

华为云新加坡金融行业监管要求遵从性指南

文档版本

3.0

发布日期

2024-01-26



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI 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	1
2 华为云安全与隐私合规	2
3 华为云安全责任共担模型	5
4 华为云全球基础设施	6
5 华为云如何符合 MAS《外包指南》的要求	7
5.1 与 MAS 在外包的合作	7
5.2 风险管理实践	7
5.3 云计算	11
6 华为云如何符合 MAS《科技风险管理指南》的要求	13
6.1 科技风险治理和监督	13
6.2 科技风险管理框架	15
6.3 IT 项目管理和设计安全	16
6.4 软件应用程序开发与管理	19
6.5 IT 恢复能力	21
6.6 访问控制	24
6.7 数据和基础设施安全	25
7 华为云如何符合 MAS《关于网络卫生的通知》的要求	29
8 华为云如何符合 ABS《外包服务商控制目标和流程指南》的要求	33
8.1 审计和检查	33
8.2 实体级别控制	35
8.3 通用 IT 控制	37
8.4 服务控制	42
9 华为云如何符合 ABS《ABS 云计算实施指南》的要求	44
9.1 尽职调查建议的活动	44
9.2 进入云外包安排时建议的控制措施	46
10 华为云如何符合 MAS《业务连续性管理指南》的要求	56
10.1 关键业务服务和职能	56

10.2 服务恢复时间目标	57
10.3 依赖映射关系	58
10.4 集中风险	60
10.5 持续审视与改进	61
10.6 测试	63
10.7 审计	65
10.8 事件与危机管理	66
11 华为云如何符合 MAS 《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》的要求	69
11.1 共同承担网络安全责任	69
11.2 身份访问管理	70
11.3 保护公有云中的应用程序	73
11.4 数据安全和加密密钥管理	76
11.5 不可变工作负载和基础设施即代码	77
11.6 网络安全运营	78
11.7 云韧性风险管理	79
11.8 云服务提供商的外包尽职调查	80
11.9 供应商锁定和集中风险管理	81
11.10 技能	82
12 结语	83
13 版本历史	84

1 简介

在科技发展的浪潮中，越来越多的金融机构在逐渐寻求业务转型并希望借助先进的技术以降低成本、提升运营效率、实现业务模式的创新。为了规范金融行业对于信息科技的运用，新加坡金融监管局（MAS）以及新加坡银行协会（ABS）发布了一系列监管要求、指南和通知，针对新加坡金融机构科技风险管理、科技外包管理以及云计算实施等方面提出了相关监管要求。

华为云作为云服务供应商，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符合金融行业标准要求的云服务及业务运行环境。为此，华为云目前已建立起一套涵盖业界主流云安全标准以及华为云安全管理要求的方法体系，覆盖了网络安全与隐私保护领域中多个方面的要求，其实施有助于提升华为云自身合规水平，同时能够协助金融客户满足相关监管要求、指南和通知。

本文将针对新加坡金融机构在使用云服务时通常需遵循的以下监管要求和指南，详细阐述华为云将如何协助其满足监管要求：

- **MAS 外包指南：**针对已经或计划将业务活动外包给服务供应商的金融机构，提出了希望金融机构能够遵守的外包管理相关要求，为金融机构外包活动的风险管理提供了良好实践指导。
- **MAS 科技风险管理指南：**规定了科技风险管理原则和最佳实践标准，指导金融机构建立健全、可靠的科技风险管理框架。
- **MAS 关于网络卫生的通知：**为新加坡金融机构提供了关于遵循相关法令的实践指导。
- **ABS 外包服务商控制目标和流程指南：**规定了为金融机构提供服务的外包服务供应商应具备的最低/基线控制措施。
- **ABS 云计算实施指南：**为金融机构提供了关于使用云服务的最佳实践和注意事项。
- **MAS 业务连续性管理指南：**为新加坡金融机构加强业务连续性管理提供指导，旨在帮助金融机构增强抵御服务中断的能力，同时最大限度地减少服务中断所造成的负面影响。
- **MAS 针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见：**强调了金融机构在采用公有云服务前应考虑的一些常见的关键风险和控制措施。为金融机构更加安全地使用公有云服务，降低相关风险提供指导。

2 华为云安全与隐私合规

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

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

华为云部分标准类认证/鉴证示例：

认证	描述
ISO27001:2022	ISO27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理系统的持续运行。
ISO27017:2015	ISO27017 是针对云计算信息安全的国际认证。ISO27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO27018:2019	ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。 ⁷
TL 9000& ISO 9001	ISO 9001 是 ISO 9000 族标准所包括的一组质量管理体系核心标准之一，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。 TL 9000 是一个建立在 ISO9001 基础上的，由全球电信业优质供应商联盟（QuEST Forum）针对全球信息和通讯技术（ICT）行业特定设计的、为 ICT 产品和服务供方提供的一套通用的质量管理体系要求。它包括了 ISO9001 的所有要求，ISO9001 将来的任何改动也会导致 TL9000 的改动。 华为云取得了 ISO9001 / TL9000 认证证书，表明华为云可以为您提供更快，更好和更具成本效益的服务。
ISO20000-1:2018	ISO20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的 IT 服务来满足客户和业务的需

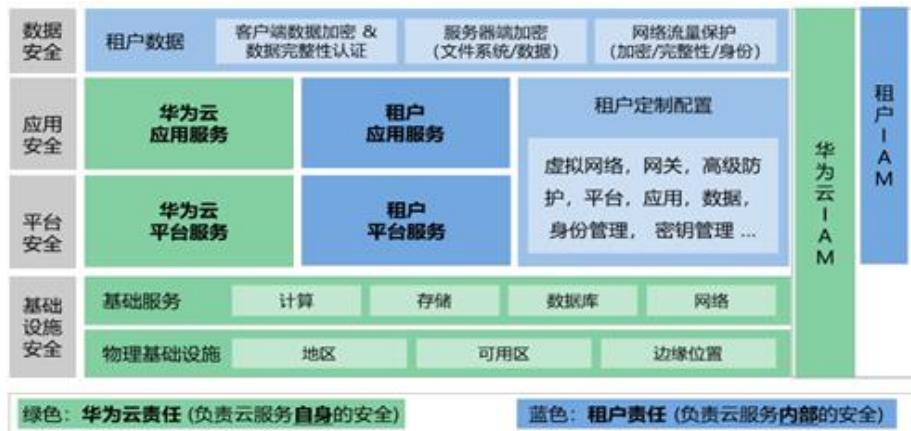
认证	描述
	求。
ISO22301:2019	ISO22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
CSA STAR 认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
ISO27701:2019	ISO27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS10012 是 BSI 发布的个人信息数据管理体系标准，BS10012 认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
ISO 29151:2017	ISO29151 是国际个人身份信息保护实践指南。ISO29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
PCI DSS	支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
PCI 3DS	PCI 3DS 标准，旨在保护执行特定 3DS 功能或者存储 3DS 数据的 3DS 环境，支持 3DS 的实施。PCI 3DS 的评估对象为 3D 协议执行环境，包括访问控制服务器、目录服务器或 3DS 服务器功能；以及 3D 执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估 3D 协议执行环境的过程、流程、人员管理等。
ISO 27799:2016	ISO/IEC 27799 是专注于医疗行业的信息安全管理标准，为医疗行业及其相关机构提供了关于如何更好地保护个人健康信息的保密性、完整性、可审计性和可用性的指导。 华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。
ISO 27034	ISO/IEC 27034 是国际标准化组织 ISO 通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得 ISO/IEC 27034 认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。

认证	描述
SOC 审计报告	SOC 审计报告是由第三方审计机构根据美国注册会计师协会 (AICPA) 制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。

3 华为云安全责任共担模型

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

华为云如何符合 MAS《外包指南》的要求

《外包指南》从风险管理的角度阐述了金融机构在进行业务外包时需要考虑的事项及应遵守的要求。MAS 外包指南涵盖与 MAS 在外包、风险管理实践和云计算方面的合作，表达了新加坡金融管理局对金融机构外包管理方面的期望。

以下内容将总结该指南中与云服务供应商相关的控制要求，并详细阐述了华为云作为金融机构的云服务供应商时，会如何帮助其满足这些控制要求。

5.1 与 MAS 在外包的合作

《外包指南》第四章要求金融机构持续向 MAS 证明其遵守这些准则，覆盖遵守指南和不良发展通知。相关控制要求及华为云应答如下：

编号	控制域	具体控制要求	华为云的应答
4.1	遵守准则	一个机构应准备好向 MAS 证明其遵守这些准则。MAS 可直接与该机构的所在地或东道监管机构以及该机构的服务提供商沟通，说明它们是否有能力和意愿与 MAS 合作监督该机构的外包风险。	客户应定期对其外包服务提供商进行审计或评估，确保服务提供商提供的云服务不低于自身安全管理要求。
4.2	不良发展通知		如果金融机构向华为云发起审计请求，华为云将安排人员积极配合审计。

5.2 风险管理实践

《外包指南》第五章要求金融机构就外包安排制定风险管理政策并遵守外包风险管理相关实践，覆盖概述、董事会和高级管理层的责任、风险评估、服务提供商评估、外包协议、保密和安全、业务连续性管理、外包安排的监控和控制、审计和检查、新加坡境外外包、集团内外包以及将内部审计外包给外部审计方等领域。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
5.3	风险评估	<p>为了确保外包安排不会导致机构的风险管理、内部控制、商业行为或机构声誉受到损害或削弱，机构应建立风险评估框架。此类风险评估应在机构计划与现有或新的服务供应商签订外包安排时进行，并定期对现有外包安排进行重新评估，作为机构外包安排的批准、战略规划、风险管理或内部控制审查的一部分。</p>	<p>客户应建立风险评估框架，定期评估外包安排的风险。华为云可配合并积极响应客户需求。此外，华为云内部也制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。</p>
5.4	服务供应商评估	<p>在考虑重新谈判或更新外包安排时，机构应对服务供应商进行适当的尽职调查，以评估与外包安排相关的风险。必要时，金融机构应对服务供应商进行现场考察，并尽可能获得服务供应商的独立审查和市场反馈，以补充机构的评估。机构还应确保其外包服务供应商的雇员均经过评估，以满足机构自身的聘用标准。</p>	<p>客户应对其服务供应商进行尽职调查，以识别其外包安排的风险。华为云会安排专人积极配合金融机构的尽职调查。为了让用户享受安全可信的云平台和云服务，华为云按照全球各地权威的安全标准，从安全技术、安全制度、人员管理等各方面构建了完备的安全体系，并获得了国内外众多安全认证。华为在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。并贯穿在华为云招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。</p>
5.5	外包协议	<p>机构与外包服务供应商应书面定义合同条款和条件以约束双方的关系、义务、责任、权力和期望。合同应由主管当局（如法律顾问）审查其合法性和适宜性。机构应确保每个外包协议都能解决风险评估和尽职调查阶段发现的风险。每项外包协议都应允许重新谈判和续期，以使该机构能够对外包安排保持适当程度的控制，并有权采取适当措施进行干预，以履行其法律义务和监管义务。每项协议都应量身定制，以解决国家风险引起的问题以及对新加坡境外服务供应商就外包安排进行监督和管理时可能遇到的</p>	<p>客户与外包服务供应商应签订外包协议，并保证协议的合法性和适宜性。为配合客户行使对云服务供应商的监管，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，在其中与客户共同约定相应要求。更多详细信息请参见《华为云用户协议》。</p>

编号	控制域	具体控制要求	华为云的应答
		障碍。	
5.6	保密和安全	金融机构必须确保服务供应商的安全政策、程序和控制措施将使机构能够保护其客户信息的保密性和安全性。	<p>客户可以采取协议约束、审查监督等方式确保服务供应商的安全政策、程序和控制措施将使机构能够保护其客户信息的保密性和安全性。</p> <p>华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户所在国家或地区的安全法规以及行业监管要求的基础上，参考业界最佳实践从组织、流程、规范、技术、合规、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足客户的安全需求。同时，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专家报告。更多详细信息请参见《华为云安全白皮书》。</p>
5.7	业务连续性管理	金融机构应确保其业务连续性不会因外包安排而受损，以便在服务中断或失败、外包安排意外终止或服务供应商清算的情况下，机构仍能够以诚信的方式有能力开展业务。	<p>客户应制定业务连续性计划，并考虑其外包安排对其业务连续性的影响。如果金融机构在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。</p> <p>此外，华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。</p>

编号	控制域	具体控制要求	华为云的应答
5.8	外包安排的监控	<p>金融机构应建立外包管理控制小组，持续监控外包服务。对所有重大外包安排进行定期审查，对新的外包安排或对现有外包安排进行修订时，进行全面的实施前和实施后审查。如果外包安排有重大修改，还应对外包安排进行全面的尽职调查。</p>	<p>客户应该建立外包管理机制，持续监控并定期审查外包服务。华为云的云监控服务（Cloud Eye）可实现对客户自身云资源的使用情况和绩效的监控。华为云可以根据客户的需求按照 SLA 向客户提供服务报告，华为云也会安排专人负责客户方发起的尽职调查。</p>
5.9	审计和检查	<p>金融机构的外包安排不应干扰其自身管理能力和金融监管局的监督能力，也不应妨碍金融监管局履行其监督职能和目标。机构应确保对其所有外包安排进行独立审计和/或专家评估。</p> <p>外包协议还应包括要求服务供应商尽快满足金融监管局或机构向服务供应商及其分包商提出的任何要求的条款，以提交与外包安排相关的服务供应商及其分包商的安全和控制环境报告。重大问题和担忧应及时提请机构和服务供应商的高级管理层或机构董事会注意（如有必要）。如果构成的风险不再在机构的风险承受能力范围内，机构应采取行动审查外包安排。</p>	<p>客户应定期对其外包服务供应商执行独立审计或专家评估，并将识别的问题知会服务供应商的高级管理层。客户应该在与服务供应商签订的协议中要求包含服务供应商对其分包商的安全承诺。</p> <p>华为云会安排专人积极配合客户发起的审计要求。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过 ISO27001、ISO27017、ISO27018、SOC、CSA STAR 等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。此外，华为云制定了完善的供应商管理机制，定期对供应商（包括外包人员）的表现进行考核，考核结果作为下次采购的关键参考。华为云也会与供应商（包括外包人员个人）签订安全合规和保密协议。</p>
5.10	新加坡境外外包	<p>金融机构在外国聘用外包服务供应商可能会面临国家风险，因此在外包安排的风险管理中，尽职调查应包括政府政策、政经状况、外国的法律监管发展以及机构有效监测供应商的能力。机构还应了解外包供应商的恢复安排和地点并考虑传输媒介的相关风险。机构应仅与处于能够遵守保密条款的司法管辖区内以及法律和行政限制不会妨碍机构获取信</p>	<p>客户在选择外包服务供应商时，应提前对其进行尽职调查，保证外包服务供应商的政府政策、经济情况、法律监管以及服务能力符合客户业务发展的需要以及监管要求。</p> <p>华为云会安排专人积极配合客户的尽职调查。此外，华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户所在国家或地区的</p>

编号	控制域	具体控制要求	华为云的应答
		息的服务供应商签订协议。	<p>安全法规以及行业监管要求的基础上，参考业界最佳实践从组织、流程、规范、技术、合规、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足客户的安全需求。</p> <p>华为云在新加坡建立了两个数据中心，实现双可用区冗余。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：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。</p>
5.1 1	集团内外包	对集团内部服务提供者的尽职调查可以采取评估服务提供者应对该机构特有风险能力的定性方面的形式，特别是与业务连续性管理、监测和控制、审计和检查有关的风险，包括确认向 MAS 提供的访问权，保留对该机构的有效监督，以及遵守当地监管标准。	<p>客户在选择服务提供商之前，应对其进行尽职调查。客户审查服务提供商的业务连续性机制是否满足业务要求。客户与服务提供商洽谈，最终与供应商就合同内容达成一致。</p> <p>华为云将安排人员积极配合客户的检查和尽职调查。华为云每年都会聘请专业的外部资源进行 SOC2 认证。如果客户对用户协议提出更多要求，华为云将尝试与其达成协议。华为云将积极配合 MAS 和金融机构对华为云及其供应商的审计。</p>

5.3 云计算

《外包指南》第六章提出了金融机构使用云服务时需要考虑的注意事项及应遵守的相关要求。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	云计算	金融机构在订购云服务时，机构应执行必要的尽职调查，机构应采取积极措施应对与数据访问、保密性、完整性、主权、可恢复性、合规性和审计相关的风险。机构应确保服务供应商拥有使用强有力的物理或逻辑控制来明确识别和隔离客户数据的能力。服务供应商应建立可靠的访问控制来保护客户信息，此类访问控制应在云服务合同有效期内存续。	客户在订购云服务前，应对云服务供应商进行尽职调查，特别是了解云服务在实现数据访问、保密性、主权、可恢复性、合规性方面的控制措施，以及多租户场景下如何实现客户数据隔离的解决方案。 华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证与访问控制、权限管理、数据隔离、传输安全、存储安全、数据删除、物理销毁、数据备份恢复等方面，采用优秀技术、实践和流程，保证用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。更多详细信息请参见《华为云数据安全白皮书》第4部分。

6

华为云如何符合 MAS《科技风险管理指南》的要求

新加坡金融管理局（MAS）发布的《2021 科技风险管理指南》规定了金融机构关于科技风险的管理原则和最佳实践标准，以指导新加坡金融机构建立一个健全的、可靠的科技风险管理框架，加强系统的安全性、可靠性、弹性和可恢复性，保护客户数据、交易及信息系统。《2021 科技风险管理指南》的要求覆盖了科技风险管理框架、IT 项目管理和设计安全、软件应用程序开发和管理、IT 服务管理、IT 弹性、访问控制、密码学、数据和基础设施安全、网络安全运营、网络安全评估、在线金融服务和 IT 审计等领域。

以下内容总结了《2021 科技风险管理指南》中与云服务供应商相关的合规要求条款，并阐述华为云是如何帮助金融机构满足其要求。

6.1 科技风险管理

鉴于 IT 职能在支持金融机构业务方面的重要性，《2021 科技风险管理指南》第三章要求金融机构的董事会和高级管理层监督其科技风险，并确保组织的 IT 职能能够支持其业务战略和目标。相关要求覆盖董事会和高级管理层的作用、政策、标准和程序、信息资产管理、第三方服务管理、能力和背景审查以及安全意识和培训。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
3.2	政策、标准和程序	应基于行业标准和最佳做法，制定政策、标准和程序，并以此来管理科技风险和保护信息资产。应定期审查和更新政策、标准和程序，以确保其仍然与不断变化的科技和网络威胁格局相关。	客户应建立并定期审查正式的信息安全政策和流程。 根据 ISO 27001 标准，华为云构建了完善的信息安全管理体系，制定了华为云的整体信息安全战略，明确了信息安全管理机构的结构和职责、信息安全管理文件的管理办法、关键方向和目标，包括资产安全、访问控制、密码学、物理安全、运营安全、通信安全、系统开

			发安全、供应商管理、信息安全事件管理和业务连续性。华为云全力保护客户系统和数据的不可侵犯性、完整性和可用性。此外，华为云专注于培养员工和外包人员的安全意识，并制定了适用的安全意识培训计划，定期进行培训。
3. 3	信息资产管理	为了准确、完整地了解其 IT 运营环境，金融机构应建立信息资产管理实践。应维护、定期审查所有信息资产的清单，并在发生更改时更新清单。	客户应对其信息资产进行统一管理，明确相应资产的分类和数据存储的物理位置（国家或地区），并识别相应国家或地区发布的数据保留和信息安全要求。 华为云为客户提供统一的管理界面，以供客户查询和管理已购买的华为云资源。客户还可以使用华为云主机安全服务（HSS）的资产管理功能，对其资产进行统一管理。
3. 4	第三方服务管理	在签订合同协议或伙伴关系之前，金融机构应评估和管理其面临的技术风险，这些风险可能影响第三方 IT 系统和数据的机密性、完整性和可用性。	客户在选择服务提供商之前应进行尽职调查，特别是在治理、风险和合规管理方面的机制。客户应制定一份信誉良好的服务提供商列表，并能够确定是否有任何可行的替代首选服务提供商。 华为云提供在线版本的《华为云服务等级协议》，明确了提供的服务的内容和级别，以及华为云的职责。华为云会安排专人积极配合金融机构的尽职调查。客户以及其监管机构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约定。华为云已获得 ISO27001、ISO 27017、ISO 27018、SOC、CSA STAR 等国际安全和隐私保护认证，并每年接受第三方审计。
3. 5	能力与背景审查	由于人们在 IT 环境中管理系统和流程中发挥着重要作用，金融机构应实施全面有效的筛选流程。	客户应制定和实施人员筛选策略和程序。 华为云在招聘员工前进行了充分的背景调查，包括犯罪记录、财务违规、不诚实记录、政府背景、制裁国家经验、是否制裁国家公民。同时，为了有序管理，降低人员管理风险对业务连续性和安全的潜在影响，华为云针对运维工程师等关键岗位实施了专门的人员管理计划，包括入职安全审查、在职安全培训

			与赋能、入职资格管理、离职安全审查。
3.6	安全意识和培训	所有能访问金融机构 IT 资源和 IT 系统的承包商和供应商应制定安全意识培训计划并至少每年执行或更新一次。	为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为云从意识教育普及、宣传活动开展、华为员工商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育，并每年至少执行一次针对全员的安全意识培训。

6.2 科技风险管理框架

《2021 科技风险管理指南》第 4 章要求金融机构建立风险管理框架来管理技术风险，覆盖风险管理框架、风险识别、风险评估、风险处理、风险监控、审查和报告。相关控制要求及华为云应答如下：

编号	控制域	具体控制要求	华为云的应答
4.1	风险管理框架	金融机构应建立风险管理框架来管理科技风险。金融机构应建立适当的治理结构和流程，明确界定角色、责任和清晰的跨部门的报告关系。	客户应建立风险评估框架，定期评估外包安排的风险。 华为云可配合并积极响应客户需求。此外，华为云内部也制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云环境的安全、稳定运行。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法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。
4.2	风险识别	金融机构应识别其 IT 环境的威胁和漏洞应用程序，包括由第三方服务提供商维护或支持的信息资产。对金融	客户应对其外包业务和首选服务提供商进行风险评估，以识别潜在风险。

		机构及其利益相关者产生严重影响的安全威胁示例包括内部破坏、恶意软件和数据盗窃。	华为云开发并维护内部风险管理框架，识别、分析和管理已识别的风险。华为云至少每年进行一次正式风险评估，并制定了风险计算和分类的流程，以确定已识别风险的可能性和影响。每种风险相关的可能性和影响是独立确定的，应考虑每种风险类别。根据风险标准，将风险降低到可接受的水平包括解决时间，都应该由管理层制定、记录和批准。此外，华为云至少每月组织一次会议，讨论网络安全和隐私保护风险评估。华为云采取并记录相应的后续行动，以确保风险按照华为风险管理要求得到适当管理。
4.3	风险评估	金融机构应分析威胁和漏洞对整体业务和运营的潜在影响和后果。金融机构在评估科技风险时，应考虑财务、运营、法律、声誉和监管因素。	
4.4	风险处置	金融机构应制定和实施与信息资产的重要性和风险承受能力水平一致的风险缓解和控制措施。应定期审查和更新 IT 控制和风险缓解方法，同时考虑不断变化的威胁形势和金融机构风险状况的变化。	
4.5	风险监控、审查和报告	金融机构应建立一个评估和监控 IT 控制的设计和运营有效性的流程，以应对已确定的风险。	

6.3 IT 项目管理设计安全

《2021 科技风险管理指南》第 5 章要求金融机构建立项目管理框架，以确保项目管理实践的一致性。相关要求覆盖项目管理框架、项目指导委员会、系统获取、系统开发生命周期和设计安全、系统需求分析、系统设计和实施、系统测试和验收以及质量管理。相关控制要求及华为云应答如下：

编号	控制域	具体控制要求	华为云的应答
5.1	项目管理框架	应建立项目管理框架，以确保项目管理做法的一致性，并提供符合项目目标和要求的成果。应为所有 IT 项目制定详细的 IT 项目计划，其中包括项目范围、活动、里程碑和项目每个阶段要实现的可交付成果。	客户应建立项目管理框架，确保外包项目的交付和实践流程满足其项目目标和要求。对于每个 IT 项目计划，客户应考虑项目范围、活动、里程碑以及每个阶段应交付的内容。 华为云制定了完整的项目管理办法，实施基于 CCM5/CMMI、ISO 9001:2000 和 PMI 框架的实践，使合格的项目管理专业人员在全球成

			功实施项目。
5.3	系统获取	金融机构应制定供应商评估和选择的标准和程序，以确保选定的供应商是合格的，并能够满足其项目要求和交付成果。所执行的评估和尽职调查水平应与项目交付成果对 FI 的重要性相称。	<p>客户在选择服务提供商之前应进行尽职调查，特别是在治理、风险和合规管理机制方面。客户应制定一份信誉良好的服务提供商列表，并能够确定是否有任何可行的替代首选服务提供商。</p> <p>华为云提供在线版本的《华为云服务等级协议》，明确了提供的服务的内容和级别，以及华为云的职责。华为云将派专人积极配合 FI 的尽职调查。客户在华为云的审计和监督权将根据情况在与客户签署的协议中承诺。</p> <p>华为云已获得 ISO27001、ISO 27017、ISO 27018、SOC、CSA STAR 等国际安全和隐私保护认证，并每年接受第三方审计。</p> <p>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。</p> <p>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。</p> <p>商业声誉：华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、</p>

			<p>汽车制造等行业，华为云已实现大突破。在海外市场，华为云香港、俄罗斯、泰国、南非、新加坡大区相继开服。</p> <p>适合金融机构的企业文化和服务政策：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。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。</p>
5.4	系统开发生命周期和设计安全	金融机构应建立一个框架来管理其系统开发生命周期(SDLC)。框架应明确定义生命周期每个阶段的流程、程序和控制，如启动/规划、需求分析、设计、实施、测试和验收。	<p>客户应根据要求建立一个框架来管理其系统开发生命周期(SDLC)。</p> <p>华为云追求新的 DevOps 流程，具有快速持续迭代能力，集成了华为安全开发生命周期(SDL)。此外，逐步形成高度自动化的新安全生命周期管理办法和流程，称为 DevSecOps，与云安全工程能力和工具链一起确保 DevSecOps 的顺利灵活实施。</p> <p>华为云对开发环境进行分层管理，并实施物理隔离、逻辑隔离、访问控制、数据传输通道审批和审计等保护措施。</p>
5.5	系统需求分析	金融机构应确定、定义和记录 IT 系统的功能要求。除了功能要求外，还应建立和记录系统性能、复原力和安全控制等关键要求。	<p>客户应确定、定义和记录 IT 系统的功能要求，覆盖系统性能、弹性和安全控制。</p> <p>华为云根据内部业务连续性管理体系的要求，制定了完善的恢复策略，以支撑云服务持续运营的关键业务。</p> <p>客户可以依赖华为云数据中心集群的区域和可用区架构，实现业务系统的容灾和备份。按规则在全球部署数据中心。</p> <p>客户通过两个地方拥有灾难数据备份中心。如果发生故障，系统会自动从受影响区域传输</p>

			<p>客户应用程序和数据，在满足合规策略的前提下，确保业务连续性。华为云还部署了全球服务器负载均衡中心。客户应用可以在数据中心实现 N+1 部署。即使一个数据中心发生故障，它也可以将流量负载均衡到其他中心。</p> <p>目前，华为云已获得 ISO 27001、ISO 27017、ISO 27018、SOC、CSA STAR 等国际安全和隐私保护认证，并每年接受第三方审计。</p>
5.7	系统测试与验收	应建立系统测试的方法论。测试的范围应包括业务逻辑、系统功能、安全控制和各种负载和压力条件下的系统性能。测试前应制定并批准测试计划。	<p>客户应定期对关键业务进行系统测试和修复，并分析结果。此外，华为云基于漏洞管理系统进行漏洞管理，确保自研和第三方基础设施、平台、应用层、云服务和运维工具的漏洞在 SLA 规定的时间内被发现和修复。这降低了恶意利用漏洞带来的风险和对金融机构业务产生不利影响。对于涉及云平台和金融机构业务的漏洞，华为云将及时向最终用户和金融机构推送漏洞缓解和恢复建议和解决方案，确保主动披露不会造成高攻击风险。华为云将与金融机构一起面临安全漏洞带来的挑战。</p>
5.8	质量管理	质量保证应由独立的质量保证职能执行，以确保项目活动和交付成果符合金融机构的政策、程序和标准。	<p>客户应按照要求进行质量保证。</p> <p>基于 CCM5/CMMI、ISO 9001:2000 和 PMI 框架的实践，华为云制定了完整的项目管理方法，使用合格的项目管理和专业人员在全球成功实施项目。</p>

6.4 软件应用程序开发与管理

《2021 科技风险管理指南》第 6 章要求金融机构确保软件应用程序开发和管理的安全，涵盖安全编码、源代码审查和应用程序安全测试、敏捷软件开发、DevSecOps 管理、

应用程序编程接口开发、最终用户计算和应用程序的管理。相关控制要求及华为云应答如下：

编号	控制域	具体控制要求	华为云的应答
6.1	安全编码、源代码审查和应用程序安全测试	为了最大限度地减少其软件中的错误和漏洞，金融机构应采用安全编码、源代码审查和应用程序安全测试的标准。安全编码和源代码审查标准应涵盖安全编程实践、输入验证、输出编码、访问控制、身份验证、密码实践以及错误和异常处理等领域。	客户应建立源代码安全管理机制。 为满足客户合规要求，华为云严格遵守华为发布的安全编码规范。此外，我们还引入了静态代码扫描工具的每日检查，生成的数据将输入云服务持续集成/持续部署（CI/CD）工具链，通过使用质量阈值进行控制和云服务产品质量评估。源代码在编译前由变更经理审查和批准。开发人员无法批准和编译代码。在任何云产品或云服务发布前，必须完成静态代码扫描告警清除，有效减少因代码延长上线时间的相关问题。所有云服务在发布前都通过了多次安全测试。测试环境与生产环境隔离，避免使用生产数据或敏感生产数据进行测试，并在使用后需要清除。
6.2	敏捷软件开发	在采用敏捷软件开发方法时，金融机构应继续在其敏捷过程中纳入必要的软件开发生命周期和设计安全原则。	客户应建立敏捷软件开发方法的机制。 华为云制定了一套完整的软件开发和隐私活动指南。本指南的目标是指导和标准化安全活动融入研发流程。它提供了产品安全和隐私要求的具体定义和活动指南。华为云要求在早期规划阶段集成安全规划和安全需求分析，确保安全可靠的高效开发云服务。在设计阶段，将进行隐私风险评估和安全隐私设计。 华为云还要求云服务产品团队成员通过参加培训课程，主动学习安全和隐私的基础知识。

6.3	DevSecOps 管理	金融机构应实施适当的安全措施，并对其 DevSecOps 流程中的软件开发、测试和发布职能实施职责分离。	客户应建立 DevSecOps 管理机制。 客户可以通过华为云 IAM 管理使用云资源的用户帐户，以满足职责分离的要求。
6.4	应用编程接口开发	应采用强大的加密标准和密钥管理控制，以确保通过 API 传输敏感数据的安全。	客户应采用强大的加密标准和密钥管理控制，以确保通过 API 传输敏感数据的安全。 华为云在信息传输过程中使用安全的加密通道（如 HTTPS），对存储的静态数据使用安全的加密算法，确保不同状态下的数据机密性。通过数字签名、时间戳等控制机制，防止数据传输过程中的篡改，保证信息的完整性，以及防止重放攻击。记录应用服务中的操作日志，以此来支持审计。对接口进行身份认证、传输和边界保护，确保 API 应用的安全。

6.5 IT 恢复能力

《2021 科技风险管理指南》第 8 章要求金融机构确保其系统的可用性，并实施和测试灾难恢复计划，以最大限度地减少严重事件造成的系统和业务中断。要求覆盖系统可用性、系统可恢复性、灾难恢复计划测试、系统备份和恢复以及数据中心恢复能力。相关控制要求及华为云应答如下：

编号	控制域	具体控制要求	华为云的应答
8.1	系统可用性	IT 系统的设计和实施应达到与其业务需求相称的系统可用性水平。对于系统可用性要求高的 IT 系统，应实施冗余或容错解决方案。	客户可以依托华为云数据中心集群多区域（Region）和多可用区（AZ）架构，实现业务系统的容灾和备份。数据中心部署在世界各地，因此客户将在灾难发生时拥有相互的灾难数据备份中心。当一个区域发生一次故障时，系统会自动将客户应用程序和数据从受影响区域转移到

			数据备份中心，在满足合规策略的同时，确保受影响客户的业务连续性。华为云还部署了全球负载均衡管理中心，客户的应用在数据中心内实现 N+1 部署规模，同时将流量负载均衡到其他中心，即使数据中心故障也是如此。
8. 2	系统可恢复性	金融机构的灾难恢复计划应包括从各种灾难情景中恢复系统的程序，以及相关人员在恢复过程中的角色和责任。灾难恢复计划应至少每年审查一次，并在业务运营、信息资产或环境因素发生重大变化时更新。	华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。
8. 3	灾难恢复计划测试	金融机构应测试系统之间恢复的依赖性。如果网络和系统与特定服务供应商相关联，则应进行双边或多边恢复测试。金融机构应该让用户参与完整的测试用例设计和执行过程，以验证恢复的系统是否能正常运行。金融机构还应参与由其服务供应商（包括位于海外的系统）进行的灾难恢复测试。	客户应对其关键系统建立灾难恢复计划，并考虑是否涉及外包供应商的配合工作，并定期测试该计划。 如果需要华为云协助执行客户的灾难恢复计划，华为会积极配合。 同时，华为云在提供高可用基础设施、冗余数据备份、可用区灾备等服务外，还制定了自身的业务连续性计划。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。如果华为云的灾难测

			试过程中需要客户的参与，华为会提前通知。
8. 4	系统备份与恢复	金融机构应制定系统和数据备份策略，并制定执行定期备份的计划，以便在系统中断或数据损坏或删除时恢复系统和数据。为确保符合金融机构的业务要求数据可用性，金融机构应制定管理备份数据生命周期的政策，其中包括确定数据备份频率和数据保留期、管理数据存储机制以及安全销毁备份数据。	客户应建立其业务连续性机制来备份关键数据。客户可以通过华为云的数据备份归档服务进行数据备份，确保在灾难发生时数据不丢失。此外，客户还可以依托华为云的数据中心集群多区域（Region）和多可用区（AZ）架构，实现业务系统的容灾和备份。数据中心部署在世界各地，因此客户将在灾难发生时拥有相互的灾难数据备份中心。当一个区域发生一次故障时，系统会自动将客户应用程序和数据从受影响区域转移到数据备份中心，在满足合规策略的同时，保证受影响客户的业务连续性。华为云还部署了全球负载均衡管理中心，客户的应用在该中心实现了 N1 部署规模 华为云建立了可指导人员的管理备份流程。
8. 5	数据中心恢复能力	金融机构应对其数据中心（DC）进行威胁和漏洞风险评估（TVRA），以确定潜在的漏洞和弱点，以及为保护数据中心免受物理和环境威胁而应建立的保护。	客户应根据威胁的各种可能情况，综合考虑数据中心建筑结构、周边环境、数据中心基础设施、日常安全流程、关键系统、物理和逻辑访问控制等因素，评估威胁和漏洞的风险。当金融机构选择数据中心提供商时，他们应获取和评估其数据中心威胁和漏洞风险评估（TVRA）报告，并确保 TVRA 报告是最新的，并且数据中心提供商致力于解决已发现的任何重大漏洞。 华为云制定了全面的物理安全和环境安全防护措施、策略和程序，符合 GB 50174《电子信息机房设计规范》A 类标准和 TIA-942《数据中心电信基础设施标准》T3+ 标准。- 华为云运维团队

			定期对全球数据中心进行风险评估，确保数据中心执行严格的访问控制、安全措施、日常监控审计、应急响应等措施。此外，华为 PSIRT 和华为云的安全运维团队已经建立了成熟而全面的漏洞检测、识别、响应和披露计划和框架。华为云依靠该计划和框架来管理漏洞，确保无论是由华为技术还是第三方技术中发现的华为云基础设施和云服务、运维工具中的漏洞，都能在 SLA 内处理和解决。华为云致力于降低并最终避免漏洞被利用对客户造成的业务影响。
--	--	--	--

6.6 访问控制

《2021 科技风险管理指南》第 9 章要求金融机构采取适当的控制措施。要求包括用户访问管理、特权访问管理和远程访问管理。相关控制要求及华为云应答如下：

编号	控制域	具体控制要求	华为云的应答
9.1	用户访问管理	服务供应商或服务供应商的员工，如果被授权访问金融机构的关键系统和其他计算机资源，则会产生与金融机构内部员工类似的风险。金融机构应对这些外部员工和对待内部员工一样地进行严格的监督，监控和访问限制。	客户应建立信息系统的身份认证与访问控制管理机制，对访问系统的行为进行权限限制和监督。 客户可通过华为云的 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。此外，华为云的 云审计服务（Cloud Trace Service，简称 CTS） ，可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分

编号	控制域	具体控制要求	华为云的应答
			<p>析、合规审计、资源跟踪和问题定位等常见应用场景。</p> <p>为配合客户满足合规要求，华为云内部建立了完善的运维和运营账号管理机制。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。所有运维账号由 LDAP 集中管理，通过统一运维审计平台集中监控并进行自动审计。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。并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。保证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。</p>
9.2	特权访问管理	金融机构应密切监督具有较高系统访问权限的员工，并记录和审查他们的系统活动。	<p>客户应建立特权账号的管理机制，密切监督特权账号的使用。</p> <p>为配合客户满足合规要求，华为云相关系统的管理员登录系统时必须先经过双因子认证后，才能通过跳板机接入管理平面。所有操作都会记录日志并及时传送到集中日志审计系统。该审计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。而且华为云有专门的内审部门，会定期对运维流程各项活动进行审计。</p>
9.3	远程访问管理	金融机构应确保仅允许符合金融机构安全标准受保护的设备远程访问金融机构的信息资产。	<p>客户应建立远程访问管理机制。</p> <p>除了通过 IAM 管理远程接入人员的身份和权限外，华为云还提供 VPN、HTTPS 等加密传输方式供客户选择。</p> <p>此外，华为云只能通过华为云统一管理接入网关和 SVN 权限远程访问其内部系统。此外，接入网关支持强日志审计，确保运维人员能够在目标主机上的行为可以定位到个人。</p>

6.7 数据和基础设施安全

《科技风险管理指南》第 11 章要求金融机构确保其数据中心的安全，覆盖数据安全、网络安全、系统安全和虚拟化安全。相关控制要求及华为云应答如下：

编	控制域	具体控制要求	华为云的应答
---	-----	--------	--------

号			
11.1	数据安全	金融机构应制定全面的数据丢失预防策略，并采取措施检测和防止未经授权的访问、修改、复制或传输其机密数据。	客户应识别和分类其重要数据，以便采取适当的控制措施来保护数据。 华为云建议在数据生命周期开始时对数据进行区分和隔离，首先对客户数据进行分类和风险分析。根据风险分析结果，明确存储位置、存储服务和数据保护措施。为了满足合规要求，华为云还在认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理破坏等方面，通过优秀的技术、实践和流程，为客户提供一系列遵循先进行业标准的数据安全生命周期管理服务。它还确保租户隐私、所有权和对其数据的控制不受侵犯，为用户提供最有效的数据保护。更多详细信息，请参见《华为云数据安全白皮书》。
11.2	网络安全	为了将横向移动和内部威胁等网络威胁的风险降至最低，金融机构应部署有效安全机制来保护信息资产。金融机构应安装防火墙等网络安全设备，以保护金融机构和互联网以及与第三方的连接。应在金融机构的网络中部署网络入侵防御系统，以检测和阻止恶意网络流量。	针对常见 CVE 漏洞，华为云将立即分析和更新规则，提供快速、专业的 CVE 漏洞扫描。客户可以部署 WAF(Web Application Firewall)，从多维度检测和保护网站业务流量。华为云严格执行相应的控制措施，确保华为云在架构设计、设备选型、主机网络（多种多层次物理和虚拟网络安全隔离方法）、访问控制、边界防护技术、配置等方面的安全。为了检测和拦截来自 Internet 的攻击以及租户虚拟网络之间的东西向攻击，华为云的网络中部署了网络 IPS 设备，包括但不限于面向公众的网络边界、安全区域信任边界、租户空间边界。华为云的 IPS 可以实时分析网络流量，触发对协议攻击、暴力破解、端口和漏洞扫描、病毒和木马攻击、针对特定漏洞的攻击等各种入侵的拦截。此外，华为云还配置了防火墙设备，以此限制对华为生

			产网络的访问。应在机器上配置防火墙策略的配置，并每月进行一次审查，以确保防火墙规则基于标准配置。因改变防火墙规则而产生的偏差都将被跟踪和补救。华为云通过配置防火墙策略，限制高危端口的访问和高危协议的使用。
11. 3	系统安全	金融机构硬件和软件（例如操作系统、数据库、网络设备和终端设备）的安全标准应概述配置，将网络威胁降到最低。应定期审查标准的相关性和有效性。	客户需要为每个系统制定安全配置基线，并定期检查基线。对于配置不符合安全配置基线的情况，客户需要评估风险，制定规避措施。 华为云为客户提供主机安全服务（HSS），可以识别不安全项目，防范安全风险。HSS 支持主机基线检查，包括检查系统密码复杂度策略、常见弱密码、风险帐户、常见系统和中间件配置。 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。
11. 4	虚拟化安全	应实施强访问控制，以限制对虚拟机管理程序和主机操作系统的管理访问，因为这两者都控制虚拟环境中的来宾操作系统和其他组件。	应制定并记录正式的逻辑安全的政策和程序。及时批准、添加、修改或禁用，并定期审查华为员工和承包商的用户帐户。 华为建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循和授予的。堡垒主机提供基于密码和邮箱验证码的双因素身份验证功能，以验证用户的身份。用户通过互联网访问华为云办公子网，需要根据注册设备及其账号和密码进行双因素认证。华为云员工可以在 CloudScope 中进行逻辑访问管理，CloudScope 涵盖 CloudMNet System、CBC 帐户中心、堡垒机、FUXI 和 SVN 等多种支撑工具。支持工具涵盖本报告范围内所有产品的操作系统，包括但不限于虚拟服

		务器和基础设施设备的支持工具。在所有相关层的支持工具中的访问授权基于最小权限强制实施。高于最低权限的访问需要获得指定人的批准。
--	--	---

7

华为云如何符合 MAS《关于网络卫生的通知》的要求

新加坡金融管理局（MAS）于 2019 年 8 月 6 日和 2019 年 11 月 5 日发布了 11 份针对不同金融机构行业的《关于网络卫生的通知》，为新加坡金融机构提供了关于遵循相关法令的实践指导，《关于网络卫生的通知》的要求覆盖了特权账号、安全补丁、安全标准、网络边界防御、恶意软件防护、多因素认证等领域。

以下内容总结了《关于网络卫生的通知》中与云服务提供商相关的控制要求，并阐述华为云会如何帮助客户满足这些控制要求。

编号	控制域	具体控制要求	华为云的应答
4.1	特权账号	相关实体必须确保与任何操作系统、数据库、应用程序、安全设备或网络设备有关的每个管理帐户都受到保护，以防止未经授权访问或使用此类帐户。	<p>客户应建立特权账号的管理机制，密切监督特权账号的使用。</p> <p>客户可通过华为云的 IAM 服务及 PAM 功能可以更有效地细化管理特权账户。客户也可通过云审计服务（Cloud Trace Service，简称 CTS）作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。</p> <p>华为云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需要经过多级的评审和批准。华为云仅会在得到客户授权后（提供账号/密码）登陆租户的控制台或者资源实例协助客户进行维护。</p>

编号	控制域	具体控制要求	华为云的应答
4.2	安全补丁	<p>(a) 相关实体必须确保应用安全补丁来解决每个系统的漏洞，并在与每个漏洞所构成的风险相称的时限内应用此类安全补丁。</p> <p>(b) 如果没有安全补丁来解决漏洞，相关实体必须确保采取控制措施，以减少这种漏洞对此类系统构成的任何风险。</p>	<p>客户需建立漏洞管理流程，并针对不能通过补丁修复的漏洞制定补偿措施。</p> <p>华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。对于涉及云平台、租户服务等的漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，向最终用户/租户及时推送漏洞规避和修复方案和建议，与租户共同面对安全漏洞带来的挑战。</p>
4.3	安全标准	<p>(a) 相关实体必须确保每个系统都有一套书面安全标准。</p> <p>(b) 在不违反(c)分段的情况下，有关实体必须确保每个系统都符合一套安全标准。</p> <p>(c) 如果系统无法符合一套安全标准，相关实体必须确保采取控制措施，以减少这种不符合规定所构成的任何风险。</p>	<p>客户需对所有系统制定安全配置基线，并定期进行基线检查。针对不符合安全配置基线的情况，需进行风险评估并制定补偿措施。</p> <p>客户可使用华为云企业主机安全（HSS - Host Security Service）对主机进行基线检查，包括检测系统口令复杂度策略、经典弱口令、风险账号，以及常用系统与中间件的配置，以识别不安全项目，预防安全风险。</p>
4.4	网络边界防御	相关实体必须在其网络周边实施控制，以限制所有未经授权的网络流量。	<p>客户需对其网络进行安全区域划分和隔离，针对不同安全域之间的访问进行严格的管控。</p> <p>为配合客户满足要求，华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，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。为了感知来</p>

编号	控制域	具体控制要求	华为云的应答
			自互联网以及客户虚拟网络之间东西向的攻击，并针对攻击实施阻断，华为云在网络边界部署了 IPS 设备，包括但不限于外网边界、安全区域边界和客户空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。
4.5	恶意软件防护	相关实体必须确保在每个系统上实施一项或多项恶意软件保护措施，以降低恶意软件感染的风险。相关实体可以实施可用的恶意软件保护措施。	客户需在所有系统上部署防病毒软件。 为了保证华为云平台以及网络的安全、稳定运行，华为云采取了一系列管理措施，包括：漏洞分析和处理，日志监控和事件响应、云产品默认安全配置优化、安全补丁部署、防病毒软件部署以及定期备份系统和设备配置文件并测试其有效性。
4.6	多因素认证	相关实体必须确保对以下账户实施多因素身份验证： (a) 与作为关键系统的任何操作系统、数据库、应用程序、安全设备或网络设备有关的所有特权帐户；以及 (b) 相关实体通过互联网访问任何系统上的客户信息的所有账户。 如果相关实体在 2020 年 8 月 6 日至 2021 年 2 月 5 日期间已识别到未对以上账户进行多因素认证而造成的风险，且高级管理层或委员会接受该风险或采取补偿措施以降低风险，则在此期间可不满足该要求。	客户需对关键系统的特权账户和可以访问最终客户信息的账户进行多因素认证。在例外情况下，客户需识别并评估未满足上述要求而造成的风险，且高级管理层或委员会接受风险或采取补偿措施以降低风险。 客户可通过华为云的统一身份认证服务（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。 为配合客户满足要求，华为云内部建立了完善的运维和运营账号管理机制。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。另外，华为云相关系统的管理员登录系统

编号	控制域	具体控制要求	华为云的应答
			时必须先经过双因子认证后，才能通过跳板机接入管理平面。所有操作都会记录日志并及时传送到集中日志审计系统。

8

华为云如何符合 ABS《外包服务商控制目标和流程指南》的要求

《外包服务商控制目标和流程指南》为新加坡银行协会（ABS）针对在新加坡运营的金融机构外包服务供应商（OSP）制定的控制目标和流程指南，提出了金融机构的外包服务商必须遵守的最低/基线控制要求，包括审计和检查、实体级别控制、通用 IT 控制和服务控制。此外，针对这些控制要求，外包服务供应商还须提供相关的第三方审计报告（OSPAR）。

以下内容将总结《外包服务商控制目标和流程指南》中与云服务供应商相关的控制要求，并阐述华为云会如何帮助其满足这些控制要求。

8.1 审计和检查

《外包服务商控制目标和流程指南》明确要求为金融机构提供服务的外包服务供应商需要定期聘请外部审计方进行审计，并根据《外包服务商控制目标和流程指南》的要求提供 OSPAR 审计报告。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
I	外部审计方参与	外包服务供应商应聘请合格的审计者根据本指南对提供给金融机构的服务进行审计。如果外包服务供应商决定更换外部审计者或决定指定另一不同的外部审计来验证整改情况，外包服务供应商必须确保新旧审计者之间有适当的工作交接，以确保金融机构的利益得到保护。	华为云目前已获得多项国际上权威的安全与合规认证。华为云每年会聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计。为了建立新加坡金融机构对华为云的信心，华为云在选择审计机构时会参照该指南，保证被选择的审计机构在新加坡银行业具备丰富的审计经验，能满足该指南对外部审计方的资质要求。如果更换审计机构，华为云也将遵循内部规范的流程，确保上任审计机构与新任审计机构进行充分的工作交接。
II	外部审计方资质的标准	聘请的审计公司必须在过去 5 年内对至少 2 家在新加坡经营的商业银行进行过审计，且签署审计报告的合伙人必须在过去 5 年内至少对超过 2 家在新加坡经营的	

编号	控制域	具体控制要求	华为云的应答
		商业银行进行过审计。	
III	审计的频率	审计应每 12 个月进行一次。为测试控制措施的操作有效性而选择的样本应覆盖自上次审计以来的整个期间，最小测试期为 6 个月。如果少于 6 个月，应在报告中说明期限较短的原因。	华为云每年会聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计，并且会按照外包服务供应商审计报告(OSPAR)模板中规定的格式发布审计报告，在报告形成后，华为云将根据内部流程向金融行业客户发布审计报告的副本。
IV	审计报告	指定的外聘审计者应以外包服务供应商审计报告(OSPAR)模板中规定的格式发布审计报告。外包服务供应商必须向其金融机构客户提供其审计报告的副本。	
V	汇报和处理控制缺失/控制目标的质量	<p>如果审计者发现与控制目标有关的控制活动的设计和/或操作有效性的不足，审计者应评估失败对提供给金融机构的服务的潜在影响。相关的审计标准规定了控制目标的鉴定程序，审计者应当遵循。</p> <p>外包服务供应商应在不迟于外包服务供应商审计报告(OSPAR)发布日期之前通知金融机构重大问题和关注点以及补救计划。但是，如果问题可能导致外包安排中长期服务失败或中断，或违反金融机构客户信息的安全性和保密性，外包服务供应商应在出现问题后立即通知金融机构。</p> <p>外包服务供应商应制定补救计划，以解决审计中发现的问题。如果问题需要更长的时间来纠正，外包服务供应商应确定短期措施以缓解风险。补救措施应通过审计方或其它有能力的独立方的验证。</p>	<p>华为云会根据外部审计机构的要求，提供用于验证华为云安全和合规管控措施有效性的审计样本，如安全体系管理文件、操作记录、系统日志等。如有特殊情况导致审计样本覆盖的时间不满足要求，华为云将配合审计机构在审计报告中注明原因。</p> <p>针对审计过程中发现的所有问题，华为云将在审计机构的协助下，根据风险评估机制，评估这些问题对金融行业客户的潜在影响。若经评估后，识别出可能对客户业务/数据的可用性、完整性和保密性造成严重影响的问题，华为云会将此类问题列为安全事件，并根据已制定的客户通知流程，及时对受影响的客户群体进行通知，通知的内容包括但不限于问题描述、问题影响、下一步补救计划等。同时，华为云会根据内部的安全事件管理流程对问题进行整改，整改完成后审计机构会进行再评估。</p>
VI	金融机构和 MAS 的权力	新加坡金融监管局(MAS)和金融机构有权对外包服务供应商以及外包服务供应商的分包商进行审计。	<p>客户应建立正式的审计程序，定期对其外包供应商进行审计。</p> <p>华为云会积极配合新加坡金融监管局(MAS)和金融机构对华为云以及华为云的供应商进行审计。</p>

8.2 实体级别控制

《外包服务商控制目标和流程指南》中第一部分的控制要求为实体级别控制，即企业内部控制，以确保外包服务供应商执行与整个实体相关的管理指令。实体级别的控制主要包括控制环境、风险评估、信息和沟通、监控、信息安全政策、人力资源政策和流程、以及与分包相关的实践七大部分，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
I. (a)	控制环境	控制环境确定了外包服务供应商的企业内部优先级和文化，影响了员工对内部控制的意识和态度。是实施有效内部控制的基础，提供了纪律和组织架构。	为了让所有员工不断提升安全意识，更好地保障客户利益和产品与服务信誉，华为在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。这种文化的影响贯穿在华为云招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。在组织方面，全球网络安全与隐私保护委员会作为最高网络安全管理机构，决策和批准公司总体网络安全战略。全球网络安全与隐私保护官及其办公室负责制定和执行华为端到端网络安全保障体系。
I. (b)	风险评估	外包服务供应商的风险评估过程可能会对提供给金融机构服务造成影响。以下是风险评估因素列表： <ul style="list-style-type: none">• 运营环境的变化• 新员工• 新的或改进的信息系统• 快速增长• 新技术• 新的商业模式、产品或活动• 公司重组• 海外业务的扩展• 环境扫描	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法律法规、标准发生重大变化时，华为云会增加风险评估的次数。
I. (c)	信息和沟	外包服务供应商的内部控制信息和沟通部分应包	客户可通过华为云官网来了解华为云提供的云服务的相关信息。华为云对外提

编号	控制域	具体控制要求	华为云的应答
	通	括：信息系统中必须记录启动、授权、记录、处理和报告金融机构的交易的程序，外包服务供应商如何传达其角色和职责以及如何传达与提供给金融机构的服务相关的重要事项。	供了统一的电话热线、邮箱地址以及工单系统处理金融机构的服务请求。华为云也会建立与相关监管机构的联系，以便必要的沟通。
I. (d)	监控	外包服务供应商可以雇用内部审计员或其他人员，通过持续活动、定期评估或两者结合的方式来评估控制的有效性。外包服务供应商应制定流程，将此类评估确定的重大问题和需要关注的事项上报给外包服务供应商的高级管理层，此外，如果影响到所提供的服务，也需要告知金融机构。对于其分包商活动中会影响提供给金融机构服务的活动，外包服务供应商对这类活动应进行监测。外包服务供应商也应该监控外部沟通，如客户投诉和监管机构发来的信息，其结果应提供给金融机构。	华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。华为内部审计团队直接向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。严格的审计活动在推动网络安全流程和标准落地，保障结果交付上起着关键的作用。此外，华为云建立了完备的供应商选择机制和管理机制，除了对供应商的绩效进行日常监督和管理之外，也会定期对供应商进行风险评估。针对审计发现的问题，组织内会进行再评估，如果问题对金融机构的业务会造成重大影响，华为云会告知金融机构。 华为云对外提供了统一的沟通接口，负责收集并处理客户侧的投诉，以及向金融客户同步监管机构发布的通告。
I. (e)	信息安全政策	将信息安全政策和流程形成文档，至少每 12 个月和在有变化发生时对其进行审查。信息安全政策和流程应指明负责信息安全管理的人员。 这些文件由管理层审查和批准。明确系统和网络的特定安全控制以保护系统和数据的保密性、完整性和可用性。记录、跟踪和修复任何已识别出的差距。若存在影响所提供的服务的差距，应立即告知金融机构。 应建立信息安全意识培训	客户应建立正式的信息安全政策和流程，并定期对其进行审查。 华为云参照 ISO27001 构建了完善的信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性。全方位保护客户系统和数据的保密性、完整性和可用性。此外，华为云重点关注员工以及外包人员的安全意识培养，制定了可落地的安全意识培训计划并定期执行。

编号	控制域	具体控制要求	华为云的应答
		计划。为可以访问 IT 资源和系统的外包服务供应商工作人员、分包商和供应商定期开展培训计划。	
I. (f)	人力资源政策和流程	外包服务供应商应对候选人进行背景调查，并确保考虑雇佣的个人要通过对其经验、专业能力、诚实和正直道德品质的充分筛选。使其能够满足 ABS 控制目标和 MAS 外包指南相关的要求。	华为云建立了人力资源管理框架，是建立在法律基础之上。云安全对 HR 的诉求主要是保证员工背景和资历适合华为云业务的需要。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。员工有履行其职责必备的知识、技能和经验。华为云对运维工程师等重点岗位实施专项管理。包括：上岗安全检查、在岗安全培训赋能、上岗资格管理、离岗安全审查。
I. (g)	与分包相关的实践	金融机构希望对外包服务供应商的分包商进行和对外包服务供应商本身同样严格的管理。因此，外包服务供应商应要求并确保其分包商遵守本指南	华为云制定了自身的供应商管理机制，从供应商的产品和供应商本身的内部管理都提出了安全需求。此外，华为云会对供应商进行定期的稽核，对有风险的供应商会到现场进行审核。此外会与涉及网络安全的供应商签署网络安全协议，在服务过程也中会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应商进行合作降级处理。

8.3 通用 IT 控制

《外包服务商控制目标和流程指南》中第二部分的控制要求为通用 IT 控制，涵盖了网络安全方面的各个领域，包括逻辑安全、物理安全、变更管理、事件管理、备份和灾难恢复、网络和安全管理、安全事件响应、系统脆弱性评估及技术更新管理，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
II. (a)	逻辑安全	金融机构应确保对程序、数据和操作系统软件的逻辑访问根据按需原则来授权。金融机构应根据商定的信息安全要求/标准定期审查应用程序/系统的密码管理情况。严格控制具有较高访问权限账号的使用。	在本文的“ 6.7 数据和基础设施安全 ”中详细阐述了华为云是如何满足该指南对身份认证和访问控制的要求

编号	控制域	具体控制要求	华为云的应答
II. (a)	逻辑安全	金融机构应建立相关的数据删除流程，以在每次终止服务时根据流程安全销毁或删除金融机构的数据。这一要求也适用于备份数据。	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，华为云会严格遵循数据销毁标准以及与客户之间的协议约定，对存储的客户数据进行清除。关于数据删除的详细信息请参见《华为云数据安全白皮书》4.8 永久销毁
II. (a)	逻辑安全	应根据 MAS 技术风险管理指南（TRM）部署行业公认的加密标准并与金融机构达成一致，以保护金融机构客户信息和其他敏感数据。	华为云将复杂的数据加解密、密钥管理逻辑进行封装。目前，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，采用高强度的算法对存储的数据进行加密。 服务端加密功能集成了华为云 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。
II. (b)	物理安全	数据中心/控制区域应受到物理保护以保护其不受内部和外部威胁。主要包括：限制对数据中心/控制区域的访问、所有入口安装入侵警报、对安全区域的出入进行跟踪审计、定期审查对数据中心的访问、管理物理访问凭证、执行威胁和脆弱性风险评估（TVRA）。 数据中心/控制区域的安	华为云已制定并实施了完善的物理和环境安全防护策略、规程和措施，满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中的 T3+ 标准。更多详细信息请参见《华为云安全白皮书》的“物理与环境安全”。

编号	控制域	具体控制要求	华为云的应答
		全措施还应保护 IT 资产的韧性。包括安装完备的环境控制系统，并对环境控制设备进行检查、测试和维护。	
II. (c)	变更管理	<p>金融机构应以受控方式评估、批准、测试、实施和审查应用程序、系统软件和网络组件的变更。</p> <p>保证开发、测试、分级和生产环境的隔离。</p> <p>UAT 数据应该是匿名的，如果 UAT 包含生产数据，则环境必须受到适当的生产级别的控制。</p> <p>对高风险系统和应用程序的变更进行源代码审查，以在实施这些变更之前识别安全漏洞和缺陷、代码错误、缺陷和恶意代码。</p>	<p>客户应建立正式的变更管理程序，并定期对变更的执行进行审查，特别是源代码的审查。客户应该保证其开发、测试和生产环境相互隔离，并严格管控不同环境的使用。</p> <p>为配合客户满足合规要求，华为云也制定了变更管理程序，管理应用变更和基础设施变更。在提出变更申请生成后，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。</p> <p>华为云开发、测试和生产环境都进行了隔离，并且严格控制未脱敏的数据流入测试环境。华为云严格遵从华为对内发布的多种编程语言的安全编码规范。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。</p>
II. (d)	事件管理	金融机构应保证系统和网络的运行问题得到及时和有效的解决，保证存在正式的记录在案的事件管理流程，该流程应明确记录参与事件管理流程（包括问题和事件的记录、分析、修复和监控）的员工的角色和职责，事件升级和事件解决时限要求，以记录和跟踪事件的信息，分析事件原因，找出根本原因，防止事故再次发生。	<p>客户应建立正式的事件管理程序，及时解决系统和网络故障。</p> <p>为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）</p>

编号	控制域	具体控制要求	华为云的应答
			记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。
II. (e)	备份和灾难恢复	金融法机构应执行信息系统的备份和安全存储。并记录、批准、测试和维护业务和信息系统恢复和连续性计划。	<p>客户应制定其业务连续性机制，对关键数据进行备份。</p> <p>客户可通过华为云的数据备份归档服务，对数据进行备份，保证在灾难发生时数据不丢失。</p> <p>同时，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。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。</p>
II. (f)	网络和安全管理	系统和网络控制是根据客户的业务需求来实现的。金融机构应定义系统和网络的特定安全控制；为各种中间件、操作系统、数据库和网络设备定义安全基线标准；执行能确保定期安装和更新反病毒/反恶意软件的流程；建立补丁管理流程；记录与安全政策/标准的偏差，并实施缓解控制措施以降低风险；有文件完整性检查；部署网络安全控制以保护内部网络；定期对网络安全设备的规则进行备份和审查；记录、保存和监控安全系统的事件。	<p>客户应建立正式的系统以及网络管理程序。</p> <p>为配合客户满足合规要求，华为作为云技术的研发者和云服务运营者的双重角色，华为云负责其作为 CSP 的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全保障。华为云一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层次安全隔离，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。此外为了保证华为云平台以及网络的安全、稳定运行，华为云采取了一系列管理措施，包括：漏洞分析和处理，日志监控和事件响应、云产品默认安全配置优化、安全补丁部署、防病毒软件部署以及定期备份系统和设备配置文件并测试其有效性。</p>

编号	控制域	具体控制要求	华为云的应答
II. (g)	安全事件响应	应确保在安全事件发生时能够联系适当的人员，并针对安全事件立即采取措施。	华为云内部制定了完善的安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有 7*24 的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。在事件解决后，会根据具体情况向客户提供事件报告。
II. (h)	系统脆弱性评估	外包服务供应商持续监控紧急安全漏洞，并定期对 IT 环境进行脆弱性评估，以应对常见和紧急的内部和外部安全威胁。脆弱性评估的频率应根据金融机构的风险评估结果与金融机构达成共识。外包服务供应商应至少每 12 个月执行一次针对面向互联网的系统的渗透测试。通过脆弱性评估和渗透测试确定的问题得到及时修复和并重新对其进行验证，以确保已确定的差距已经完全解决。	华为 PSIRT 和华为云安全运维团队已经建立了完善的漏洞感知、处置和对外披露的机制。同时，华为云会积极实施云产品和云平台的安全质量保证工作，每年会开展内部和第三方渗透测试和安全评估，以保证华为云云环境的安全性。
II. (i)	技术更新管理	金融机构应实施合理的控制措施保证在生产和灾难恢复环境中使用的软件和硬件组件会被及时更新。控制措施包括：至少每 12 个月以及在有变更时对技术更新管理计划和流程进行记录和审查；维护支持金融机构的生产和灾难恢复环境中使用的软件和硬件组件的最新库存，以便于跟踪 IT 资源；外包服务供应商积极管理其支持金融机构的 IT 系	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。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。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和灾难

编号	控制域	具体控制要求	华为云的应答
		统和软件；外包服务供应商应告知金融机构识别出来的要停止使用或更换的系统；当停止使用 IT 系统时，外包服务供应商应确保金融机构的信息安全地从系统中销毁/清除，以防止数据泄漏；对接近终止技术支持（EOS）日期的系统进行风险评估，评估继续使用可能会导致的风险，并在必要时建立有效的风险缓解控制措施。	恢复计划，并定期对其进行测试。以保证应急预案符合当前的组织环境和 IT 环境。 华为云致力于保护租户数据在删除过程中及删除后不至泄露。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，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。所涉的数据删除类型包括：内存删除、数据安全（软）删除、磁盘数据删除、加密数据防泄漏、物理磁盘报废，更多详细信息请参见《华为云安全白皮书》4.6.4 数据删除与销毁。

8.4 服务控制

《外包服务商控制目标和流程指南》中第三部分控制要求为服务控制，涵盖外包服务供应商为金融机构提供服务过程中管理方面的控制，涵盖建立新的客户/流程、授权和处理交易、维护记录、保护资产、服务报告和监控。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
III. (a)	建立新的客户/流程	应制定并监控外包服务供应商合同流程。并且外包服务供应商的流程应按照金融机构的协议和指示建立和管理。	客户应建立正式的外包合同管理程序。 为配合客户满足合规要求并行使对云服务供应商的监管，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，在其中与客户共同约定相应要求。如有必要，华为云会积极配合客户方发起的尽职调查。 同时，华为云制定了自身的供应商管理机制，对供应商的产品和供应商本身的内部管理都提出了安全需求。华为云会对供应商进行定期的稽核，对有风险的供应商会到现场进行审核。此外，华为云会与涉及网络安全的供应商签署网络安全协议，在服务过程中会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应

编号	控制域	具体控制要求	华为云的应答
			商进行合作降级处理。
III. (b)	授权和处理交易	外包服务供应商的服务和相关流程应得到全面、准确和及时的授权和记录，服务接受内部检查，以降低出错的可能性，服务由独立方分阶段处理，从开始到完成都应有职责分离。	客户应管理外包服务供应商的服务。 为配合客户满足合规要求，华为云制定了完善的服务管理体系，且通过了 ISO20000 的认证，保证提供有效的 IT 服务来满足客户的需求
III. (c)	维护记录	应根据敏感度对数据进行分类，敏感度决定数据保护要求、访问权限和限制以及保留和销毁要求。	为保障客户安全的处理云上数据，华为云对数据从数据创建、数据存储、数据使用、数据共享、数据归档到数据销毁全生命周期的各阶段进行层层防护，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。更多详细信息请参见《华为云数据安全白皮书》
III. (d)	保护资产	应保护实物资产不受损失、滥用和未经授权的使用。	华为云已制定并实施了完善的物理和环境安全防护策略、规程和措施，满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中的 T3+ 标准。更多详细信息请参考《华为云安全白皮书》物理与环境安全部分。
III. (e)	服务报告和监测	外包活动应得到妥善管理和监控。	客户应管理和监控外包活动。 客户可通过华为云的云监控服务，监控自身云资源的使用情况和绩效。华为云也可以根据客户的需求按照 SLA 提供服务报告。

9

华为云如何符合 ABS《ABS 云计算实施指南》的要求

新加坡银行协会（ABS）于 2019 年 8 月发布了《ABS 云计算实施指南 2.0》，该指南为金融机构提供了关于使用云服务的最佳实践和注意事项，包括对云服务供应商尽职调查建议的活动以及在采用云服务时需要考虑的关键控制措施。

以下内容将总结《ABS 云计算实施指南 2.0》中与云服务供应商相关的控制要求，并详细阐述了华为云作为金融机构的云服务供应商如何帮助金融机构满足这些控制要求。

9.1 尽职调查建议的活动

《ABS 云计算实施指南 2.0》第三部分向金融机构提供了在使用云服务方面关于尽职调查和供应商管理的建议，涵盖了使用云服务之前以及采用云服务后持续的风险评估和对云服务供应商的监管。指导建议主要包括治理、对云服务供应商的评估和合同考虑，相关控制要求及华为云的应答如下：

原文编号	控制域	具体控制要求	华为云的应答
第 1 条	治理	<p>金融机构应确保与云服务供应商在书面协议中充分规定了关于所有缔约方的角色、关系、义务和责任的合同条款和条件，以及所购买云服务的 KPI、关键活动、投入和产出以及一旦出现违背协议情况的问责制。</p> <p>金融机构应该进行尽职调查，了解其正在采用的服务以及金融机构和云服务供应商</p>	<p>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》对客户和华为云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，需通知客户，并对分包的服务负责。</p> <p>华为云明确定义了与客户之间的安全责任共担模型，客户可在华为云官网上查阅《华为云安全白皮书》中关于责任共担模型的具体内容。华为云制定了完善的信息安全风险管理框架，也会对外包商以及外包人员进行严格的安全管理，并会定期对其供应商进行审计和安全评估。</p>

原文 编号	控制 域	具体控制要求	华为云的应答
		的职责。云服务供应商应该能够证明它实施并维护了一个强大的风险管理与治理框架，该框架可有效管理云服务安排，包括任何分包安排。	华为云已通过 ISO 27001 认证，并且每年会聘请专业的外部资源进行 SOC2 鉴证。关于日常安全运维运营的具体实践，华为云在《华为云安全白皮书》中进行了详细介绍。
第 2 条	对云服务供应商的评估	金融机构应对云服务供应商进行尽职调查，需要考虑的因素包括：财务状况、公司治理和实体控制、数据中心地理位置、物理安全风险评估、尽职调查流程、分包。	<p>财务状况：华为每年会发布年报，会包含华为云的营收情况，并对外公开。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。</p> <p>公司治理和实体控制：华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”的原则，网络安全已经成为了华为公司的发展战略。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。</p> <p>数据中心地理位置：客户购买云服务时可自行选择数据中心，华为云遵循客户的选择。华为云不会在未经客户同意的情况下将客户内容从选择的区域中迁移，除非 (a) 必须迁移以遵守适用的法律法规或者政府机关的约束性命令；(b) 为了提供账单、管理、技术服务或者出于调查安全事件或调查违反合同规定的行为。</p> <p>物理安全风险评估：华为云会定期对全球的数据中心进行风险评估，生成评估报告，并针对评估过程中识别出来的风险制定详细的风险处置计划。</p> <p>尽职调查流程：华为云会安排专人配合金融机构协助其尽职调查。为了便于金融机构了解华为云符合金融机构尽职调查涵盖的要求，华为云也主动聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计，并且会按照外包服务供应商审计报告（OSPAR）模板中规定的格式发</p>

原文 编号	控制 域	具体控制要求	华为云的应答
			布审计报告。在报告形成后，华为云将根据内部流程向金融行业客户发布审计报告的副本。 分包： 华为集团有完善的供应商和外包管理规范，华为云遵循华为集团的外包管理规定。
第 3 条	合同 考虑	金融机构应确保与云服务供应商的合同协议中包括关于以下内容的条款：数据机密性和控制权、数据传输和数据所在位置、审计和检查、业务连续性管理、服务级别协议、数据保留、违约终止、退出计划。	为配合客户行使对云服务供应商的监管，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，在其中与客户共同约定相应要求。

9.2 进入云外包安排时建议的控制措施

《ABS 云计算实施指南 2.0》第四部分规定了金融机构在进入云外包安排时对其标准工作应实施的最低/基线控制，以及对重要和关键工作应采取的额外的控制措施。该指南将控制要求涉及的领域按照使用云服务需经历的各个阶段进行分类，包括治理云、设计和保护云、运行云。相关控制要求及华为云的应答如下：

原文 编号	控制 域	具体控制要求	华为云的应答
治理云			
第 1 条	对云服务提供商管理的组织上的考虑	金融机构应对与云外包安排相关的风险进行有力和及时的监督，包括对云服务供应商进行尽职调查、监督 SLA 执行情况、监督安全事件相关风险等。金融机构的业务部门和运营部门与云服务供应商之间应有相应的沟通渠道。	为满足客户对云外包安排监督的要求，华为云对外提供了统一的电话热线、邮箱地址以及工单系统处理客户的服务请求。若客户需要对华为云发起尽职调查，华为云将有专人负责对接；华为云向客户提供云监控服务，供客户监控自身云资源的使用情况和绩效，并且可以根据客户的需求按照 SLA 提供定制化服务报告，但此服务可能会涉及费用。

原文 编号	控制 域	具体控制要求	华为云的应答
第 3 条	计费 模型	金融机构应对其云资源和云成本进行管理。保证基于服务级别协议的关键服务监控到位，并与 CSP 建立协议，防止基于配额的服务停止。	为满足客户对服务配额的要求，华为云会列算各服务消费的详细费用清单，租户可核算自身的消费情况。客户可在华为云管理控制台（Console）中监控账户消费情况是否超过配额，以提醒租户根据配额使用服务，防止因为总配额耗尽而导致服务中断。另外，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。
设计和保护云			
第 1 条	云架构参考解决方案及实践	金融机构应创建符合金融机构内部政策和监管要求的云产品服务目录，设计和实施优化的云服务。	华为云为金融客户提供专门的金融行业解决方案，帮助金融客户快速实现业务云化部署。
第 2 条	虚拟化、容器化及 DevOps	管理与数据混合或共享租赁环境相关的机密性和完整性风险。如果软件或硬件出现故障，请确保信息资产保持安全或被安全移除。 定义一套标准的工具和流程来管理容器、镜像和发布管理。	客户应考虑建立标准化的发布流程管理容器和镜像。同时，华为云针对 弹性云服务器（Elastic Cloud Server，简称 ECS） 配套提供了镜像服务，租户可自行选择华为云官网提供的标准镜像或者私有化镜像，通过控制台（Console）的管理，可以方便地进行版本管理和发布管理。 另外，华为云从网络隔离、数据隔离、外部威胁防御以及身份认证与访问控制等多方面保证在多租户场景下客户信息的安全性。更多详细资料请参见《华为云安全白皮书》。 当发生软硬件故障后，如果相应的资源被释放掉后，客户内容会自动进行销毁，华为云会通过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恢复。
第 3 条	云架构韧性	金融机构需要仔细考虑和规划其云的应用，以确保云服务的弹性和可用性与其需求相称。	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弹性和可用性，数据中心按规则部署在全球各地，客户可通过两地互为冗余，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，保证业务的持续运行。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

原文 编号	控制 域	具体控制要求	华为云的应答
			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。
第 4 条	网络架构	金融机构应实施保护云环境和内部环境的措施，以降低威胁扩散的风险，确保基于云的业务免受网络攻击。 金融机构应确保根据需要授予对云环境的访问权限。	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（VPC - Virtual Private Cloud）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，为保证租户业务不影响管理操作，确保设备、资源和流量不会脱离有效监管，华为云将其网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、BMC（Baseboard Management Controller）管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，便于实现职责分离。
第 5 条	密钥管理	金融机构应管理加密材料，使金融机构数据的机密性和完整性不会受到损害。管理措施包括：定期轮换密钥、制定详细的政策和程序管理加密材料的生命周期以及加密材料的备份等。	华为云为客户提供了数据加密服务（DEW）的密钥管理功能，可对密钥进行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。华为云使用硬件安全模块（HSM）为客户创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露，保护密钥安全。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，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。
第 6 条	加密	金融机构应确保只有授权方才可以访问传输中的和静态的数据。 金融机构应确保数据的机密性和/或完整性，并提供消息来源的身份验证	客户应制定数据管理机制，保证数据的机密性、完整性。客户可通过华为云的数据存储加密服务实现对数据的加密，华为云将复杂的数据加解密、密钥管理逻辑进行封装，使得客户的数据加密操作变得简单易行。目前，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，采用高强度的算法对存储的数

原文 编号	控制 域	具体控制要求	华为云的应答
		及消息的不可抵赖。	<p>据进行加密。服务端加密功能集成了华为云数据加密服务（DEW）的密钥管理功能，其中使用的硬件安全模块（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客户根密钥。对于传输中的数据，当客户通过互联网提供 Web 网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给 Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。针对客户业务混合云部署和全球化布局的场景，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。</p>
第 8 条	用户访问管理和认证	金融客户应考虑用户访问管理的整个生命周期，以确保用户仅能访问其履行职责所需的信息资产、保证数据的机密性和完整性、确保敏感角色的职责分离。	<p>客户应制定身份认证与访问管理机制，管控其员工对相应资产的访问权限。华为云的统一身份认证服务（IAM）为客户提供云上资源访问控制。使用 IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用 IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过云审计服务（CTS）作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。</p> <p>同时，华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，如 USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。</p>
第 9 条	特权用户访问管理	金融机构应适当管理特权用户访问，并确保第三方服务供应商只能通过授权的例外情况访问	<p>客户可通过华为云的 IAM 服务及 PAM 功能可以更有效地细化管理特权账户。</p> <p>为配合客户满足合规要求，华为云对于运维人员实行基于角色的访问控制，限定不同岗</p>

原文 编号	控制 域	具体控制要求	华为云的应答
		其信息资产。	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需要经过多级的评审和批准。华为云仅会在得到客户授权后（提供账号/密码）登陆租户的控制台或者资源实例协助客户进行维护。
第 10 条	远程访问	金融机构应管理对其云环境中的平台和系统进行的各种级别的远程访问。云服务供应商也应对其自身系统的远程访问进行管理。	客户应建立远程访问管理机制。 客户除了通过统一身份认证服务（IAM），对远程接入人员的身份和权限进行管理外，华为云还提供了加密传输的方式供客户自行选择，比如 VPN、HTTPS 等。 同时，对于华为云内部系统的远程访问仅可以通过堡垒机和 SVN 的方式。华为云统一管理堡垒机和 SVN 的权限，对华为云运维人员进行身份认证，并且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。
第 11 条	数据防丢失	金融机构应制定全面的数据丢失防护策略，保护传输到云中和存储在云中的数据的安全，以免云环境中的数据免遭未经授权或无意的泄漏，并监控和控制经批准和未经批准的数据传输以及对云服务的访问。	客户应建立正式的数据保护机制。 为配合客户满足合规要求，华为云向客户提供一系列数据存储服务，服务遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，保证租户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。
第 12 条	源代码审查	金融机构应确保源代码及其他代码工件（例如编译和非编译代码、库、运行时模块）的机密性和完整性，在发布管理过程中进行源代码审查。	客户应建立源代码的安全管理机制。 为配合客户满足合规要求，华为云严格遵从华为对内发布的多种编程语言的安全编码规范。引入了静态代码扫描工具进行每日检查，确保所有云产品、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。所有云服务发布前都经过了多轮安全测试。测试环境与生产环境隔离，并避免生产数据或未脱敏的生产数据用于测试，使用完成后需要进行数据清理。
第 13	渗透	云服务供应商的渗透测试报告可用于	客户应该对 CSP 的环境进行渗透测试。

原文 编号	控制 域	具体控制要求	华为云的应答
条	测试	<p>确保底层系统安全性，并确保测试涵盖服务提供中涉及的所有系统，对所有漏洞进行风险评估、跟踪和适当管理/处理。</p> <p>金融机构应该考虑使用红队方法来测试云服务供应商的环境。</p>	<p>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。</p> <p>华为云已与合作伙伴联合推出了主机入侵检测、Web 应用防火墙、主机漏洞检测、网页防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力。</p>
第 14 条	安全事件监控	<p>金融机构应建立适当的集中式系统，以便对来自各种监控系统的安全日志进行自动分析、关联和分类，并确保日志的完整性和可用性。以便及时检测和响应云环境中的安全事态和事件。</p> <p>金融机构应确保云服务供应商的关键数据库和记录系统具有快照功能，以实现灾难恢复和业务连续性。</p>	<p>客户应建立集中的监控平台对各个系统的安全日志进行自动分析，及时检测和响应安全事态和事件。</p> <p>为配合客户满足合规要求，华为云有集中、完整的日志审计系统。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。华为云日志管理系统是基于 ELK 建立的。华为云使用大数据安全分析系统，关联各种安全设备的告警日志，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。</p> <p>华为云提供关系型数据库服务，是一款允许租户快速发放不同类型数据库，并可根据业务需要对计算资源和存储资源进行弹性扩容的数据库服务。其提供自动备份、数据库快照、数据库恢复等功能，以防止数据丢失。</p>
第 15 条	保护日志及备份	金融机构和云服务供应商应该对系统生成的日志数据采取适当的保护措施，确保日志数据的机密性和完整性，并保证日志数据不包含敏感信息。	<p>华为云的云审计服务（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。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。CTS 会对各服务发送过来的日志数据进行检视，确保数据本身不含敏感信息；在传输阶段，通过身份认证、格式校验、白名单校验以及单向接收机制等手段，确保日志信息传输和保存的准确、全面；在保存阶段，采取多重备份，并根据华为网络安全规范要求，对数据库自身安全进行安全加固，杜绝仿冒、抵赖、篡改以及信息泄露等风险；最后，CTS 支持数据以加密的方式保存到 OBS 桶。</p> <p>同时，华为云针对所有物理设备、网络、平</p>

原文 编号	控制 域	具体控制要求	华为云的应答
			台、应用、数据库和安全系统的管理行为日志也会进行管理，确保所有日志保存时间超过 180 天，90 天内可以实时查询。
运行云			
第 1 条	变更 管理	应确保所有变更遵循变更管理流程，包括由云服务供应商控制的 IaaS、PaaS 和 SaaS 环境的变更，并提供与其风险相称的监督。确保对可能影响云操作环境稳定性和/或安全性的重大变更进行监督，并检测未经授权或错误的变更。	客户应建立正式的变更管理程序。华为云提供的云审计服务（CTS）可以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。可实时、系统地记录所有人员的操作，以便客户对各项变更执行事后审计。 同时，华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的变更管理。华为云制定了完善的变更管理流程并定期对其评审和更新。按照变更可能对业务造成影响的程度定义了变更类别和变更窗口，以及变更通告机制。该流程要求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。
第 2 条	配置 管理	金融机构应实施监控，以检测云环境的未授权变更。在可能的情况下，金融机构应实施自动恢复，以减轻高风险变更。	客户应对其变更进行监控，以检测未经授权的变更。华为云提供的云审计服务（CTS）可以记录操作人员对华为云上的资源和系统配置的变更，供用户查询、审计和回溯使用。 同时，华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的配置管理。华为云设置配置经理对所有业务单元进行配置管理，包括提取配置模型(配置项类型、各类配置项属性、配置项间的关系等)、记录配置信息等，并通过专业的配置管理数据库工具（CMDB - Configuration Management Database）对配置项、配置项的属性和配置项之间的关系进行管理。
第 3 条	重大 事件 管理	应定义和监控关键事件，以确保云环境的机密性、可用性和完整性不受损害。提供对信息技术环境中网络和系统异常的早期检	客户应该制定重大事件管理程序，确保重大事件及时发现、快速解决，以保证云环境的安全、稳定运行。华为云的云监控服务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

原文 编号	控制 域	具体控制要求	华为云的应答
		测，以便及时应对潜在的技术和安全事故，并根据事件的关键程度和分配的所有权，适当地管理和上报事件。	则和通知策略，以便用户及时检测云资源的异常并采取应对措施。 同时，华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的重大事件管理。华为云拥有集中、完整的日志审计系统。并利用大数据安全分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的重大事件。并根据事件的实时状态进行事件升级和通报。
第 4 条	事件 和问 题管 理	当新的威胁情报可用时，在信息技术环境中提供合理水平的安全事件追溯检测。确保技术和安全事故得到适当升级，并通知相关利益相关方以采取管理措施。确保环境中的事件得到适当审查，并纠正已发现的差距，以防止再次发生。	客户应建立正式的事件和问题管理程序。华为云的云监控服务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。可协助用户快速获取云资源的告警，经采取相应的应对措施。同时华为云还可提供 Anti-DDoS 流量清洗服务、Web 应用防火墙服务、 数据库安全服务（Database Security Service，简称 DBSS） 、云审计服务（CTS）可帮助用户精准有效地实现对流量型攻击和应用层、数据层攻击的全面防护，以及事后对安全事件进行追溯和审计的功能。 同时，华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的事件和变更管理。华为云制定了完善的事件和管理流程并定期对其进行评审和更新。华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。
第 5 条	容量 管理	金融机构应清楚地了解其业务运营对资源的要求，以确保业务职能能够不受任何干扰地继续进行。对资源进行	客户应建立正式的容量管理程序，对其云资源进行监控，确保云资源能够满足业务增长的需要。客户可通过华为云的云监控服务对弹性云服务器、带宽等资源进行的立体化监控。云监控服务的监控对象是基础设施、平台及应用服务的资源使用数据，不监控或触

原文 编号	控制 域	具体控制要求	华为云的应答
		适当的监控，以了解平均利用率和峰值。保证系统拥有适当的资源，以便在发生故障或计划外停机时能够恢复。	<p>碰租户数据。云监控服务目前可以监控下列云服务的相关指标：弹性计算服务（ECS）、云硬盘服务（EVS）、虚拟私有云服务（VPC）、关系型数据库服务（RDS）、分布式缓存服务（DCS）、分布式消息服务（DMS）、弹性负载均衡（ELB）、弹性伸缩服务（AS）、网站应用防火墙（WAF）、主机漏洞检测服务（HVD）、云桌面服务（Workspace）、机器学习服务（MLS）、网页防篡改服务（WTP）、数据仓库服务（DWS）、人工智能服务（AIS）等。用户可以通过这些指标，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。</p> <p>同时，华为云内部也制定了完善的性能与容量管理流程，通过提前识别资源需求以及对平台资源容量和设备库存进行统筹管理，对资源使用率和资源可用性水平的不断优化，最终保证云资源满足用户的业务正常需求。</p>
第 6 条	补丁 和漏 洞管 理	确保云环境中所有资产都有明确的所有权，并对其重要性进行评级。快速识别潜在的漏洞和系统不稳定性并快速安全地部署安全和操作系统补丁。	客户应建立正式的资产管理程序，对其资产进行分类，并定义资产所有者，以便快速识别资产的漏洞并进行修复。同时，华为云也建立了完善的漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。对于涉及云平台、租户服务等的漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，向最终用户/租户及时推送漏洞规避和修复方案和建议，与租户共同面对安全漏洞带来的挑战。
第 7 条	合作 的灾 难恢 复测 试	金融机构应针对关键业务功能制定业务连续性计划并执行自己的模拟灾难恢复测试，尽可能与 CSP 联合进行测试。 CSP 应制定灾难恢复和业务连续性计划，并在适当的情况下与金融机构共	客户应建立自身的业务连续性机制，并制定保证其关键业务连续的 RTO、RPO 指标。 如果金融机构在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。 为配合客户满足合规要求，华为云除了提供高可用基础设施、冗余数据备份、可用区设备等外，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得 IS022301 认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测

原文 编号	控制 域	具体控制要求	华为云的应答
		享这些计划。确保服务的持续可用性与其在云环境中的关键程度相称。确保数据、系统和应用程序能够在金融机构要求的时间范围内恢复。	试，持续优化应急响应机制。

10

华为云如何符合 MAS《业务连续性管理指南》的要求

新加坡金融管理局（MAS）于 2022 年 6 月 6 日发布了《业务连续性管理指南》，为新加坡金融机构加强业务连续性管理提供指导，旨在帮助金融机构增强抵御服务中断的能力，最大限度地减少服务中断所造成的影响。《业务连续性管理指南》的要求覆盖了关键业务服务和职能、服务恢复时间目标、依赖关系映射、集中风险、持续审视和改进、测试、审计以及事件和危机管理等领域。

以下内容总结了《业务连续性管理指南》中与云服务供应商相关的合规要求条款，并阐述华为云是如何帮助金融机构满足其要求。

10.1 关键业务服务和职能

《业务连续性管理指南》指出业务职能是向金融机构客户提供业务服务的基础，当业务职能中断时，所有依赖它的业务服务都可能中断。该指南第二部分针对关键业务服务和职能提出了具体控制要求，以便能够促使金融机构在发生中断时尽快确认并恢复其关键业务服务和职能。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
2.2	业务连续性及灾难恢复计划管理	金融机构应根据其业务服务和职能的重要性确定其恢复的优先次序，并确定适当的恢复战略和资源分配。	客户应确定关键业务服务和职能的恢复优先级并合理分配资源。 为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。在该体系框架的要求下，华为云会定期开展业务影响分析，识别关键业务，确定关键业务的恢复目标、最小恢复水平和恢复优先级，确定恢复所需的相关支持资源。此外，华为云还将识别中断对于组织所带来的风险并进行系统分析，确认风险处置措施。基于业务影响分析与风险评估的结

			果，华为云将会制定关键业务流程的各关键资源（包括人员、场地、设备、第三方、信息系统）的适当的恢复策略。
--	--	--	---

10.2 服务恢复时间目标

《业务连续性管理指南》指出服务恢复时间目标能够为金融机构提供预计的业务服务的恢复时间。该指南第三部分针对服务恢复时间目标的确定提出了具体控制要求，这将有助于确定资源的优先级并监测中断的恢复进度。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 3.2	业务连续性及灾难恢复计划管理	金融机构应建立自身的业务连续性机制，并制定保证其关键业务连续的 RTO、RPO 指标。	客户应建立业务连续性机制，并保障 RTO 与 RPO 的实现。 华为云遵循 ISO22301 业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。在该体系框架的要求下，华为云会定期开展业务影响分析，识别关键业务，确定关键业务的恢复时间目标与恢复点目标以及最小恢复水平。在识别关键业务的过程中，华为云将业务中断对客户的影响程度作为判断关键业务的一个重要标准。
3.3	业务连续性及灾难恢复计划管理	当金融机构的关键业务服务遇到部分中断时，金融机构应为明确其业务连续性计划的启动标准及恢复标准，以在中断发生时及时的启动业务连续性计划。	客户应明确发生关键业务部分中断时其业务连续性计划的启动标准与恢复标准。 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，华为云制定了突发事件分级标准，确定了突发事件的各等级定义以及判断事例。华为云将突发事件分为重大、较大和一般等级。其中，一般等级安全事件涵盖了部分中断的情况，例如一般性系统故障，但不影响整体系统运行，仅对业务或功能有轻微影响。针对不同级别的突发事件，华为云明确了相应的风险容忍度与处置措施，以规避、降低或转移突发事件所带来的风险，保障华为云

		业务的连续性。
--	--	---------

10.3 依赖映射关系

《业务连续性管理指南》指出随着对 IT 系统和第三方的依赖不断增加，金融行业的相互关联性也日益增强。为减轻此类联系所产生的风险，同时保障金融机构的业务连续性，该指南第四部分针对金融机构与第三方的联系提出了具体控制要求。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
4.4	业务连续性及灾难恢复计划管理	<p>金融机构应采取措施，使第三方能够满足其关键业务服务的 SRTO，如：</p> <p>(a) 与第三方制定并定期审查业务水平或服务水平协议；</p> <p>(b) 审查第三方的业务连续性计划；</p> <p>(c) 与第三方作出安排，以保障资源的供应；</p> <p>(d) 对第三方进行审计；</p> <p>(e) 与第三方进行联合测试。</p>	<p>客户应通过采取有效措施使第三方能够满足关键业务服务的 SRTO。</p> <p>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。华为云会遵从与客户订立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。如果金融机构在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。</p>
4.5	业务连续性及灾难恢复计划管理	金融机构应制定计划和程序，以解决第三方所导致的任何不可预见的中断、失败或终止。	<p>客户应制定有效的业务连续性计划，以解决针对第三方所导致的服务中断。</p> <p>为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。在该体系框架的要求下，华为云会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）以及不同场景的应急预案并进行演练，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。</p>
4.6	业务连续性及灾	金融机构应实施冗余	客户应采取适当措施解决支持关

	难恢复计划管理或替代应急安排解决支持关键业务服务的共同公用事业服务的中断问题。	键业务服务的共同公用事业服务的中断问题。华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。 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，系统在遵从监管要求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。此外，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云向客户提供存储容灾服务（SDRS - Storage Disaster Recovery Service）为弹性云服务器、云硬盘和专属分布式存储（DSS -Dedicated Distributed Storage Service）等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。
--	---	---

10.4 集中风险

《业务连续性管理指南》指出当多项关键业务服务和/或职能外包给同一个服务提供商时，金融机构可能面临集中风险。为减轻集中风险，该指南第五部分提出了具体控制要求。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
5.2	云服务安全	金融机构可考虑采取将关键业务服务和职能的主从站点或基础设施（如数据中心）分开到不同的区域，以降低集中风险，并在发生中断时减少影响。	<p>华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。</p> <p>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，系统在遵从监管要求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。此外，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云向客户提供存储容灾服务（SDRS - Storage Disaster Recovery Service）为弹性云服务器、云硬盘和专属分布式存储（DSS - Dedicated Distributed Storage Service）等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间</p>

			从另外的位置启动并正常运行，从而提升业务连续性。
--	--	--	--------------------------

10.5 持续审视与改进

《业务连续性管理指南》指出业务连续性管理是一项持续努力，以确保所采取的措施能够应对最新威胁以及未来潜在威胁所造成的风险。该指南第六部分针对金融机构持续审视和改进自身业务连续性提出了多项具体控制要求。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	业务连续性及灾难恢复计划管理	金融机构应建立自身的业务连续性机制，并制定保证其关键业务连续的 RTO、RPO 指标。定期测试和评估业务连续性计划和灾难恢复计划。	客户应建立业务连续性机制，明确 RTO、RPO 指标，并对业务连续性计划与灾难恢复计划进行定期测试。 华为云拥有完善的业务连续性管理策略和流程，制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。为确保业务连续性的适宜性、充分性和有效性，华为云定期对其业务连续性体系进行审查以对其程序和能力进行评价。华为云会对审查中发现的不足进行纠正，对其进行记录、分析以及改进，并且基于审查的结果对业务连续性计划进行更新，以确保业务连续性计划持续有效。
6.3	安全监控	金融机构应多渠道收集和分析网络威胁情报，识别和检测对其正常运营造成影响的外部威胁，并及时向利益相关方通报相关威胁。	客户应通过不同渠道收集和分析威胁情报，识别和检测外部威胁并进行通报。 华为云持续关注业界知名漏洞库、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华为云相关的漏洞信息。同时，华为云通过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，结合大数据分析、高准确度的威胁情报库，“实时监控”云上威胁，分析威胁攻击情况，及时提供告警通知，并可针对典型威胁事件预置响应策略。 华为云制定和实施了安全事件的定级标准与升级流程。一方面，

			<p>华为云对安全事件进行了清晰的等级划分，并明确了各等级安全事件的定义。另一方面，若发生安全事件，华为云会获取相关信息并依据定级标准进行定级。如在处理过程在安全事件达成更高一级的定级标准，华为云将实时刷新定级，并依照公司规定作出相应处置。</p> <p>此外，华为云还明确了不同级别的安全事件所对应的通报时间与通报范围等要求。发生安全事件时，华为云会依照公司有关要求，在规定时间内，向公司内部有关责任人以及管理人员通报安全事件有关情况。</p>
6.5	业务连续性及灾难恢复计划管理	金融机构应定期测试和评估业务连续性计划，并从事件中吸取教训，以加强其业务连续性准备。	<p>客户应定期评估和测试业务连续性计划并改进。</p> <p>华为云拥有完善的业务连续性管理策略和流程，制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。为确保业务连续性的适宜性、充分性和有效性，华为云定期对其业务连续性体系进行审查以对其程序和能力进行评价。华为云会对审查中发现的不足进行纠正，对其进行记录、分析以及改进，并且基于审查的结果对业务连续性计划进行更新，以确保业务连续性计划持续有效。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，找出根本原因并制定解决方案从根源上杜绝该类事件的发生。</p>
6.7	业务连续性及灾难恢复计划管理	金融机构应定期测试和评估业务连续性计划和灾难恢复计划，并根据其运营环境和威胁形势的变化进行适当的更新。	<p>客户应定期测试和评估业务连续计划和灾难恢复计划并改进。</p> <p>华为云拥有完善的业务连续性管理策略和流程，制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。为确保业务连续性的适宜性、充分性和有效性，华为云定期对其业务连续性体系进行审查以对其程序和能力进行评价。华为云会对审查中发现的不足进行纠正，对其进行记录、分析以及改进，</p>

		并且基于审查的结果对业务连续性计划进行更新，以确保业务连续性计划持续有效。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本上杜绝该类事件的发生。
--	--	---

10.6 测试

《业务连续性管理指南》指出测试对于验证金融机构的业务连续性管理的有效性至关重要。为指导金融机构对业务连续性开展测试，该指南第七部分提出了多项具体控制要求。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	业务连续性及灾难恢复计划管理	金融机构应定期对其业务连续性计划进行全面测试，以确保其响应和恢复安排的可靠性，并使其能够在中断后及时继续提供关键业务服务。	客户应定期测试业务连续性计划确保其有效性。 为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。华为云会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）以及不同场景的应急预案并进行演练，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。
7.2	业务连续性及灾难恢复计划管理	金融机构应规划其测试活动，以有意义地测试其业务连续性管理框架的所有方面，并实现以下测试目标： (a) 使用适当的衡量标准验证和衡量 BCP 的有效性，并补救恢复过程中发现的任何差距或弱点； (b) 使参与业务连续性和危机管理的人员，包括相关第三方的人员熟悉其作用和责任； (c) 使参与危机管理的高级管理层和工作人员了解危机局势中可能出现的潜在关切领域，并练习在模拟	

		条件下作出决定; (d) 在严重但合理的情况下对 BCP 进行压力测试, 使 FI 能够挑战其目前的规划假设, 确保其 BCP 的相关性和有效性; 以及 (e) 核实是否可以通过既定的恢复战略满足其关键业务服务的 SRTO 和其关键业务职能的 RTO。	
7.3	业务连续性及灾难恢复计划管理	金融机构应定期测试和评估业务连续性计划和灾难恢复计划, 根据不同的业务服务和职能明确其测试的频率和范围, 并保留测试记录。业务连续性测试中发现的差距和弱点应报告给最高管理层。	
7.4	业务连续性及灾难恢复计划管理	金融机构应建立一个正式的程序, 以跟进和记录每次测试中确定的补救行动。	客户应跟进和记录针对业务连续性计划的补救活动。 华为云拥有完善的业务连续性管理策略和流程, 制定了符合自身业务特色的业务连续性管理体系, 并已获得 ISO 22301 认证。为确保业务连续性的适宜性、充分性和有效性, 华为云定期对其业务连续性体系进行审查以对其程序和能力进行评价。华为云会对审查中发现的不足进行纠正, 对其进行记录、分析以及改进, 并且基于审查的结果对业务连续性计划进行更新, 以确保业务连续性计划持续有效。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。

10.7 审计

《业务连续性管理指南》指出业务连续性审计是独立评估金融机构业务连续性管理框架执行的充分性和有效性的重要手段。该指南第八部分针对审计金融机构的业务连续性提出了多项具体控制要求。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
8.2	评估与审计	金融机构应至少每三年审计一次其整体业务连续性管理框架和其每项关键业务服务的业务连续性管理。	客户应定期（至少每三年一次）审计其业务连续性管理框架及相关工作。 华为云拥有完善的业务连续性管理策略和流程，制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。为确保业务连续性的适宜性、充分性和有效性，华为云定期对其业务连续性体系进行审查以对其程序和能力进行评价。华为云会对审查中发现的不足进行纠正，对其进行记录、分析以及改进，并且基于审查的结果对业务连续性计划进行更新，以确保业务连续性计划持续有效。此外，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。
8.4	业务连续性及灾难恢复计划管理	金融机构应建立一个正式的程序，以跟进和记录补救行动的执行情况。金融机构应将对其业务连续性管理产生重大影响的审计结果上报至管理层，并根据 MAS 的要求提交审计报告。	客户应跟进和补救针对业务连续性计划的补救活动。此外，客户还应将对其业务连续性管理产生重大影响的审计结果上报至管理层，并根据 MAS 的要求提交审计报告。 华为云拥有完善的业务连续性管理策略和流程，制定了符合自身业务特色的业务连续性管理体系，并已获得 ISO 22301 认证。为确保业务连续性的适宜性、充分性和有效性，华为云定期对其业务连续性体系进行审查以对其程序和能力进行评价。华为云会对审查中发现的不足进行纠正，对其进行记录、分析以及改进，并且基于审查的结果对业务连续性计划进行更新，以确保业务连续性计划持续有效。

10.8 事件与危机管理

《业务连续性管理指南》对事件与危机管理的规范是保障金融机构的业务连续性的重要方面。《业务连续性管理指南》第九部分针对金融机构开展事件和危机管理管理提出了多项具体控制要求。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
9.1	安全事件响应	金融机构应建立事件管理流程，以便在规定的 SRTO/RTO 内恢复关键业务服务和职能。若业务服务的交付依赖于多个业务职能，则应任命一位总协调员。	客户应建立完善的安全事件管理流程。 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。根据内部管理的要求，华为云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。
9.2	安全事件响应	金融机构应制定危机管理活动，如： (a) 危机管理结构，明确界定作用、责任、报告关系和指挥系统； (b) 一套预先确定的及时启动危机管理结构的触发因素和标准； (c) 指导 FI 在危机期间采取的行动和决定的计划和程序； (d) 工具和程序，以便利及时更新和评估最新局势，以支持危机期间的决策； (e) 关键业务服务中断时要通知的所有内部和外部利益相关者的名单，以及每个利益相关者的沟通计划和要求；以及 (f) 沟通渠道，包括主流和社交媒体，与利益相关者有效沟	客户应开展有效的危机管理活动。 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。根据内部管理的要求，华为云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。 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。该系统统一收集物理设备、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

		<p>通，包括在主要沟通渠道不可用时可使用的替代渠道。</p>	<p>定解决方案从根源上杜绝该类事件的发生。</p> <p>华为云会对应急处置中所有相关的信息和处理过程进行严格记录，所有过程资料应由专人存档保管。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。</p> <p>华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。</p>
9.4	安全事件响应	<p>金融机构应确保与外部利益相关者进行积极主动的沟通，在中断或危机期间保持客户信心。</p>	<p>客户应与外部利益相关者开展积极主动的沟通。</p> <p>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。华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。</p>

9.5	安全事件响应	金融机构应制定内外部沟通计划，明确在发生中断时可立即发布声明。同时应确保能够与相关行业协会保持良好和充分的沟通，在发生中断时可以对公共提供一致的信息。金融机构应指定一位发言人，负责向媒体和公众发表讲话。	客户应制定有效的内外部沟通计划，同时与各利益相关方保持良好与充分沟通。此外，客户还应指定负责对外发表讲话的发言人。 华为云按照政策要求，在公司内部与外部间建立了多条信息沟通渠道，以确保华为云在内部员工之间，以及华为云内外部云服务客户间的有效沟通。华为云确保网络安全保障体系在各体系、各区域、全流程的实施，积极推动与政府、客户、合作伙伴、员工等各利益相关方的沟通，以确保利益相关方能及时有效地接收到的华为云网络安全有关信息。为促进与外部的顺畅沟通，华为云配备专人与行政机构、风险和合规组织、地方当局和监管机构保持联系并建立联络点。与外部利益相关者紧密合作，共享信息，以期推动网络安全领域的进步。
9.6	安全事件响应	金融机构应确保尽快按照 MAS 事件报告模板通知 MAS，不迟于发现业务运营将严重中断的事件后的一小时，或 BCP 将被激活以响应事件。	客户应在规定时间内向监管机构通报安全事件相关情况。 为配合客户满足网络安全事件上报 MAS，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。

11 华为云如何符合 MAS《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》的要求

新加坡金融管理局（MAS）于 2021 年 6 月 1 日发布了《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》，强调了金融机构在采用公有云服务前应考虑的一些常见的关键风险和控制措施。为金融机构更加安全地使用公有云服务，降低相关风险提供了指导。

以下内容总结了《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》中与云服务供应商相关的合规要求条款，并阐述华为云是如何帮助金融机构满足其要求。

11.1 共同承担网络安全责任

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》以公有云服务下的网络安全责任划分为关注点，指出在公有云服务中，金融机构与云服务提供商各自应承担的责任。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	合同协议	<p>云服务提供商负责“云安全”，而金融机构则负责“云端安全”：</p> <p>a) “云安全”是指由 CSP 负责的公有云服务的安全。在 IaaS 或 PaaS 安排中，通常包括底层硬件、系统软件和管理程序的安全。对于 SaaS，还包括应用软件的底层安全；</p> <p>b) “云端安全”是指由金融机构负责的云工作负载的安全。在 IaaS 或 PaaS 安排中，通常应包括确保应用程序、操作系统和协调工具等 IT 系统组件的安全。在 SaaS 安排中，一般包括管理用户账户权限和数据访问权限。</p>	<p>客户应明确其与云服务供应商等相关方的网络安全责任。</p> <p>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（可见本遵从性指南中的“3. 华为云安全责任共担模型”）。此外，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》。</p> <p>为配合客户满足合规要求并行使对云服务供应商的监管，华为云线上的《华为云用户协议》对客</p>

8	合同协议	金融机构应该意识到，虽然CSP负责“云安全”，但在某些情况下，金融机构可能要分担管理CSP实施的控制措施的责任。	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，在其中与客户共同约定相应要求。如有必要，华为云会积极配合客户方发起的尽职调查。
9	合同协议	金融机构确保在与云服务供应商签订的外包协议中明确规定所有合同方的网络安全责任。	华为云会安排专人积极配合金融机构的尽职调查。客户以及其监管机构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约定。此外，华为云每年会聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计，并且会按照外包服务供应商审计报告(OSPAR)模板中规定的格式发布审计报告，在报告形成后，华为云将根据内部流程向金融行业客户发布审计报告的副本。

11.2 身份访问管理

为有效管理云安全风险，《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》建议金融机构实施身份访问管理，并为此提出了多项具体要求，以规范身份访问管理机制。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
10	身份与访问管理	金融机构在授予公有云中的信息资产访问权限时应严格执行最小特权原则。	客户应建立信息系统的身份认证与访问控制管理机制，对访问系统的行为进行权限限制和监督。同时，在授予针对公有云中的信息资产访问权限时，严格执行最小特权原则。
11	身份与访问管理	金融机构应对拥有特权的员工实施多因素身份验证。	客户可通过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
13	身份与访问管理	若将公有云工作负载与内部部署身份验证服务集成在一起，金融机构应采用最佳实践措施来确保此类实施的安全，以最大限度地降低传染风险。	

		<p>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。此外，华为云的云审计服务（Cloud Trace Service，简称 CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。</p> <p>为配合客户满足合规要求，华为云内部建立了完善的运维和运营账号管理机制。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。华为云相关系统的管理员登录系统时必须先经过双因子认证后，才能通过跳板机接入管理平面。所有操作都会记录日志并及时传送到集中日志审计系统。该审计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。而且华为云有专门的内审部门，会定期对运维流程各项活动进行审计。</p> <p>华为云所有运维账号由 LDAP 集中管理，通过统一运维审计平台集中监控并进行自动审计，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，并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理，保证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。</p> <p>此外，华为云建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循和授予的。堡垒主机提供基于密码和邮箱验证码的双因素身份验证功能，以验证用户的身份。用户通过互联网访问华为云办公子网，需要根据注册设备及其账号和密码进行双因素认</p>
--	--	--

			证。
12	证书与密钥管理	系统/应用服务用于公有云身份验证的凭证应定期更改。如果不使用凭据，应立即删除	<p>客户需对用于身份验证凭证进行定期更改或删除。</p> <p>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。</p> <p>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。</p> <p>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验证码进行二次认证。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。</p> <p>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 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。</p>
14	网络安全架构	使用多种公有云服务的金融机构可能需要对使用不同公有云服务的安全策略进行集中管理，并确保这些策略得到一致	<p>当使用多种公有云服务时，客户应对使用云服务的安全策略进行统一管理并确保其有效落实。</p> <p>为了检测和拦截来自 Internet 的</p>

		<p>的执行。</p> <p>攻击以及租户虚拟网络之间的东向攻击，华为云的网络中部署了网络 IPS 设备，包括但不限于面向公众的网络边界、安全区域信任边界、租户空间边界。华为云的 IPS 可以实时分析网络流量，触发对协议攻击、暴力破解、端口和漏洞扫描、病毒和木马攻击、针对特定漏洞的攻击等各种入侵的拦截。</p> <p>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（VPC - Virtual Private Cloud）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。</p>
--	--	---

11.3 保护公有云中的应用程序

公有云中应用程序的安全是本文件的关注点之一。《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》围绕着如何保护公有云中的应用程序的安全，提出了多项建议。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
16	开发过程安全	<p>在针对公有云环境开发应用程序时，金融机构应采用适当的安全软件开发生命周期（SSDLC）流程，进行稳健的威胁建模，并实施软件安全方面的现行最佳做法。如果金融机构使用 DevOps 流程，则应将安全嵌入到整个持续集成/持续开发（CI/CD）工具链中。金融机构应采用 DevSecOps，即在软件开发流程中自动集成 IT 运营、质量保证和安全实践的做法。</p>	<p>客户应采用适当的安全软件开发生命周期（SSDLC）流程并建立 DevSecOps 管理机制。</p> <p>华为云追求新的 DevOps 流程，具有快速持续迭代能力，集成了华为安全开发生命周期(SDL)。此外，逐步形成高度自动化的新安全生命周期管理方法和流程，称为 DevSecOps，与云安全工程能力和工具链一起确保 DevSecOps 的顺利灵活实施。华为云对开发环境进行分层管理，并实施物理隔离、逻辑隔离、访问控制、数据传输通道审批和审</p>

			计等保护措施。
17	身份与访问管理	当采用微服务架构时，金融机构应该确保适当的安全控制落实到位，包括使用服务网格对 API 进行细粒度访问控制，以及为微服务实现有效的身份验证等。	<p>客户应实施有效的安全控制措施，以确保在采用微服务架构时的安全性。</p> <p>为了检测和拦截来自 Internet 的攻击以及租户虚拟网络之间的东西向攻击，华为云的网络中部署了网络 IPS 设备，包括但不限于面向公众的网络边界、安全区域信任边界、租户空间边界。华为云的 IPS 可以实时分析网络流量，触发对协议攻击、暴力破解、端口和漏洞扫描、病毒和木马攻击、针对特定漏洞的攻击等各种入侵的拦截。</p> <p>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（VPC - Virtual Private Cloud）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。</p>
18	身份与访问管理	在确保 API 的安全时，金融机构应实施细粒度访问控制，并采用最小特权原则，即严格限制对服务的访问，只允许访问所需的服务，并授予所需的最低权限。金融机构还应实施强大的 IAM 来验证服务请求。金融机构在授予访问权限时不应依赖隐式信任（例如，根据请求者的静态 IP 地址允许访问）。	<p>客户可通过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。此外，华为云的云审计服务（Cloud Trace Service，简称 CTS），可提供对</p>

		<p>各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。</p> <p>为配合客户满足合规要求，华为云内部建立了完善的运维和运营账号管理机制。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。华为云相关系统的管理员登录系统时必须先经过双因子认证后，才能通过跳板机接入管理平面。所有操作都会记录日志并及时传送到集中日志审计系统。该审计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。而且华为云有专门的内审部门，会定期对运维流程各项活动进行审计。</p> <p>华为云所有运维账号由 LDAP 集中管理，通过统一运维审计平台集中监控并进行自动审计，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，并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理，保证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。</p> <p>此外，华为云建立了一系列分层认证体系要求，包括对内部 IT 环境、系统平台、中间件、网络设备、应用系统以及相关的技术要求。所有访问都是基于最小权限概念遵循和授予的。堡垒主机提供基于密码和邮箱验证码的双因素身份验证功能，以验证用户的身份。用户通过互联网访问华为云办公子网，需要根据注册设备及其账号和密码进行双因素认证。</p>
--	--	---

11.4 数据安全和加密密钥管理

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》从数据安全以及加密密钥的管理着手，建议金融机构采取适当的数据安全保护措施，同时加强对加密密钥的管理。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
21	数据安全	<p>金融机构应实施适当的数据安全措施，保护公有云中敏感数据的保密性和完整性，同时考虑到静态数据、动态数据和使用中的数据（如适用）。</p> <p>a)对于静态数据，即云存储中的数据，金融机构除了在平台层面提供的加密之外，还可以实施其他措施，例如数据对象加密、文件加密或令牌化。</p> <p>b)对于动态数据，即往返于公有云以及在公有云内部的数据，金融机构除了在平台级别提供加密之外，还可以实施会话加密或数据对象加密。</p> <p>c)对于使用中的数据，即正在公有云中使用或处理的数据，金融机构可以实施云计算服务提供商提供的保密计算解决方案。机密计算解决方案在处理过程中将敏感数据隔离在一个受保护的、基于硬件的计算环境中，从而保护数据。</p>	<p>客户应实施适当的数据安全措施，在使用加密措施保护数据时，还应考虑采用业内认可的加密算法和密钥管理机制。此外，客户可以在硬件安全模块中管理密钥，并将其托管在安全环境中。客户还应确保加密密钥服务提供商的加密密钥管理政策、标准和程序能够充分保护密钥的安全。</p> <p>华为云将复杂的数据加解密、密钥管理逻辑进行封装。目前，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，采用高强度的算法对存储的数据进行加密。</p> <p>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。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业</p>
22	证书与密钥管理	金融机构应考虑采用加密密钥管理策略，对用于加密敏感数据的加密密钥进行高度控制和保护。	
23	证书与密钥管理	为确保用于加密敏感数据的加密密钥的安全，金融机构可考虑在硬件安全模块（HSM）中生成、存储和管理密钥，并将 HSM 托管在金融机构可控制程度较高的环境中。	
24	证书与密钥管理	金融机构应确保加密密钥服务提供商的加密密钥管理政策、标准和程序足以在加密密钥管理的整个生命周期内保护密钥免遭未经授权的访问、使用和	

		披露。	务的无缝集成、对接。
--	--	-----	------------

11.5 不可变工作负载和基础设施即代码

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》围绕使用不可变工作负载以及使用“基础设施即代码”来配置或管理金融机构在公有云中的工作负载提出了多项建议。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
25	虚拟化安全能力	金融机构可考虑使用不可变工作负载，以确保工作负载组件的安全性和稳定性，尤其是在软件升级或打安全补丁期间。对于不可变工作负载，服务器实例会被替换为更新的映像，而不是被更改。如果服务器实例受到威胁，可以迅速用干净的镜像替换。应在不可变工作负载镜像上进行测试，以确保镜像安全稳定，然后再在生产环境中实施。	客户可通过使用不可变工作负载，以维护工作负载相关组件的安全性与稳定性。 为配合客户遵从监管要求，华为云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。
26	安全配置管理	使用“基础设施即代码”来配置或管理公有云工作负载的金融机构应实施必要的控制措施，以最大限度地降低配置错误的风险。此外，金融机构还应确保相关配置文件不受未经授权的访问和修改。	当通过“基础设施即代码”开展配置或管理在云中的工作负载时，客户应实施适当的控制措施，保障配置的安全性，降低相关风险。 华为云目前已建立运维配置管理流程指导，通过对运维配置项及关联关系的生命周期管理，确保运维流程中的配置项被正确地识别并记录，以提供准确、可靠的配置信息，支撑运维业务安全、稳定、高效运作。 华为云对支撑业务运营的服务器操作系统、数据库管理系统及网络设备建立了统一的基线配置标准，以实现对服务基线配置的统一管理。此外，华为云构建了配置监控平台，实现对服务器操作系统、数据库管理系统及网络设备的配置项进行实时监控。配置监控平台会将实际的配置项同标准配置基线进行对比。当出现差

		异时，差异分析结果会通过邮件自动发送至巡检管理员进行后续跟进处理。此外，华为云会基于现有的防火墙配置策略与现网实施情况定期执行一致性审视，对识别出的差异项进行修复。
--	--	--

11.6 网络安全运营

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》为金融机构开展网络安全的日常运营工作提出了多项建议。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
27	安全监控	为保持对信息资产的整体网络态势感知，金融机构应避免孤立地对内部部署应用程序或基础设施以及公有云工作负载进行安全监控。金融机构应将公有云工作负载的网络相关信息反馈到各自的企业级 IT 安全监控服务中，以促进对网络事件的持续监控和分析。	<p>客户应建立集中的监控平台对各个系统的安全日志进行自动分析，及时检测和响应安全事态和事件。</p> <p>为配合客户满足合规要求，华为云有集中、完整的日志审计系统。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。华为云日志管理系统是基于 ELK 建立的。华为云使用大数据安全分析系统，关联各种安全设备的告警日志，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。</p> <p>华为云提供关系型数据库服务，是一款允许租户快速发放不同类型数据库，并可根据业务需要对计算资源和存储资源进行弹性扩容的数据库服务。其提供自动备份、数据库快照、数据库恢复等功能，以防止数据丢失。</p>
28	安全事件响应	金融机构还应确保其事件响应、处理和调查流程适合公有云工作负载。	<p>客户应建立适当的事件管理程序，及时解决系统和网络故障。</p> <p>华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的重大事件管理。华为云拥有集中、完整的日志审计系统。并利用大数据安全分析系统，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</p>

		预判尚未发生的威胁。华为云拥有专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的重大事件。并根据事件的实时状态进行事件升级和通报。
--	--	--

11.7 云韧性风险管理

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》建议金融机构评估和监控在云服务的韧性方面的情况，并采取适当措施确保云服务的韧性。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
29	云基础架构安全	金融机构应评估云服务供应商在维护其公有云服务韧性方面的跟踪记录，以验证这些记录是否与金融机构的业务需求相称。此类评估应在聘请云服务供应商服务之前进行，并在聘请云服务供应商后定期进行。	客户应定期评估云服务提供商在维护其公有云服务韧性方面的跟踪记录。华为云会安排专人积极配合金融机构的监督与调查。同时，客户还应确保云服务供应商具有适当的云冗余或容错能力。 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韧性和可用性，数据中心按规则部署在全球各地，客户可通过两地互为冗余，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，保证业务的持续运行。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。
30	云基础架构安全	对于需要高可用性的云工作负载，金融机构有责任确保云服务供应商具有适当的云冗余或容错能力，并为云工作负载启用适当的功能。云工作负载也可部署在多个地理位置分离的数据中心，以减少可能会干扰公有云服务交付的特定位置问题。	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韧性和可用性，数据中心按规则部署在全球各地，客户可通过两地互为冗余，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，保证业务的持续运行。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。
31	安全监控	金融机构应主动监察云服务供应商公布的维修计划、服务中断、服务变更和服务终止，以便能够及时采取措施，确保金融机构的系统继续可用。	客户应积极监控云服务供应商公布的服务中断等信息，以便能够采取适当的应对措施。此外，客户还应建立集中的监控平台对各个系统的安全日志进行自动分析，及时检测和响应安全事态和事件。 客户可通过华为云官网来了解华为云提供的云服务的相关信息。

		<p>华为云对外提供了统一的电话热线、邮箱地址以及工单系统处理金融机构的服务请求。华为云也会建立与相关监管机构的联系，以便必要的沟通。</p> <p>为配合客户满足合规要求，华为云有集中、完整的日志审计系统。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。华为云日志管理系统是基于 ELK 建立的。华为云使用大数据安全分析系统，关联各种安全设备的告警日志，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。</p> <p>华为云的云监控服务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，以便用户及时检测云资源的异常并采取应对措施。</p>
--	--	--

11.8 云服务提供商的外包尽职调查

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》针对金融机构对于云服务提供商开展的尽职调查提出多项建议。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
32	合同协议	部分云服务提供商可能向使用公有云服务的金融机构提供为定制的合同条款和条件，使金融机构能够更好地满足其外包尽职调查、风险管理及监管合规需求。这些条款和条件可能包括授予金融机构及其监管机构审计和信息访问权，以执行外包尽职调查和进行监管审查。在考虑云外包安排时，金融机构应确保其管理风险和满足监管要求/期望的能力不受合同条款和条件的阻碍。	客户应与云服务提供商签订外包协议，并在其中明确规定授予金融机构及其监管机构审计和信息访问权等要求。 为配合客户行使对云服务供应商的监管，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，在其中与客户共同约定相应要求。

			华为云会安排专人积极配合金融机构的尽职调查。客户以及其监管机构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约定。
33	评估与审计	金融机构应确保对云外包安排进行独立审计和/或专家评估，作为其外包尽职调查和风险管理的一部分。	<p>客户应对云外包安排进行独立审计和/或专家评估。</p> <p>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。此外，华为云目前已获得多项国际上权威的安全与合规认证。华为云每年会聘请专业的第三方审计机构对华为云提供的云计算产品和服务进行审计。</p>

11.9 供应商锁定和集中风险管理

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》针对降低供应商集中所带来的风险为金融机构提出多项建议。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
35	合同协议	对于对金融机构至关重要的云工作负载，金融机构应制定退出战略。退出战略可考虑相关的风险指标、退出触发器、退出情景、数据的可移植性和可能的迁移选项。	<p>客户应制定云服务外包的退出计划。</p> <p>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。</p> <p>在服务协议终止时，华为云提供的云数据迁移服务（CDM），支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。</p>

11.10 技能

《针对如何应对与采用公有云有关的技术和网络安全风险的咨询意见》针对金融机构员工所掌握的专业知识和技能方面提出建议。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
37	人员安全管理	金融机构应确保员工具备必要的知识和技能，了解和管理采用公有云的风险，同时能够管理其组织中使用的不同云服务的相关技术和网络风险。	客户应确保员工具备处理公有云风险的知识和技能。 华为云为确保员工的信息安全意识能够符合公司要求建立了一系列的网络安全培训及学习机制，要求员工持续学习网络安全知识，了解相关的政策和制度，了解哪些该做哪些不该做，承诺按要求执行。

12 结语

本文描述了华为云如何为客户提供符合新加坡金融行业监管要求的云服务，并表明华为云遵守新加坡金融监管局（MAS）以及新加坡银行协会（ABS）发布的重点监管要求，有助于客户详细了解华为云对于新加坡金融行业监管要求方面的合规性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合新加坡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新加坡金融行业监管要求的遵从性。

13 版本历史

日期	版本	描述
2024 年 1 月	3.0	合规要求更新
2022 年 4 月	2.0	合规要求更新
2021 年 3 月	1.1	合规要求更新
2019 年 11 月	1.0	首次发布