构通知流程，将事件通知金融机构。当发生严重的安全事件，已经或可能对大量金融机构造成严重影响时，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金融机构。至少包括事件的描述、起因、影响、华为云已采取的措施、建议金融机构采取的措施等。在事件解决后，会根据具体情况向金融机构提供事件报告。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，以确保能够及时处理重大事件。 此外，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。
5.4.2	事件报告	低：客户应建立正式的流程，向必要的利益相关者提供定期事件报告。 中：客户制定网络事件的指标和信息仪表盘作为报告的一部分。 高：客户应引入自动化以加快上报、报告和响应时间。	
5.4.3	改进	低：客户应建立正式的改进流程，以识别从过去的网络事件中改进响应和恢复能力的机会。 中：除上述控制外，客户应进行模拟测试演练以评估事件响应和恢复能力。 高：除上述控制外，客户应定期参考所有安全事件以进行趋势分析，改进网络安全措施和政策。	

5.5 态势感知

5.5.1 威胁情报

控制原则编号	控制原则主题	对客户的提示	华为云的应答

6.1.1	威胁情报	低：客户应订阅并用威胁情报来监控相关的网络威胁，加强其网络风险管理和控制。 中：除上述控制外，客户应实施正式的网络威胁情报计划，定期评估网络情报的适用性，实施从同业和政府收集信息的协议，维护网络威胁情报的集中只读存储库。 高：除上述控制外，客户应建立网络情报框架，实施正式的威胁情报计划，以实时自动地从多个来源检索威胁情报，实施威胁分析系统，对威胁进行告警并采取必要行动。	作为云服务提供商，为配合客户满足监管要求： 华为云的**威胁检测服务（Managed Threat Detection，简称MTD）**，通过接入目标区域中用户在华为云操作所产生的的IAM日志、DNS日志、CTS日志、OBS日志、VPC日志，持续检测日志中访问者的IP或域名是否存在潜在的恶意活动和未经授权行为，发现异常将及时告警。此服务集成了AI智能引擎、威胁情报、规则基线三种能力检测云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中隐含的异常访问行为，主动发现潜在威胁，对可能存在威胁的访问行为生成告警信息。用户可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护用户的帐户安全、保障服务稳定运行。 **态势感知（Situation Awareness，简称SA）**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。 华为云使用态势感知分析系统安全云脑，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，包括最常见的云攻击威胁：暴力破解、端口扫描、肉鸡、Web 攻击、Web 未授权访问、APT 攻击等。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。

5.6 第三方风险管理

5.6.1 外部连接

控制原则编号	控制原则主题	对客户的提示	华为云的应答
7.1.1	识别	低：客户创建网络和系统数据流图，识别所有外部连接和网络连接的第三方，并定期进行审查和更新。 中：除上述控制外，客户应识别和评估外部连接的相关风险。 高：除上述控制外，客户应对识别的风险实施适当风险缓解策略。	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、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。 在网络分区分域方面，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，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。 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（PublicService）、资源交付区（POD–PointofDelivery）、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。 华为云对云端数据的隔离是通过**虚拟私有云（Virtual Private Cloud，简称VPC）**实施的，VPC采用网络隔离技术，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的

7.1.2	保护	低：客户应通过企业范围内的安全架构的边界保护设备组成的管理接口进行外部网络或信息系统的连接。 中：除上述控制外，客户应实施控制以限制与信息系统的不必要的外部网络连接，并根据需要和最低权限原则授予访问权限，设置默认拒绝网络通信流量，定期监控和测试外部第三方连接。 高：除上述控制外，出站流量应通过预定义的网络阻塞点路由，使用网络安全设备对入站流量进行保护，使用集中的控制台或界面来监控和管理代理服务器，并采用边界防护机制。	虚拟网络构建与配置：一方面，结合**虚拟专用网络（Virtual Private Network，简称VPN）**或**云专线（Direct Connect，简称DC）**，将VPC与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用VPC的ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。 华为云各服务可通过公开的 API 进行配置管理，对接企业已有的 IT 管理和审计系统。考虑到 API 对云服务承载的重要功能和其在 HTTP 应用层面临的安全威胁，业界普遍把 API 视为云服务至关重要的安全边界，采用多重机制和措施进行重点保护。调用华为云开放的 API 是通过华为自研的 API 网关实现的。API 网关支持以下机制和场景使API 得到有效保护： （1）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。 （2）传输保护：API 调用需使用 TLS 加密以保证传输的机密性。目前 API 网关所有对外网开放的 API 均使用 TLS 1.2 版本加密协议，并且支持 PFS（Perfect Forward Secrecy）安全特性。 （3）边界防护：API 网关结合 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。通过负载均衡器对 TLS 加密传输进行解密，多层高级边界防护机制可对 API 网关流量明文进行监控，对攻击执行阻断。 （4）API 流量控制：API 网关实现对用户调用 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。API 网关提供针对 API 级别和租户级别的秒级流控配置。每个开放的 API 在 API 网关需要配置对应的流控信息，在单位时间内，每个 API 基于所有华为云租户调用该 API 次数的配额、每个华为云租户调用该 API 次数的配额分别进行流控。

5.6.2 第三方管理

控制原则编号	控制原则主题	对客户的提示	华为云的应答
7.2.1	合同管理	低：客户应与联网并处理敏感或关键的机构数据的第三方签署相关安全与隐私要求的合同，明确第三方的安全与隐私责任、机构对第三方违约的索赔权及合同终止时的数据返还或销毁要求。 中：除上述控制外，客户应在与第三方的协议中约定网络安全事件和漏洞通知的责任。 高：除上述控制外，客户应与第三方建立终止/退出策略，并定期进行测试，将中高风险项及其处理方法提交管理层批准。	华为云明确定义了与客户之间的安全责任共担模型，关于责任共担模型的具体内容可参见本文第3章。 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。 同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。华为云可能会随时自行修改或中止服务或修改或移除服务的功能。如果您订阅的服务发生重大变更或中止，我们会通过在我们的网站发布通知或其他方式通知您。
7.2.2	尽职调查	低：客户应对第三方服务提供商的网络安全能力、人员能力等进行充分的尽职调查。 中：客户应定期对第三方服务提供商进行安全评估或审计。 高：除上述控制外，客户应制定和实施对分包商的网络安全状况进行定期安全评估的程序。	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。 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。

5.6.3 对第三方风险的持续监控

控制原则编号	控制原则主题	对客户的提示	华为云的应答

7.3.1	对第三方风险的持续监控	低：客户应对联网并处理机构敏感或关键数据的第三方建立定期的网络安全监控程序。 中：除上述控制外，客户应基于第三方的风险考虑对第三方监控的深度和频率方面的调整。 高：除上述控制外，客户应对第三方的安全审计报告进行定期现场评估或审查，基于最小特权原则，跟踪第三方员工对于机构托管系统上的敏感和关键数据的访问。	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。 华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，华为云目前获得了国际上多项权威的安全与隐私保护认证，第三方测评公司也会定期对华为云展开保密性、安全充分性和合规性的审核并出具第三方审计报告。关于第三方审计报告的获取的要求，可以根据实际情况在客户签订的协议中约定。 华为云内部也建立了完善的供应商管理机制，会对外包商以及外包人员进行严格的安全管理，并会定期对供应商进行审计和安全评估。华为云会将客户在合同中的安全要求传递给供应商，确保供应商提供的产品和服务能满足华为云客户的安全要求。此外华为云会根据不同客户的需求，在重要供应商发生变更时，及时对客户进行通知。

6 结语

本文描述了华为云如何为客户提供遵从C-RAF 2.0成熟度评估矩阵要求的云服务，并表明华为云遵守中国香港金管局（HKMA）发布的重点监管要求，有助于客户详细了解华为云对C-RAF 2.0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、构建和部署遵从中国香港金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供一般性参考，不具备任何法律效力或构成任何形式的法律建议，客户应酌情评估自身使用云服务的情况，并负责确保在使用华为云时对相关中国香港金融行业监管要求的遵从性。

7 版本历史

日期	版本	描述
2022年8月	1.0	首次发布