华为云中华人民共和国香港特别行政区金融行业监管要求遵从性指南

文档版本 1.2

发布日期 2023-08-03

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 简介

香港金融管理局（金管局）发布了一系列指引及通告，为香港金融机构进行信息科技风险管理提供了实用指南。随着金融机构在业务转型过程中逐渐引入先进技术，如将业务部署在云环境中运行，金管局期望其建立有效的科技风险管理框架，在实现其自身商业目标的同时，也最大限度地降低风险，并满足监管要求。

华为云持续关注金管局发布的监管指引及通告，并致力于协助金融客户满足这些监管指引及通告的要求。本文将针对金融机构通常需遵循的以下监管指引及通告，详细阐述华为云将如何协助其满足监管要求。

监管指引：

- **TM-G-1 科技风险管理的一般原则监管政策手册**：就管理科技有关风险时应考虑的一般原则向认可机构提供建议。
- **SA-2 外包监管政策手册**：列出金管局对外包活动的监管方式及建议认可机构在外包业务时需处理的主要事项。
- **TM-G-2 持续业务运作规划监管政策手册**：说明金管局对持续业务运作规划的监管方式，以及金管局期望认可机构在持续业务运作规划时会考虑的稳健做法。
- **虚拟银行的认可指引**：列出了金管局在决定是否认可虚拟银行在港开展银行业务时所考虑的原则。
- **云计算指南**：说明金管局期望认可机构在采用云计算时需考虑实施的风险管理举措。
- **TM-E-1 电子银行风险管理**：金管局就认可机构管控与电子银行业务相关的风险提出了指导。

  注：认可机构：金管局负责监管并认可的香港持牌银行、有限制牌照的银行及接受存款的公司。上述三类机构被统称为认可机构。

监管通告：

- **客户数据保护通告**：提醒认可机构保护客户数据机密性的重要性，以及保护客户数据的一些关键控制措施。
- **事件响应与管理程序通告**：提醒认可机构，必须具备有效的事件响应和管理能力及程序以处理重大事件，并列出认可机构就此类事件进行任何公众沟通时应遵循的原则。

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，对云服务各项服务的集成、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：

认证	描述
ISO 20000-1:2011	ISO 20000 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。
ISO 27001:2013	ISO 27001 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。
ISO 27017:2015	ISO 27017 是针对云计算信息安全的国际认证。ISO 27017 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。
ISO 22301:2012	ISO 22301 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。
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 Level 3 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 Level 3 等级认证。
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

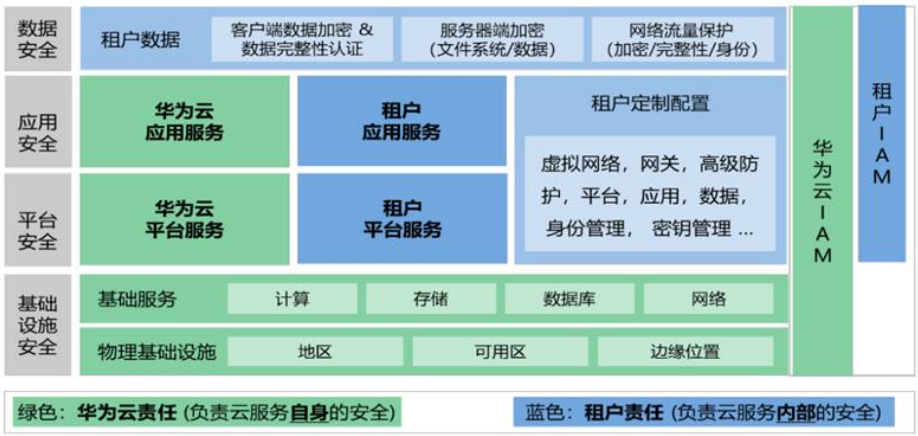
认证	描述
	部控制情况出具的独立审计报告。
PCI DSS 认证	支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
CSA STAR 金牌认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务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。华为私有云和公有云双双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。
国际通用准则 CC EAL3+	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。
ISO 27018:2014	ISO 27018 是专注于云中个人数据保护的国际行为准则。ISO 27018 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。
ISO 29151:2017	ISO 29151 是国际个人身份信息保护实践指南。ISO 29151 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。
ISO 27701:2019	ISO 27701 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 ISO 27701 表明了其在

认证	描述
	个人数据保护具有健全的体制。
BS 10012:2017	BS 10012 是 BSI 发布的个人信息数据管理体系标准，BS 10012 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。

3 华为云安全责任共担模型

华为云的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。

租户的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。关于更多华为云基础设施的信息，可参见华为云官网“全球基础设施”。

5 华为云如何遵从及协助客户满足《TM-G-1 科技风险管理的一般原则监管政策手册》的要求

《TM-G-1 科技风险管理的一般原则监管政策手册》为认可机构进行科技风险管理提供了通用原则和最佳实践指引，指引涵盖了信息科技治理、安全管理、系统开发及变更管理、信息处理、通信网络、技术服务供应商管理六大领域。

以下内容将总结 TM-G-1 中与云服务供应商相关的控制要求，并详细阐述华为云作为认可机构的云服务供应商时，会如何帮助认可机构满足这些控制要求。

5.1 安全管理

TM-G-1 第三章“安全管理”要求认可机构建立适当的安全管理机制，涵盖信息分类及保障、身份认证及访问控制、安全管理及监控、系统安全、物理和人员安全等安全领域。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
3.1	信息分类及保障	认可机构应保护存储信息的所有纸质或电子媒介，并建立稳妥的流程，以弃置及销毁存放在媒介上的敏感信息。	客户应考虑对所有存储信息的介质（包括纸质和电子）进行保护。针对存储金融行业客户内容数据的存储介质，华为云制定了完善的介质管理流程，确保存储在介质中的数据的安全。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循适用的法律法规，以及与客户之间的协议约定，按照数据销毁标准清除客户的数据。实现方式如下：当客户确认删除操作后，华为云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。
		认可机构应采用业	客户在使用加密措施保护数据时，应考虑采用业内

编号	控制域	具体控制要求	华为云的应答
		内认可的加密解决方案及稳健的密钥管理手法，以保护有关的加密密钥。	认可的加密算法和密钥管理机制。 目前，华为云云硬盘、对象存储、镜像服务和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 华为云服务端加密功能还集成了**数据加密服务（Data Encryption Workshop，简称 DEW）**的密钥管理功能，由 DEW 进行密钥全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW 采用分层密钥管理机制，方便各层密钥的轮换。通过 DEW 的控制台或 API 进行关联设置，各存储服务加密数据时使用的加密密钥，能够由保存在 DEW 中的客户主密钥进行加密，该客户主密钥又由保存在硬件安全模块 HSM 中的根密钥进行加密，构成了一条完整的安全、可信的密钥链。HSM 经过严格的国际安全认证，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取根密钥。
3.2	身份认证及访问控制	认可机构应使用适当的身份认证机制来限制对信息及应用系统的访问。对于每个应用系统，所有用户都应使用唯一的用户标识码（例如用户 ID）和适当的身份验证方法（例如密码）进行标识，以确保对其活动负责。 认可机构应制定有效的密码规则，以确保不会使用容易被猜中的密码，并定期更改密码。 较高风险的交易或活动应采用更严格的认证方法，通常应采取多因素认证机制对用户进行身份认证。	华为云通过**统一身份认证服务（Identity and Access Management，简称 IAM）**为客户提供适合企业级组织结构的用户账号管理和身份认证。每一位华为云客户在华为云都拥有唯一可辨识的用户 ID，并提供多种用户身份验证机制，包括账号密码、多因素认证等。 IAM 支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM 还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。 IAM 同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。 同时，华为云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。此外，还采用双因子认证对华为云运维人员进行身份认证，如 USB

编号	控制域	具体控制要求	华为云的应答
			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。
3.2	身份认证及访问控制	认可机构应对特权账号和紧急账号进行如下管控： • 仅在必要的情况下对用户授予特权或紧急账号； • 特权或紧急账号的使用必须经过审批； • 需对特权或紧急账号进行的操作活动进行监控； • 采取安全措施保护特权和紧急账号，在用户交还特权或紧急账号时应立即更改密码。	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。 同时，为配合遵从监管要求，华为云还做到： • 对于运维人员实行基于角色的访问控制，限定不同岗位不同职责的人员只能对所授权的运维目标进行特定操作，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仅需要经过多级的评审和批准。 • 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。运维人员首先通过双因子认证接入运维环境，再集中从堡垒机跳转到目标机进行操作，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。 • 目标机的口令被堡垒机回收并定期更新，确保运维人员无需也无法获取口令。
3.3	安全管理及监控	认可机构应设立安全管理职能及制定正式程序，以管理系统资源及应用系统权限的分配，并监控系统资源的使用，以侦测是否有异常或未经授权进行的活动。 认可机构应在安全管理职能上进行职责分离，或采取其他补偿措施，以减少未授权行为。 认可机构应制定事件响应及通报程	华为云的统一身份认证服务（IAM）可允许客户的租户管理员灵活地进行用户权限管理，控制对云资源的创建、删除、修改、设置等操作的权限。此外，华为云通过**云审计服务（Cloud Trace Service，简称 CTS）**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。 同时，为配合客户满足权限分配的要求，华为云内部人员的权限创建、变更及撤销均需经过指定人员的正式审批。所有运维账号，所有设备及应用的账号均实现统一管理，并通过统一审计平台集中监控，并且自动审计，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。账号管理员根据华为云内部规范的账号权限管理机制，对用户权限进行定期审核。 华为云遵从法律法规要求，具备集中、完整的日志审计系统。内部人员运维操作均被日志平台采集并

编号	控制域	具体控制要求	华为云的应答
		序，程序应包括及时向金管局汇报与 IT 相关的欺诈活动或重大安全事件。	记录。华为云的日志审计系统有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。华为云设置独立的内审部门，定期对运维流程各项活动进行审计，以及时发现、纠正违规行为。 此外，华为云拥有完善的安全事件定级处置流程，根据安全事件对全网及客户的影响，对事件进行分级响应。同时，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，对相关安全事件及时披露，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。 记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触发的操作。
3.4	系统安全	认可机构应制定以下管控程序以保护应用程序、操作系统、系统软件及数据库的安全： • 通过身份认证及授权对数据和程序进行访问控制； • 定期检查静态数据（如系统参数）的完整性； • 对操作系统、系统软件、数据库和服务器进行安全配置，并禁用或删除所有不必要的服务和程序。应考虑使用安全工具来加强关键系统和服务器的安全性； • 清晰划分职责，以确保机构能及时识别、评价及测试供应商开发	为配合客户遵从监管要求，华为云服务产品和组件遵从华为安全设计原则、规范、基线，提供了多层次的安全防护和保障： • 华为云的统一身份认证服务（IAM）为客户提供身份认证和云上资源访问控制。 • 采取完整性校验机制保证系统参数的完整性，如在虚拟机操作系统层面，华为云镜像服务支持镜像完整性检测。在基于镜像创建虚拟机时，系统会自动检查镜像完整性，以确保创建的虚拟机包含完整的镜像内容。同时，通过完善的变更管理程序，防止华为云内部运维人员对系统配置参数进行未授权变更。 • 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。 • 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。在出现开源漏洞问题时，华为云将第一时间发现漏洞并修复。漏洞响应时，须将开源及第三方软件作为服务和解决方案的一部分开展测试，验证开源及第三方软件的已知漏洞是否修复，并在服务的 Release notes 里体现开

编号	控制域	具体控制要求	华为云的应答
		的必要补丁程序及安全更新程序，并适时地应用到相关系统内； • 记录操作系统、系统软件、数据库及服务器所有配置，并定期审核安全配置； • 对于系统及用户的活动，应保存充足的记录，并进行充足的监察，以识别异常行为，有关的记录数据应稳妥保管，以免遭到篡改。	源及第三方软件的漏洞修复列表。 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，同时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。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。
3.6	物理和人员安全	认可机构应采取物理安全措施，以保护计算机和其他设备免受损坏或未经授权的访问。 数据中心选址时应充分考虑环境风险因素（如邻近具危险性的工厂）。此外，应监控可能会对信息处理设施的运行造成不利影响的环境因素。	为配合客户遵从监管要求，华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以确保华为云数据中心的物理和环境安全 。更多有关物理和环境安全的详细信息，可参考已发布的《华为云安全白皮书》。
3.6	物理和人员安全	在聘用长期及临时性质的科技人员及合约员工应有适当的审查程序（包括核实身份及背景审查）。对与敏感的科技有关的职位来说，此举更为重要。	华为云遵循华为公司的整体人力资源管理框架，在任用华为云正式员工或外包人员时，均进行严格的背景审查，确保员工背景和资历适合华为云安全业务要求，其中针对关键岗位会实施专项管理。

5.2 系统开发及变更管理

TM-G-1 第四章“系统开发及变更管理”中要求认可机构制定系统开发生命周期的项目管理方法及流程，并建立规范的变更管理程序。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.2	项目生命周期	认可机构应制定及执行一套完整的项目周期管理方法，以规定重要系统开发、实施及运维过程。 应由独立的部门（如质量保证部门、科技审计小组）就跟科技有关的主要项目进行质量审查，如有需要，法律及法规遵行部门应提供协助。 应制定正式的验收程序，以确保只有经正式测试及核准的系统才可在生产环境发布，系统及用户验收测试应在独立于生产环境以外的环境进行。除非数据已经脱敏并事先获得数据所有者的核准，否则生产数据不应用于开发或测试。	为配合客户遵从监管要求，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。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公司对内发布的多种编程语言的安全编码规范。使用静态代码扫描工具例行检查，其结果数据进入云服务工具链，以评估编码的质量。所有云服务在发布前，均须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。 华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，确保发布的云服务满足安全要求，测试在与生产环境隔离的测试环境中进行，并避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱敏，使用完成后需要进行数据清理。 此外，华为云云平台版本、重要云服务上线前，需要通过华为公司全球网络安全与用户隐私保护官和首席法务官的严格审查，针对所服务区域的安全隐私要求的遵从性进行分析、判断，确保为华为云以及华为开发的云服务满足各区域法律法规和客户安全需求。
4.3	变更管理	认可机构应制定正式的变更管理程	客户应考虑通过正式的程序来管理变更。为配合客户遵从监管要求，华为云制定了规范的变

编号	控制域	具体控制要求	华为云的应答
		序，程序应涵盖变更的影响评估、变更的计划、跟踪、监控、实施以及变更回滚等。 同时，认可机构应制定正式的紧急变更管理程序，规定紧急变更的审批机制、紧急变更的执行规范等。	更管理流程，生产环境的各要素发生变更，都需要通过有序的活动进行变更管理。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。同时华为云制定了更细粒度的变更操作规范，指导整个变更的实施、跟踪以及变更执行后的验证，确保变更达到预期目的。 同时，华为云也制定了规范的紧急变更管理流程。若紧急变更影响到用户，会按规定的时限提前通过公告、邮件、电话、会议等方式与用户沟通；若紧急变更不满足提前规定的通知时限，变更将升级至华为云高层领导，并在变更实施后及时对用户公告。 紧急变更均留有记录，在变更执行前保留旧的程序版本及数据，在变更过程中通过双人操作等机制保证变更顺利进行，尽量减少对生产环境的影响。变更实施后，有专人进行验证，确保变更达到预期的目的。

5.3 信息处理

TM-G-1 第五章“信息处理”中要求认可机构应制定适当的程序，对与信息处理设施相关的操作活动进行规范。控制要求涵盖 IT 运营管理及支持、性能管理及容量规划、IT 设施及设备运维、灾难恢复计划这四个领域。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
5.1	IT 运营管理及支持	认可机构应建立事件管理系统，对 IT 操作事故做出迅速响应，向有关的信息技术管理人员汇报事故，并对事件进行记录、分析与跟踪，直至事件得到解决。	客户应考虑通过事件管理系统对 IT 操作事故作出及时的响应。为配合客户遵从监管要求，华为云内部制定了完善的事件管理流程，秉承快速发现、快速定界、快速隔离与快速恢复的“四快”原则，根据事件对全网及客户的影响，对事件进行分级响应，并通过工单系统对事件进行记录和跟踪，确保事件可被妥善解决，并进行适当的根因分析。 此外，华为云为客户提供售后服务保障，华为

编号	控制域	具体控制要求	华为云的应答
		认可机构可成立求助台，就技术相关的事件为用户提供前线支持，并将事件移交至有关部门进行调查及解决。	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、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由 IM 企业群、技术服务经理(TAM)、服务经理等组成的专属支持。
5.2	性能监控及容量规划	认可机构应制定适当的程序，以确保持续监控应用系统的性能，并及时地、全面地汇报异常情况。 监控性能的程序应包括预测功能，在问题未对系统性能造成影响时，应能及早识别及纠正。同时该程序应有助于工作量预测，以便识别趋势，以及提供容量计划所需的信息。	客户应考虑通过正式的程序来管理系统容量。为配合客户遵从监管要求，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。 同时，华为云的**云监控服务（Cloud Eye）**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。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。
5.3	IT 设施及设备运维	认可机构应定期对 IT 设施和设备进行维护与检修，同时，应妥善保存记录，并维护硬件及设施的详细清单，以便管控及追溯所有购入及租用的硬件与软件，或便于对资产进行定期盘点。	为配合客户遵从监管要求，华为云对数据中心进行例行监控，定期对受控区（包括机房区的配电箱、PDU 配电柜、消防设施、安防设施，支持设施区的空调系统、排水系统等）进行巡检，并要求登记巡检结果，确保安全隐患能被及时发现并修复，保证设备稳定运行。 此外，华为云通过资产管理系统维护硬件及设施的详细清单，并定期盘点及更新。
5.4	灾难恢复计划	认可机构应制定信息技术的灾难恢复计划，以确保关键应用系统及服务可按照业务恢复需求恢复正常。	为配合客户满足容灾需求，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

编号	控制域	具体控制要求	华为云的应答
			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。

5.4 通信网络

TM-G-1 第六章“通信网络”中要求认可机构实施管控措施，以保护网络通信设施及网络中的信息，防止对网络服务的未授权访问。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
6.1	网络管理	网络设计应保证网络服务的健壮性，并具备完善的网络管理规范。网络拓扑、设计标准及操作程序应文档化，定期审核文档并按要求更新后传达给员工。 认可机构应识别出支撑网络服务持续运行的关键通信设施，并设立备用路径，以减少单点故障。 此外，应持续监控网络，以减少网络过载并检测网络入侵行为。 最后，应保护网络分析和监控工具免遭未授权使用。网络工具亦应严格只限于被授权员工使用，并遵循严格的审批及检查程序。	华为云可帮助客户构建网络安全防护体系，保障客户云服务的安全。在互联网边界客户可通过部署 **Anti-DDoS 流量清洗服务**，来完成对异常和超大流量攻击的检测和清洗；通过**虚拟私有云（Virtual Private Cloud，简称 VPC）**对关键网络分区进行划分和隔离；部署 **Web 应用防火墙（Web Application Firewall，简称 WAF）**应对 Web 攻击以保护部署在 DMZ 区、面向外网的 Web 应用服务和系统。 同时，华为云内部制定了完善的网络管理规范和相关的操作程序，确保所有相关人员在日常运维运营过程中遵守管理规范和操作程序的要求，并对相关文档进行定期审查及更新，更新后在公司内部进行发布。 华为云通信基础设施具备高可用性，将系统故障给客户带来的影响降到最低。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，进一步排除单点故障的风险。 华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。 华为云对于内部人员实行基于角色的访问控制权限管理，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使用网络分析和监控工具。

编号	控制域	具体控制要求	华为云的应答
6.2	网络安全及认证	为防止不安全的网络连接，认可机构应制定及执行有关使用网络及网络服务的程序。 此外，认可机构应对内部网络划分区域，对不同网络区域之间的敏感数据交互进行适当管控及保障，以免数据遭到篡改。 最后，认可机构应确保定期检查网络设备安全参数设置，维护及定期审查关键网络设备上日常活动的审计追踪记录。网络操作人员应能够即时获得关于潜在的安全问题的告警。	华为云为客户提供的虚拟私有云（VPC）服务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，对进出子网以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，华为云根据业务功能和网络安全风险，采用物理和逻辑控制并用的隔离手段，将数据中心划分为多个安全区域。在实现区域隔离上，不再是简单地使用防火墙实现，也会运用革新技术，如软件定义边界（SDP – Software Defined Perimeter）。并且，不止定义网络层区域边界，还采用多层边界划分与隔离协防，从网络层、平台层、应用层一直到用户身份层，都有信任边界和相应的访问控制。 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。所有网络设备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由日志大数据分析系统统一收集，以确保支撑网络安全事件回溯和合规。同时，华为云联动分析各安全设备的告警信息，可快速发现潜在或已发生的安全事件，并及时采取响应措施。

5.5 技术服务供应商管理

TM-G-1 第七章“技术服务供应商管理”中要求认可机构对技术服务供应商进行适当管理，减少服务外包给组织带来的风险。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
7.1	技术外包管理	认可机构管理科技外包应考虑采用以下管控措施： 科技服务供应商应具备足够资源及专业知识，以符合认可机构 IT 管控政策的实质内容； 外包协议应明确规定技术服务供应商的服务水平及	为配合客户行使对科技外包的监管，华为云线上的《华为云用户协议》对客户和华为的安全职责进行划分，华为云《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，需通知认可机构，并对分包的服务负责。

编号	控制域	具体控制要求	华为云的应答
		其他责任，以及软件与硬件拥有权的事项等。同时，协议中应要求服务供应商聘用分包商时需告知认可机构或获得批准，并对分包的服务负责； 认可机构亦应进行年度审核，以确保关键的技术服务供应商有足够的信息技术管控环境。	此外，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，并提供专人协助，积极响应及配合客户方发起的审计活动。

6 华为云如何遵从及协助客户满足《SA-2 外包监管政策手册》的要求

《SA-2 外包监管政策手册》通过阐述业务外包时应关注的主要事项，为认可机构实施业务外包提供了指引。对认可机构的控制要求覆盖服务供应商能力、外包协议、客户数据机密性、外包活动管控、应急计划、外包数据的访问等领域。

以下内容将总结 SA-2 中与云服务供应商相关的控制要求，并详细阐述华为云作为认可机构的云服务供应商时，会如何帮助认可机构满足这些控制要求。

6.1 服务供应商的能力

章节 2.3“服务供应商的能力”要求认可机构在启用服务供应商前，应进行尽职调查，确保供应商的资质，并在服务过程中对其表现进行持续监控。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.3	服务供应商的能力	在选择服务供应商前，认可机构应进行适当的尽职调查，需从以下几方面对供应商进行评估： 1. 财务稳健状况； 2. 声誉； 3. 管理能力； 4. 技术能力； 5. 运营能力； 6. 与认可机构的企业文化和未	**a.财务稳健状况：**华为云是华为的云服务品牌，自 2017 年正式上线以来，华为云一直处于快速发展中，收入保持强劲增长态势。全球权威咨询机构 IDC 发布的《2019 年 Q1 中国公有云服务市场跟踪报告》显示，从 IaaS+PaaS 整体市场份额来看华为云营收增长超过 300%，华为云 PaaS 市场份额增速接近 700%，在 Top5 厂商增速排名第一，位居中国公有云服务商第一阵营。 **b.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。 **c.管理能力：**华为云继承了华为公司的风险管理能力，建立了完善的风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中有效控制风险，力求业绩增长和风险之

		来发展策略的配合程度； 7. 对银行业的熟悉程度； 8. 紧贴市场创新步伐的能力。	间的最优平衡，持续管理内外部风险，保障公司持续健康发展。 **d.技术能力：**华为云用在线提供云服务的方式，将华为 30 多年在 ICT 基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在 AI 领域，华为云 AI 已在城市、制造、物流、互联网、医疗、园区等 10 大行业的 300+个项目进行落地。在多元架构方面，华为云打造了基于 X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 **e.运营能力：**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。 **f.与认可机构的企业文化和未来发展策略的匹配程度：**华为云在产品和服务规划和阶段会根据客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。 **g.对银行业的熟悉程度：**华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。同时，华为云已委托第三方开展独立评估，将华为云的内部管控现状与香港金管局发布的监管指引和公告要求对比，进行差距分析，并确保任何差距项均得到整改。 **h.紧贴市场创新步伐的能力：**自上线以来，华为云一直坚持技术创新，发布了一系列业界领先的新品和升级，覆盖云安全、DevOps、云容器引擎和微服务引擎、服务网格、计算、云存储、网络、云容灾等多个领域，让产品始终保持先进性。

6.2 外包协议

章节 2.4“外包协议”要求认可机构与服务供应商签订的协议中应就相关事项进行明确规定。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答

2.4	外包协议	认可机构与其服务供应商签订的服务协议应清楚列明所提供的服务内容和水平，以及服务供应商在合约下的责任和义务。	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。

6.3 客户数据机密性

章节 2.5“客户数据机密性”要求认可机构外服务在外包过程中要保障客户数据的机密性。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.5	客户数据机密性	认可机构应确保遵守客户数据的保密要求并采取防范措施保护客户数据的完整性和机密性。	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，并严格遵守《个人资料（私隐）条例》所述的数据保护原则。同时，在与金融行业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。
2.5	客户数据机密性	外包协议终止时，认可机构应确保向服务供应商取回所有客户数据或将数据销毁。	在服务协议终止时，客户可通过华为云提供的云数据迁移服务（CDM），将内容数据从华为云中迁移出去，如迁移至本地数据中心。 在客户确认删除数据后，华为云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。

6.4 外包活动的管控

章节 2.6“外包活动的管控”要求认可机构对外包服务供应商的服务进行持续监控，并建立与外包问题相关的报告机制。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.6	外包活动的管控	认可机构应对服务供应商的合约表现、遇到的重大问题、财政状况及风险情况、应急计划的有效性进行监控。 此外，认可机构应制定汇报程序，使与外包业务有关的问题能迅速升级至认可机构及服务供应商的管理层处理。	华为云每年定期接受专业第三方审计机构的审计，并可在客户需要时可向其提供相关审计报告。华为云也会安排专人负责客户方发起的尽职调查。 此外，华为云为客户提供售后服务保障，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、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由 IM 企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

6.5 应急计划

章节 2.7“应急计划”要求认可机构服务外包过程中应针对应急计划作出规划，以保障业务连续性。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.7	应急计划	认可机构及服务供应商应维护和定期测试应急计划，应急计划中应包含日常运营和系统问题的应急安排。	华为云制定了完善的突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。

6.6 外包数据访问

章节 2.8“外包数据访问”要求认可机构在服务外包时需保证金管局可调用被外包的数据，并对服务供应商进行适当审计。相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.8	外包数据访问	认可机构应在其场所内保存适当的最新记录，可供金管局检查，并确保其从服务供应商处取回的数据应准确，并随时可供金管局在香港查看。 认可机构应确保与服务供应商签订的协议载有条款，容许金管局对服务供应商的运作及管控制度做出审查。	华为云为客户提供多种数据备份和迁移服务，可帮助客户将数据迁移至客户本地数据中心等场所。同时华为云也为客户提供多种安全机制，保障客户数据存储和传输过程中的完整性。 如果客户有需要，可以与华为云签订线下合同，华为云在合同模板中将包含容许金管局对华为云的运作及管控制度进行审查的条款，并可根据不同客户的需求进行定制化。在金管局对华为云进行审查时，华为云将根据内部的流程，提供专人协助，积极配合审核。

7 华为云如何遵从及协助客户满足《TM-G-2 持续业务运作规划监管政策手册》的要求

《TM-G-2 持续业务运作规划监管政策手册》为认可机构实施有效的业务连续性管理提供了实施指引，涵盖业务影响分析恢复策略、业务连续性计划的开发、业务和技术恢复的备用站点、业务连续性计划的实施等方面。

以下内容将总结手册中与云服务供应商相关的控制要求，并详细阐述华为云作为认可机构的云服务供应商时，会如何帮助认可机构满足这些控制要求。

7.1 业务影响分析和恢复策略

《TM-G-2 持续业务运作规划监管政策手册》第三章“业务影响分析和恢复策略要求”要求认可机构执行业务影响分析，识别关键业务及关键业务的恢复目标，并制定相应的恢复策略。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
3.1	业务影响分析	认可机构应开展业务影响分析，识别关键业务，确定关键业务的恢复时间目标。业务及支撑部门应基于业务影响分析，定义灾难情况下关键服务所需维持的最低水平。	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。
3.2	恢复策略的制	各关键业务和支持部门应分别制定恢复策略，以满足业务影响分析中得出的关键业务恢复时间目标以及关键业务所需维持的最低服务水平。制定恢复策略时应考虑	客户应考虑针对业务影响分析的结果制定恢复策略。为配合客户遵从监管要求，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

编号	控制域	控制要求	华为云的应答
	定	维持关键业务最低服务水平所需的备用场地、人员及工作场所、信息系统、办公设施及重要记录等因素。	统、第三方等各个方面。

7.2 业务连续性计划的开发

《TM-G-2 持续业务运作规划监管政策手册》第四章“业务连续性计划的开发”要求认可机构制定详细的程序和操作指引，用于响应危机事件，确保关键业务中断后可及时恢复。控制要求涵盖危机管理流程、业务和技术恢复、业务连续性模式、重要记录管理、公关和沟通策略等领域。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
4.2	危机管理流程	业务连续性计划中应包括危机管理流程，用于指导突发事件的应对和遏制。高级管理层应识别潜在的危机场景，并制定应对危机场景的危机管理程序。危机管理程序中应包括突发事件的检测和报告流程、危机管理团队对事件进行影响评估的流程、业务连续性计划的启动条件、内外部沟通流程等。	为配合客户遵从监管要求，华为云根据内部业务连续性管理体系的要求，定期开展风险评估，识别并分析支撑云服务持续运行的关键资源所面临的潜在风险。针对突出风险，进一步考虑突发事件发生的场景，并制定应对各种突发事件场景的危机管理程序，以最大程度地降低突发事件的影响。危机管理程序中详细规定了突发事件的预警和报告流程、事件升级流程、应急预案启动的条件、事件进展的通报流程、内外部沟通流程等。
4.4	技术恢复	应关注关键技术设施的韧性，如不间断电源供应器及冷却系统等，对这些设施进行持续监察，并定期维修与测试。 同时，应指派适当的人员负责技术恢复，并为关键恢复人员指定后备人员。	华为云基础设施具备高可用性，同时华为云内部制定了完善的流程，确保对基础设施的运行状况进行持续监控、定期维修、定期测试，将系统故障给客户带来的影响降到最低。华为云基础设施具备高可用性，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，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从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。 此外，华为云针对支撑云服务的重要岗

编号	控制域	控制要求	华为云的应答
			位设置了一岗多人、岗位互备的机制。
4.5	业务连续性模式	认可机构可采取不同的业务连续性模式应对业务出现长时间中断的情况，如传统的“常用/备用” 模式，即设立常用运作场地，并为常用运作场地设立相应的备用场地；或新型的“业务分割”模式，即建立两个或两个以上的常用业务运作场地，互相提供后备支持。每个场地都有能力在一段时间内承担另一个场地的部分或全部工作。	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，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从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。 同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。
4.6	重要记录管理	重要记录的副本生成后应尽快储存在运作场地以外的地点。重要记录的备份必须易于存取，且备份记录需具备充分的访问控制，以确保其可用性。 对于某些关键服务，应考虑是否需要实时进行数据备份（例如采用实时数据镜像技术），以确保系统及数据的快速复原。	华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用对象存储服务的版本控制、云硬盘备份、云服务器备份等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云。 通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。 此外，为了减小由硬件故障、自然灾害或其他灾难带来的服务中断，华为云为所有数据中心提供灾难恢复计划： • 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。
4.7	公关和沟通策略	认可机构应制定与外部相关方的沟通策略，定义在灾难发生时需要联络的各方。与外部相关方的重要对话应妥善记录，外部相关方的重要联络电话和联络地址应妥善	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。

编号	控制域	控制要求	华为云的应答
		保存。	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。

7.3 业务和技术恢复的备用场地

《TM-G-2 持续业务运作规划监管政策手册》第五章“业务和技术恢复的备用场地”对灾难恢复的备用场地提出了具体要求，用以保证备用场地在突发事件场景下可承接关键业务。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
5.1	备用场地的选择标准	备用场地应与常用场地保持足够的距离，以免受同一灾难事故的影响。 此外，备用场地应易于达到，并于业务连续性计划注明的时限内随时可供使用。如果业务连续性计划有所要求，备用场地应预安装工作站、电力、电话及通风设备，以及具备足够的空间。同时，应实施适当的物理访问控制，如配备访问控制系统、保安等。	客户可通过两地互为灾备中心，如一地出现故障，系统在遵从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。华为云在数据中心选址时，确保不同的数据中心保持足够的距离，避免受到同一威胁的影响。同时，选址上保证了数据中心正常运营需要的配套资源，如市电、水、通信线路等。 华为云运维运营团队严格执行访问控制、安保措施、例行监控审计等措施，以确保华为云数据中心的物理安全。数据中心物理安全的详细信息可参见《华为云安全白皮书》。
5.2	技术恢复备用场地	后备数据中心应配备足够的 IT 设备（如工作站、服务器、打印机等），有关设备的型号、规模及容量应达到认可机构的业务连续性计划注明的恢复要求。后备数据中心也应有足够的电信设施（包括网络带宽）及预安装的网络连接。	华为云多个地域内或同一地域内多个可用区都处于运营状态，可互为灾备中心，支持在可用区之间灵活替换计算实例和存储数据。 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。
5.3	供应商或其它机构提供	认可机构应在与供应商的合约条款中规定供应商提供备用设施、技术支持或硬件的所需时间及容量。供应商应	华为云基础设施具备高可用性，华为云的数据中心依托多地域（Region）多可用区（AZ）的架构可实现数据中心本身的容灾，同时同一地域不同可用区互为灾备中心，如一地出现故障，系统在

编号	控制域	控制要求	华为云的应答
	的备用场地	能证明其本身的恢复能力。	遵从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。客户若出于业务需求需考虑灾备，需要基于多个可用区进行应用的分布式部署或选择灾备复制服务，华为云可提供相关的协助。同时，华为云《云服务等级协议》中承诺了华为云各产品和服务需达到的服务水平，其中包括了服务可用率承诺，华为云将严格按照协议的要求。同时，华为云也提供线下合同模板，若客户在容灾备份方面有特殊需求，华为云可根据客户的需求，在双方达成一致的情况下，加入关于容灾备份的特殊条款。

7.4 业务连续性计划的实施

《TM-G-2 持续业务运作规划监管政策手册》第六章“业务连续性计划的实施”要求认可机构定期对业务连续性计划进行测试及维护，确保其有效性。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
6.1	测试和演练	认可机构应至少每年对业务连续性计划进行一次测试。 主要恢复人员和后备恢复人员均需参与测试，以熟悉各自的职责。 测试的范围应全面，以涵盖业务连续性计划的主要部分，并引入重要相关方进行协调与沟通。 应有正式的测试文件，包括测试计划、测试程序、测试结果等。测试完成后，适当地更新计划或恢复策略。	华为云作为客户的供应商，会积极配合客户发起的测试需求，协助客户测试其业务连续性计划的有效性。 同时，华为云根据内部业务连续性管理体系的要求，每年对业务连续性计划和灾难恢复计划进行测试，所有的应急响应人员，包括后备人员均需参与。测试的类型包括桌面演练、功能演练和全面演练三种，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，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。
6.2	定期	各业务和支持部门应至少	客户应考虑至少每年对业务连续性计划

	维护	每年对其业务影响分析和恢复策略进行更新。 关键人员、同行、客户及服务供应商的联系信息应及时更新。 业务连续性计划文件副本应储存在主要场地以外的地点。在紧急情况下采取的主要步骤概要应提供给高级管理层及其他主要人员，并由他们保存在多个不同地点。	进行更新，并考虑业务连续性计划副本的可用性。为配合客户遵从监管要求，华为云根据内部业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。 业务连续性计划、突发事件应急预案、灾难恢复操作手册等文件通过电子和纸质的方式保留多个副本，并分发给相应的管理层及其他主要人员。

8 华为云如何遵从及协助客户满足《虚拟银行的认可指引》的要求

金管局于 2018 年 2 月 6 日发布《虚拟银行的认可指引》，并在完成公众咨询后，于 2018 年 5 月 30 日发布了《虚拟银行的认可指引》的修订指引。在该指引中，金管局表示，虚拟银行的发展将推动香港金融科技的应用和创新，提供新型的客户体验，并促进普及金融，因此金管局欢迎在香港设立虚拟银行，开放科技公司等非金融机构的申请。

同时，指引列出了申请设立虚拟银行的公司须遵守的主要要求，这些要求包括了所有权结构、持续监管、实体办事处、业务计划、技术风险、外包安排等方面。其中，在技术风险方面，指引强调申请虚拟银行的公司（虚拟银行申请人）应尤为关注信息安全、系统韧性及业务连续性这三个方面的技术风险，并采取符合业务需求的安全和技术控制措施。在外包安排方面，指引表明，外包安排必须得到有效批准，并须遵守《SA-2 外包监管政策手册》及其它相关要求。

下表将总结华为云作为云服务供应商，将如何协助虚拟银行申请人满足该指引在技术风险和外包安排方面提出的要求。

控制域	具体控制要求	华为云的应答
技术风险	虚拟银行申请人应关注信息安全、系统韧性、业务连续性方面的风险，并采取符合业务需求的安全和技术控制措施。	**信息安全：**华为云在保障云平台安全的同时，亦为客户云上数据生命周期的各阶段提供了层层防护措施，并通过友好的操作界面和接口，方便客户使用与集成，满足不同行业客户对数据安全的个性化需求。详细信息可参见《华为云数据安全白皮书》。 **系统韧性：**华为云基础设施具备高可用性，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，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从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。详细信息可参见《华为云安全白皮书》8.4 业务连续性与灾难恢复。 **业务连续性：**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

控制域	具体控制要求	华为云的应答
		系。在该体系框架下，定期进行业务影响分析和风险评估，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。
技术风险	申请人须委托有资质的独立专家对其计算机硬件、系统、安全、流程和控制出具独立评估报告	针对客户委托的专家评估，华为云可提供专人协助，积极响应及配合客户方发起的审计活动。同时，华为云每年也会定期接受专业第三方审计机构的审核，并获取审计报告。
外包安排	外包安排必须得到有效批准，并须遵守《SA-2 外包监管政策手册》，以及《个人资料（私隐）条例》和普通法下的客户保密规定。同时，外包活动中须保护客户数据的机密性和完整性。	华为云可协助客户满足外包安排方面的要求： • 本文第六章“华为云如何符合《SA-2 外包监管政策手册》”详细阐述了华为云如何协助金融机构满足 SA-2 的要求。 • 本文第九章“华为云如何符合《客户数据保护通告》的要求”详细阐述了华为云如何协助金融机构保护其客户数据。

9 华为云如何遵从及协助客户满足《客户数据保护通告》的要求

《客户数据保护通告》向认可机构阐述保护其客户数据机密性的重要性，并就如何保护客户数据提供了实施指引。

以下内容将总结通告中与云服务供应商相关的控制要求，并详细阐述华为云作为认可机构的云服务供应商时，会如何帮助认可机构满足这些控制要求。

编号	控制域	具体控制要求	华为云的应答
B	数据安全政策和意识	认可机构应制定客户数据保护的政策和程序。如涉及客户个人信息时，政策和程序亦应符合《个人资料(私隐)条例》或私隐专员发出或批准的任何有关实务守则、规则或指引。 此外，认可机构还应制定意识培训计划，向员工宣贯客户数据保护的重要性。	客户应考虑制定相应策略保护其业务中的客户数据，特别针对个人信息的保护。为配合客户遵从监管要求，华为云参照各类法规要求、监管要求、国际或行业标准建立了一套完善的信息安全和隐私保护管理体系，并持续改进。该管理体系在物理安全管控、系统安全、安全意识培训等众多安全领域均有详细的政策和程序。华为云持续践行管理体系的要求，保障客户的业务和数据安全。 华为云制定了完善的安全意识培训计划，在员工入职、在岗、转岗等环节纳入多种形式的安全意识培训，确保员工行为符合所有法律、政策、流程以及华为商业行为准则的要求。此外，华为云建立了严密的安全责任体系，贯彻违规问责机制，并通过意识培训让员工知晓违规行为可能导致的处分。
C	客户数据逻辑访问控制	认可机构应识别驻留在 AIs 网络和系统不同部分的客户数据的位置，并确保在不同层面（如应用程序层面、数据库层面、操作系统层面、网络层	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；云审计服务（CTS）可为客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。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操

编号	控制域	具体控制要求	华为云的应答
		面）实施适当的逻辑访问控制，以防止未经授权访问客户数据和未经授权/错误地向外部方传输客户数据。	作，以及华为云系统内部触发的操作。 同时，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。内部运维人员接入华为云管理网络对系统进行集中管理时，需采用双因子认证进行身份认证，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。 华为云为客户提供基础设施，将基础设施安全视为构筑多维全栈的云安全防护体系的核心组成部分，在物理环境、网络、平台、应用程序接口、数据等主要方面提供了多层次的安全防护。更多信息详见《华为云安全白皮书》中“5 基础设施安全”部分。
E	客户数据存储管控	认可机构应实施有效的控制措施，及时发现对客户数据的异常下载活动。例如，对将数据下载至存储媒介的活动进行记录，并定期对客户数据是否未经授权下载进行抽样检查。 如果介质(包括纸质和电子介质)中存储客户数据，认可机构应建立安全处理和销毁客户数据的机制。	华为云恪守“不碰数据”底线，客户对其内容数据拥有完全控制权。为防止内容数据被异常下载，针对不同的产品和服务，客户可使用不同的方式进行审计，检测异常活动。如对于对象存储、文件存储等服务，客户可以使用云审计服务来记录用户对数据的操作。对于关系型数据库服务，客户可以使用数据库安全服务来进行数据库列级的管理和访问活动记录。 在客户终止使用华为云服务，需要对内容数据进行销毁时，华为云会对指定的数据及其所有副本进行全面的清除。当客户确认删除操作后，华为云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。
G	与客户数据相关的物理安全管控	认可机构应识别其客户数据存储或可被访问的场所，并确保这些场所具备充分的物理安全管控，以防止数据被窃取或未授权访问。在对系统、设备、记录或其它资产进行搬迁时，在搬迁过程中应具备	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保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。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

编号	控制域	具体控制要求	华为云的应答
		充分的物理安全管控。在完成搬迁后，应尽快进行充分的核对或库存检查，以确保在运输过程中不会丢失客户数据。 认可机构应对处理或能访问大量敏感客户数据的场所或服务商进行管控。	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。
I	对服务供应商的其它管控	认可机构需通过公网向服务供应商传输客户数据时，应实施数据强加密措施，以保护客户数据在传输过程中的安全。	客户可以使用华为云提供的**虚拟专用网络（Virtual Private Network，简称 VPN）**、**云专线（Direct Connect，简称 DC）**、**云连接（Cloud Connect，简称 CC）**等服务，实现不同区域之间业务的互联互通和数据传输安全。其中，VPN 服务采用华为公司专业设备，基于 IKE 和 IPsec 协议在 Internet 网络上虚拟出私有网络，在本地数据中心和华为云 VPC 之间、华为云不同区域的 VPC 之间构建安全可靠的加密传输通道。云专线服务基于运营商多种类型的专线网络，在本地数据中心与华为云 VPC 之间构建专享的加密传输通道，各客户专线之间物理隔离，满足更高的安全性、稳定性要求。云连接服务能够快速在多个本地数据中心与多个云上 VPC 之间建立私有通信网络，支持跨云 VPC 的互连，大大提升了客户业务向全球拓展的安全性和速度。

10 华为云如何遵从及协助客户满足《事件响应与管理程序通告》的要求

《事件响应与管理程序通告》提醒认可机构必须具备重大事件响应与管理能力及程序，并列出认可机构就重大事件与公众沟通时应遵循的原则，为认可机构管理重大事件提供了指引。

以下内容将总结通告中与云服务供应商相关的控制要求，并详细阐述华为云作为认可机构的云服务供应商时，会如何帮助认可机构满足这些控制要求。

控制域	控制要求	华为云的应答
快速事件响应	认可机构应及时分析事件的原因，并在切实可行的范围内尽快纠正或控制问题。首要任务应该是保护已经或可能受事件影响的客户的利益。	为配合客户满足事件快速响应的要求，华为云内部制定了完善的事件管理流程，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处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。
通知客户	事件发生后，认可机构应尽快判断事件是否会影响到其他客户或其它认可机构的客户，并主动通过最有效的途径通知已受影响或可能会受影响的客户，并告诉他们需要采取的步骤或预防措施，以及银行是否会赔偿他们所蒙受的损失及申请赔偿的方法。如有需要，认可机构也应尽快通知其他受影响的认可机构（以便认可机构能通知其受影响客户）。	为配合客户满足事件后通知的要求，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。
公告	除了单独通知客户之外，在情况严重时，认可机构应考虑发布公告。公告的内容应包括事件的关	根据内部的客户通知通报流程，在底层基础平台发生严重事件，已经或可能对大量客户造成严重影响时，华为云可通

控制域	控制要求	华为云的应答
	键要素，以及受影响客户应采取的措施。	过公告在最快的时间内将事件的相关信息通知客户。通知的内容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。
对金管局报告事件	一旦意识到发生了重大事件后，认可机构应立即通知香港金管局，并向其提供当时可获得的任何信息。为免生疑问，认可机构不应等到问题得到纠正后才向香港金管局报告事件。香港金管局可能要求有关认可机构提供进一步的信息或更新。	为配合客户满足重大事件上报 HKMA 的要求，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。
应对客户和媒体的询问	认可机构应确保其职员时刻提高警觉，注意检测及向高级管理层报告重大事故的重要性。认可机构应确保其具备适当的事故应变及管理能力。	为配合客户满足事件应变管理的要求，华为云的事件管理程序中定义了事件报告的职责和程序。此外，华为云联动分析各安全设备的告警信息，结合机器学习技术和专家经验构建相应的模型，检测未知数据安全风险，并及时采取有效措施进行防御及响应。

11 华为云如何遵从及协助客户满足《云计算指南》的要求

《云计算指南》明确了金管局对于采用云计算的认可机构在监管方面的期望，并为此类认可机构如何管理云计算可能带来的相关风险提供了实施指引。

以下内容将总结通告中与云服务供应商相关的控制要求，并详细阐述华为云作为认可机构的云服务供应商时，会如何帮助认可机构满足这些控制要求。

编号	控制域	控制要求	华为云的应答
2	治理框架	认可机构应当建立适当流程，在选择云服务供应商前以及定期，通过第三方独立评估或审计等方式，对云服务供应商开展尽职调查。需从以下方面对云服务供应商进行评估： 1. 财务情况； 2. 声誉； 3. 管理能力； 4. 技术能力； 5. 运营能力； 6. 与认可机构的企业文化和未来发展策略的配合程度； 7. 对银行业的熟悉程度； 8. 紧贴市场创新步伐的能力等。	**a.财务状况**：华为云是华为的云服务品牌，自 2017 年正式上线以来，华为云一直处于快速发展中，收入保持强劲增长态势。全球权威咨询机构 IDC 发布的《2019 年 Q1 中国公有云服务市场跟踪报告》显示，从 IaaS+PaaS 整体市场份额来看华为云营收增长超过 300%，华为云 PaaS 市场份额增速接近 700%，在 Top5 厂商增速排名第一，位居中国公有云服务商第一阵营。 **b.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。 **c.管理能力**：华为云继承了华为公司的风险管理能力，建立了完善的风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不

编号	控制域	控制要求	华为云的应答
			确定市场中有效控制风险，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。 **d.技术能力：**华为云用在线提供云服务的方式，将华为 30 多年在 ICT 基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在 AI 领域，华为云 AI 已在城市、制造、物流、互联网、医疗、园区等 10 大行业的 300+个项目进行落地。在多元架构方面，华为云打造了基于 X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 **e.运营能力：**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。 **f.与认可机构的企业文化和未来发展策略的匹配程度：**华为云在产品和服务规划和阶段会根据客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。 **g.对银行业的熟悉程度：**华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。同时，华为云已委托第三方开展独立评估，将华为云的内部管

编号	控制域	控制要求	华为云的应答
			控现状与香港金管局发布的监管指引和公告要求对比，进行差距分析，并确保任何差距项均得到整改。 **h.紧贴市场创新步伐的能力：**自上线以来，华为云一直坚持技术创新，发布了一系列业界领先的新品和升级，覆盖云安全、DevOps、云容器引擎和微服务引擎、服务网格、计算、云存储、网络、云容灾等多个领域，让产品始终保持先进性。
3	持续的风险管理和控制	认可机构应了解其在与云服务供应商签订的协议下的角色和责任，并制定相应控制措施，以确保有效履行其职责。	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，以及客户和华为云的安全职责。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。
4		认可机构应制定全面的风险管理流程，使认可机构能够持续识别、监控和减轻云计算所带来的风险。	客户对华为云的审计和监督权益会根据实际情况在与金融机构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。
5		认可机构应通过有效控制措施，保护其信息资产的安全性，并遵守关于客户数据保密的相关法律要求。这些控制措施应包括： 1.充分的身份和访问管理控制； 2.清晰有效的密钥管理政策、流程和标准； 3.确保正确的安全配置和网络卫生； 4.有效的网络事件响应和恢复管理流程； 5.确保云服务供应商充分解	1.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。 同时，为配合遵从监管要求，

编号	控制域	控制要求	华为云的应答
		决与多租户云架构相关的安全和运营风险。	华为云还做到： ● 对于运维人员实行基于角色的访问控制，限定不同岗位不同职责的人员只能对所授权的运维目标进行特定操作，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仅需要经过多级的评审和批准。 ● 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。运维人员首先通过双因子认证接入运维环境，再集中从堡垒机跳转到目标机进行操作，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。 ● 目标机的口令被堡垒机回收并定期更新，确保运维人员无需也无法获取口令。 2.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。华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。 华为云服务端加密功能还集成了数据加密服务（Data Encryption Workshop，简称DEW）的密钥管理功能，由DEW 进行密钥全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW 采用分层密钥管理机制，方便各层密钥的轮换。通过 DEW 的控制台或 API 进行关联设置，各存储服务加密数据时使用的加密密

编号	控制域	控制要求	华为云的应答
			钥，能够由保存在 DEW 中的客户主密钥进行加密，该客户主密钥又由保存在硬件安全模块 HSM 中的根密钥进行加密，构成了一条完整的安全、可信的密钥链。HSM 经过严格的国际安全认证，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取根密钥。 3.华为云操作系统、系统软件、数据库和服务器的所有配置和设置都制定了明确的安全基线要求。所有产品遵循华为云制定的网络安全红线中基线要求进行网络和系统的配置，确保限制使用不必要的功能。 华为云制定了虚拟化操作系统的安全配置基线，以保证客户使用云服务时的安全性。 4.为配合客户满足事件快速响应的要求，华为云内部制定了完善的事件管理流程，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处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。 为配合客户遵从监管要求，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。 5.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。

编号	控制域	控制要求	华为云的应答
6		认可机构应制定并实施应急计划，定期进行演练和测试，以有效应对云服务中断的突发情况。	华为云制定了完善的突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。
7	保护访问权和其他合法权利	认可机构应采取适当措施，保障其与金管局对于云服务供应商进行审计、检查和监督的权利。	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机构或其指定的代理人对华为云的审计和监督。
8		认可机构应在与云服务供应商签订合同中明确服务类型与服务水平，以及各方的责任和义务等内容，以保护认可机构的利益、风险管理需求以及对监管要求的遵循。	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，以及客户和华为云的安全职责。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。
9	风险管理能力	认可机构应为监督云计算运营的员工提供具有针对性的定期培训，确保其具备安全使用和管理与云计算相关风险所需的知识和技能。	华为云制定了完善的安全意识培训计划，在员工入职、在岗、转岗等环节纳入多种形式的安全意识培训，确保员工行为符合所有法律、政策、流程以及华为商业行为准则的要求。此外，华为云建立了严密的安全责任体系，贯彻违规问责机制，并通过意识培训让员工知晓违规行为可能导致的处分。

12 华为云如何遵从及协助客户满足《TM-E-1 电子银行风险管理》的要求

《TM-E-1 电子银行风险管理》针对认可机构管控电子银行业务可能存在的风险提供了实施指引。

以下内容将总结通告中与云服务供应商相关的控制要求，并详细阐述华为云作为认可机构的云服务供应商时，会如何帮助认可机构满足这些控制要求。

12.1 电子银行风险治理

《TM-E-1 电子银行风险管理》第三章“电子银行风险治理”针对与电子银行业务有关的风险，提出认可机构在治理层面应考虑实施的管控要求，以保护认可机构开展的电子银行业务的安全性。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
3.3	独立评估和渗透测试	认可机构应制定和实施独立评估相关制度与流程，由具备专业知识与独立性的评估员开展评估并按照相关要求编制评估报告，以验证电子银行业务是否符合监管要求，以及针对相关业务是否已实施了充分的风险管控措施。 认可机构应确保由合格的独立方针对相关业务定期（至少每年一次）开展渗透测试。 认可机构应确保由具备专业知识的人员针对相关业务定期（至少每年一次）或在发生重大变化时进行风险评估。	华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。同时，华为云已委托第三方开展独立评估，将华为云的内部管控现状与香港金管局发布的监管指引和公告要求对比，进行差距分析，并确保任何差距项均得到整改。 针对客户委托的专家评估，华为云可提供专人协助，积极响应及配合客户方发起的审计活动。同时，华为云每年也会定期接受专业第三方审计机构的审核，并获取审计报告。 为配合客户满足合规要求，华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性，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。

编号	控制域	控制要求	华为云的应答
			华为云遵从华为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适用的法律法规、标准发生重大变化时，华为云会进行相应风险评估。

12.2 互联网银行的系统及网络安全

《TM-E-1 电子银行风险管理》第五章“互联网银行系统及网络安全”提出了认可机构为保障互联网银行系统的安全与正常运行应当采取的举措。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
5.1	信息的保密性和完整性	认可机构应制定健全的密钥管理措施，采用安全的国际认可的加密算法，定期评估加密控制措施的实施情况并改进，以维护客户信息的保密性。 认可机构应实施充分的控制措施，以维护其互联网银行系统所处理的信息的完整性。	客户在使用加密措施保护数据时，应考虑采用业内认可的加密算法和密钥管理机制。 目前，华为云云硬盘、对象存储、镜像服务和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 华为云服务端加密功能还集成了**数据加密服务（Data Encryption Workshop，简称 DEW）**的密钥管理功能，由 DEW 进行密钥全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW 采用分层密钥管理机制，方便各层密钥的轮换。通过 DEW 的控制台或 API 进行关联设置，各存储服务加密数据时使用的加密密钥，能够由保存在 DEW 中的客户主密钥进行加密，该客户主密钥又由保存在硬件安全模块 HSM 中的根密钥进行加密，构成了一条完整的安全、可信的密钥链。HSM 经过严格的国际安全认证，能够做到防入侵、防篡改，即使是

编号	控制域	控制要求	华为云的应答
			华为运维人员也无法窃取根密钥。 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。
5.2	互联网基础设施	认可机构应建立安全的互联网基础设施，以支持其互联网银行系统。	华为云为客户提供基础设施，将基础设施安全视为构筑多维全栈的云安全防护体系的核心组成部分，在物理环境、网络、平台、应用程序接口、数据等主要方面提供了多层次的安全防护。更多信息详见《华为云安全白皮书》中“5 基础设施安全”部分。
5.3	应用系统安全	认可机构应针对其互联网银行系统（包括任何应用程序）采取适当的控制措施，以使其具备充分的安全性，至少应涵盖应用程序的设计和开发、测试和实施。 认可机构应在启用任何互联网银行系统或进行系统变更前，由具备专业知识的独立的人员进行充分的应用系统源代码审查。	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。 ● 针对各产品，新的研发需求须经过需求分析团队的审批后才能进入开发环节。此外，针对涉及新服务构建的重要研发需求，会执行立项评审。新的产品或服务转公测或正式商用前，华为云会对产品的生产环境进行生产就绪程度评审，以满足业务要求。 ● 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。 ● 华为云引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署工具链，通过

编号	控制域	控制要求	华为云的应答
			质量门限进行控制，以评估云服务产品的质量。 ● 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。 ● 华为云建立了一系列静态代码扫描工具，确保涉及开发的产品变更在上线前经过代码审核验收。华为云建立了正式的内部测试及验收措施，以确保仅适当且经过授权的变更被发布至生产环境。
5.4	威胁监控和漏洞评估	认可机构应建立系统的监控流程，密切监控与其互联网基础设施、应用系统和其他相关系统组件和操作相关的紧急安全威胁。 认可机构应利用自动化工具定期进行漏洞评估，以识别其互联网基础设施和相关互联网银行系统中的安全漏洞。 认可机构应采取有效方法应对已查明的安全威胁或漏洞所带来的风险。	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，同时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。 为配合客户遵从监管要求，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。

12.3 欺诈和事件管理

《TM-E-1 电子银行风险管理》第八章“欺诈和风险管理”要求认可机构制定和实施相关制度和流程以有效响应安全事件。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
8.2	事件响应和定期演习	认可机构应制定和实施有效的事件响应政策和流程，及时报告和处理安全事件。同时，应定期进行事件响应演练，以评估其事件管理策略和流程的有效性 认可机构应制定有效的事件沟通策略。 发生重大事件时，相关认可机构应依据有关规定及时通知金管局。	为配合客户满足事件快速响应的要求，华为云内部制定了完善的事件管理流程，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处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。 为配合客户满足事件后通知的要求，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。 为配合客户满足重大事件上报金管局的要求，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。

12.4 系统可用性和业务连续性管理

《TM-E-1 电子银行风险管理》第九章“系统可用性和业务连续性管理”明确要求认可机构应当采取有效措施，维护电子银行系统的可用性并保障其业务连续性。以下为相关控制要求及华为云的应答：

编号	控制域	控制要求	华为云的应答
9.1	电子银行对客户的服务水平	认可机构应确保与其系统韧性以及容量规划有关的控制措施，覆盖所有相关系统和基础设施组件，以及任何服务供应商的系统和基础设施组件，以保障系统可以持续稳定为客户提供电子银行业务。	华为云基础设施具备高可用性，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，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从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。详细信息可参见《华为云安全白皮书》8.4 业务连续性与灾难恢复。 客户应考虑通过正式的程序来管理系统容量。为配合客户遵从监管要求，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。 同时，华为云的**云监控服务（Cloud Eye）**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。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。
9.2	容量规划	认可机构应定期对相关系统和基础设施的系统容量进行审查，识别任何潜在的可能影响电子银行稳定的弱点吗，并采取必要措施进行纠	客户应考虑通过正式的程序来管理系统容量。为配合客户遵从监管要求，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

编号	控制域	控制要求	华为云的应答
		正。 认可机构应制定容量规划指南与容量规范方法，明确规定系统利用率阀值和相应预防措施，同时帮助预估未来的容量需求。	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。 同时，华为云的**云监控服务（Cloud Eye）**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。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。
9.3	性能监控	认可机构应建立覆盖所有支持电子银行业务的关键系统和基础设施组件的自动性能监控和警报系统，以便在发生异常的情况可以指派专人及时处理。	客户应考虑通过正式的程序来管理系统容量。为配合客户遵从监管要求，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。 同时，华为云的**云监控服务（Cloud Eye）**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。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。
9.4	系统韧性	认可机构应对其系统韧性的实际有效性进行适当的验证和测试，确保不存在单点故障以及对非关键系统的非必要连接与依赖。 认可机构应对服务供应商的系统韧性进行监控，并了解	华为云多个地域内或同一地域内多个可用区都处于运营状态，可互为灾备中心，支持在可用区之间灵活替换计算实例和存储数据。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不同，所有可用区域与多个一

编号	控制域	控制要求	华为云的应答
		其应急计划。	级传输供应商冗余相连，进一步排除单点故障的风险。 华为云制定了完善的突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。 华为云每年定期接受专业第三方审计机构的审计，并可在客户需要时可向其提供相关审计报告。华为云也会安排专人负责客户方发起的尽职调查。
9.5	应对系统中断的控制措施	认可机构应制定并定期演练，以测试相关的 IT 灾难恢复计划和流程的有效性。 认可机构应对可能导致电子银行业务中断的问题采取适当措施进行处置和预防。 认可机构应实施适当措施及时检测和响应 DDoS 攻击等可能导致电子银行系统中断的网络攻击所构成的威胁。这些措施应经过验证并定期审查，以确保其有效性。	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。 华为云根据内部业务连续性管理体系的要求，每年对业务连续性计划和灾难恢复计划进行测试，所有的应急响应人员，包括后备人员均需参与。测试的类型包括桌面演练、功能演练和全面演练三种，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，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。 华为云在网络边界部署 DoS/DDoS 防范清洗层、下代防火墙、入侵防御系统层以及网站应用防火墙层。通过限制虚拟端口的连接跟踪数来抵御来自云平台外部或平台内部其他虚拟机的大流量攻击，此类攻击

编号	控制域	控制要求	华为云的应答
			会产生大量连接跟踪表项，如果不做限制，会耗尽连接跟踪表资源，导致不能接受新的连接请求，最终导致业务及管理流量中断。除此之外，还为客户提供了 Anti-DDoS 流量清洗服务，客户可将 Anti-DDoS 流量清洗设备部署在其数据中心网络出口区域。AntiDDoS 设备通过对互联网访问弹性云服务器、弹性负载均衡和裸金属服务器的业务流量进行实时监测，及时发现异常 DDoS 攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。

13 结语

本文描述了华为云如何为客户提供遵从香港金融行业监管要求的云服务，并表明华为云遵守香港金融管理局（HKMA）发布的重点监管要求，有助于客户详细了解华为云对于中国香港金融行业监管要求方面的遵从性，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香港金融行业监管要求的遵从性。

14 版本历史

日期	版本	描述
2023 年 8 月	1.2	例行刷新
2022 年 4 月	1.1	例行刷新
2019 年 11 月	1.0	首次发布

