华为云新加坡金融行业监管要求合规性说明

文档版本 02

发布日期 2021-03-11

HUAWEI

华为技术有限公司

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

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.....4
4 华为云全球基础设施.....5
5 华为云如何符合 MAS《外包指南》的要求.....6
5.1 风险管理实践.....6
5.2 云计算.....10
6 华为云如何符合 MAS《科技风险管理指南》的要求.....12
6.1 董事会和高级管理层对科技风险的监管.....12
6.2 IT 外包风险管理.....13
6.3 信息系统的获取和开发.....14
6.4 系统可靠性、可用性和可恢复性.....15
6.5 基础设施安全运营管理.....15
6.6 数据中心保护和控制.....16
6.7 访问控制.....16
7 华为云如何符合 MAS《关于网络卫生的通知》的要求.....18
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.....22
8.1 审计和检查.....22
8.2 实体级别控制.....24
8.3 通用 IT 控制.....27
8.4 服务控制.....32
9 华为云如何符合 ABS《ABS 云计算实施指南》的要求.....35
9.1 尽职调查建议的活动.....35
9.2 进入云外包安排时建议的控制措施.....38
10 结语.....49
11 版本历史.....50

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。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。

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[1]，全力保障客户部署业务的安全与合规，主要包括：

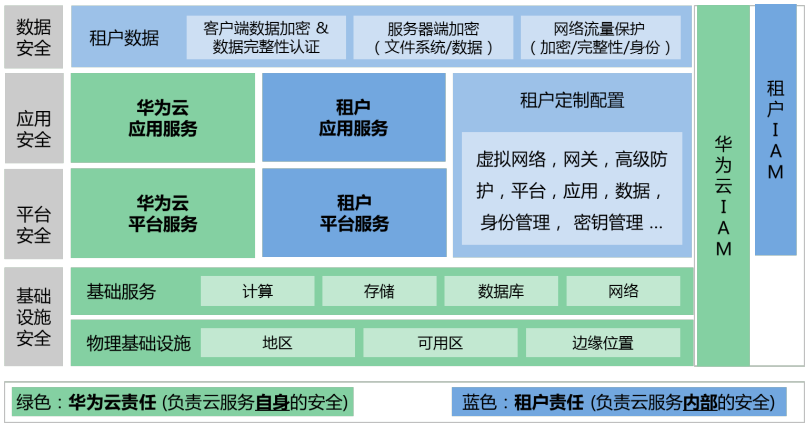
认证	描述
ISO 20000-1:2011	ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的IT服务来满足客户和业务的需求。
ISO 27001:2013	ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO 27017:2015	ISO 27017是针对云计算信息安全的国际认证。ISO 27017的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 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部控制情况出具的独立审计报告。

认证	描述
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ISO27701表明了其在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，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。

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，该指南主要覆盖了金融机构的风险管理实践和金融机构选择云服务供应商的指南及使用云服务的要求，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 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，覆盖董事会和高级管理层的职责、风险评估、对服务供应商的评估、外包协议、保密和安全、业务连续性管理、对外包安排的监控、审计和检查、新加坡境外外包、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	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。	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。

编号	控制域	具体控制要求	华为云的应答
5.4	服务供应商评估	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。	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。
5.5	外包协议	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障碍。	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》。

编号	控制域	具体控制要求	华为云的应答
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。	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。 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》。
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。	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。 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。

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	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。	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。
5.9	审计和检查	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。 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。	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。 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。

编号	控制域	具体控制要求	华为云的应答
5.10	新加坡境外外包	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息的服务供应商签订协议。	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。 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。 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。

5.2 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《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。《科技风险管理指南》的要求覆盖了董事会和高级管理层对技术风险的监管、 IT外包风险管理、信息系统的采购和开发、系统的可靠性、可用性和可恢复性、基础设施安全运营管理、数据中心保护和控制、访问控制等领域。

以下内容总结了《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 董事会和高级管理层对科技风险的监管

鉴于IT职能在支持金融机构业务方面的重要性，《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角色和责任、人员筛选、IT政策、标准和程序、IT安全意识。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
3.3	人员筛选	由于人员在IT环境中的系统和流程管理中扮演着重要角色，金融机构应实施全面有效的人员筛选流程。	客户应制定并实施人员筛选策略和程序。 华为云在聘用员工前会做充分的背景调查，背景调查的范围包括：犯罪记录、财务违规记录、不诚信记录、政府背景、制裁国家的从业经历、是否制裁国公民。同时为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。

3.4	IT安全意识	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 IT 外包风险管理

《科技风险管理指南》第五章要求金融机构对外包服务供应商进行尽职调查，并提出对云服务供应商的特殊考虑。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	尽职调查	金融机构在指定服务供应商之前，需要对其进行尽职调查，能证明其可行性、容量、可靠性、财务状况的信息，金融机构应确保所有关于缔约方的角色、关系、义务和责任的合同条款和条件均写明在书面协议中。 服务供应商应接受金融机构提出的各相关方查看其系统、运营、文档及设施的要求，金融机构应要求服务供应商就所提供服务的安全的充分性及合规性取得专家报告并定期监察和审阅。 金融机构应该要求服务供应商建立一个灾难恢复应急管理框架，该框架将明确记录、维护和测试应急计划和恢复流程的人员职责。并根据不断变化的技术条件和操作要求定期审查，更新和测试灾难恢复计划。	客户在指定服务供应商之前，应对其进行尽职调查，审查服务供应商的业务连续性机制是否满足业务需要，与供应商协商合同的内容并达成一致。 华为云会安排专人积极配合客户的尽职调查。华为云每年会聘请专业的外部资源进行SOC2鉴证。如果客户对用户协议有更多的需求，华为云会与客户商定，并尽力达成一致。 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。

编号	控制域	具体控制要求	华为云的应答
5.2	云计算	金融机构应该确保云服务供应商具备隔离并识别其客户数据和其他信息系统资产的能力。当与服务供应商签订的合同已到期或者在到期前，金融机构应有权删除或销毁存储在服务供应商的系统和备份系统中的数据。云服务供应商还需向金融机构证明在规定的恢复时间目标（RTO）内恢复外包的系统和IT服务的能力。	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。 客户可通过华为云的**备份归档解决方案**，最大程度保证灾难发生时数据的不丢失。同时，华为云制定了完备的灾难恢复计划，并定期对其进行测试。确保在灾难发生时云服务能持续运行。 关于数据隔离，华为云建议在数据生命周期的起始阶段就做好数据的区分和隔离，客户首先做好数据分类，并进行风险分析，再根据风险分析结果，明确防护数据的存储位置、存储服务和安全防护措施。当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，确保客户只能访问到自己的数据。在客户自建存储的场景下，例如在虚拟机实例上安装数据库软件时，建议客户利用华为云的**虚拟私有云（Virtual Private Cloud，简称VPC）**服务构建私有网络环境，通过子网规划、路由策略配置等进行网络区域划分，将存储放置在内部子网，并通过配置网络 ACL 和安全组规则对进出子网以及和虚拟机的网络流量进行严格的管控。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》。

6.3 信息系统的获取和开发

《科技风险管理指南》第六章要求金融机构对信息系统的获取和开发进行管理，识别在系统设计、开发和测试阶段的系统缺陷，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

6.2	安全需求测试	金融机构应该为单元测试、集成测试、系统测试和用户验收测试（UAT）维护单独的物理或逻辑环境，并密切监控供应商和开发人员对UAT环境的访问。	客户在部署开发环境、测试环境和生产环境时，应保证环境间物理和逻辑层面都实现隔离，并严格管理对环境的访问。 华为的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。

6.4 系统可靠性、可用性和可恢复性

《科技风险管理指南》第八章要求金融机构能够确保其系统的可用性，应实施并测试灾难恢复计划，以便最大限度地减少因严重事故而导致的系统和业务中断。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
8.3	灾难恢复测试	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。

6.5 基础设施安全运营管理

《科技风险管理指南》第九章对金融机构提出了关于基础设施安全运营管理方面的要求，涵盖数据防丢失、技术更新管理、网络和安全配置管理、漏洞评估和渗透测试、补丁管理、安全监控等方面，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	数据防丢失保护	金融机构应识别重要数据并采取适当措施，以发现和防止未经授权的访问、对机密信息的复制或传输。	客户应识别其重要数据并对其分级分类，以便采取适当的控制措施保障数据安全。华为云建议在数据生命周期的起始阶段就做好数据的区分和隔离，客户首先做好数据分类，并进行风险分析，再根据风险分析结果，明确数据的存储位置、存储服务和安全防护措施。更多详细信息请参见《华为云数据安全白皮书》。

6.6 数据中心保护和控制

《科技风险管理指南》第十章要求金融机构确保其数据中心的安全，主要包括威胁和漏洞风险评估、物理安全、数据中心韧性等方面，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
10.1	威胁和漏洞风险评估	金融机构应根据威胁的各种可能情况进行威胁和脆弱性风险评估，评估时应考虑数据中心的建筑结构、周边环境、数据中心基础设施、日常安全流程、关键系统以及物理和逻辑访问控制等因素。金融机构在选择数据中心供应商时，金融机构应获取并评估其数据中心的威胁和脆弱性风险评估（TVRA）报告，并确保TVRA报告是否是最新的，以及数据中心供应商是否致力于解决识别出的所有重大漏洞。	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。同时，华为云运维运营团队定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急响应等措施。同时，华为成立了华为产品安全事件响应团队（PSRIT），成为国际应急响应论坛 FIRST 成员之一，可及时获取业界最佳实践和安全信息。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。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。

6.7 访问控制

《科技风险管理指南》第十一章要求金融机构采取恰当的访问控制措施，包括用户访问管理及特权访问管理，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
11.1	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，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 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。
11.2	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。	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。 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。

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	金融机构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相关的每个特权账户均受到保护，以防止未经授权访问或使用该账户。	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。 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。 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。

编号	控制域	具体控制要求	华为云的应答
4.2	安全补丁	金融机构需建立漏洞管理流程并对所有系统实施控制措施，包括及时安装和更新安全补丁。银行需识别是否有补偿措施解决不能通过补丁修复的漏洞并建立控制措施。	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。 客户可通过华为云的**漏洞扫描服务（VSS - Vulnerability Scan Service）**实现Web漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测等功能，自动发现网站或服务器暴露在网络中的安全风险，以实现对其云上的业务进行多维度的安全检测。 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。
4.3	安全标准	金融机构需确保所有系统符合书面定义的安全配置基线，并需建立控制措施以减少系统不符合安全配置基线带来的风险。	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。 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。

编号	控制域	具体控制要求	华为云的应答
4.4	网络边界防御	金融机构需对网络边界流量实施严格管控，防止未经授权的网络流量。	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。 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	金融机构必须确保在每个系统上都可以实施一种或多种恶意软件防护措施，以减轻恶意软件感染的风险。	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。

编号	控制域	具体控制要求	华为云的应答
4.6	多因素认证	金融机构必须对以下账户进行多因素认证： 1. 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相关的所有特权账号，其中关键系统是指系统故障会对银行的运营造成重大破坏或会对为最终客户提供的服务产生重大影响的系统； 2. 可以访问客户信息的所有账户。 若金融机构在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。 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家在新加坡经营的商业银行进行过审计。	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		

编号	控制域	具体控制要求	华为云的应答
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。 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。	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		
V	汇报和处理控制缺失/控制目标的质量	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。 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。 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。	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。 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。
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。	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。 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。

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： ● 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。

编号	控制域	具体控制要求	华为云的应答
I.（c）	信息和沟通	外包服务供应商的内部控制信息和沟通部分应包括：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。	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。

编号	控制域	具体控制要求	华为云的应答
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。	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。
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 访问控制**”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
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

编号	控制域	具体控制要求	华为云的应答
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。	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
II.（c）	变更管理	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。 保证开发、测试、分级和生产环境的隔离。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。 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。	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。 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。 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。
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。	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。 为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。

编号	控制域	具体控制要求	华为云的应答
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。	客户应制定其业务连续性机制，对关键数据进行备份。 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。 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。
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。	客户应建立正式的系统以及网络管理程序。 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。

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。

编号	控制域	具体控制要求	华为云的应答
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。	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。华为云在一定程度上会遵从客户的合同流程。如有必要，华为云会积极配合客户方发起的尽职调查。 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。

编号	控制域	具体控制要求	华为云的应答
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	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。 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和治理框架，该框架可有效管理云服务安排，包括任何分包安排。	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。 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。 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。

原文编号	控制域	具体控制要求	华为云的应答
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。	**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。 **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。 **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。 **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。 **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。

原文编号	控制域	具体控制要求	华为云的应答
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。
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。

原文编号	控制域	具体控制要求	华为云的应答
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。

原文编号	控制域	具体控制要求	华为云的应答
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。

原文编号	控制域	具体控制要求	华为云的应答
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及消息的不可抵赖。	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。
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。	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。 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。

原文编号	控制域	具体控制要求	华为云的应答
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其信息资产。	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。 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。

原文编号	控制域	具体控制要求	华为云的应答
第13条	渗透测试	云服务供应商的渗透测试报告可用于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。 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。	客户应该对CSP的环境进行渗透测试。 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。 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。
第14条	安全事件监控	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。 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。	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。 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。 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。

原文编号	控制域	具体控制要求	华为云的应答
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。	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。 同时，华为云针对所有物理设备、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。

原文编号	控制域	具体控制要求	华为云的应答
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。	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。

原文编号	控制域	具体控制要求	华为云的应答
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。

原文编号	控制域	具体控制要求	华为云的应答
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。	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。 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。
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。客户可通过华为云的**漏洞扫描服务（Vulnerability Scan Service，简称VSS）**实现Web漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测等功能，自动发现网站或服务器暴露在网络中的安全风险，可协助用户对其云上的业务进行多维度的安全检测。 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。

原文编号	控制域	具体控制要求	华为云的应答
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。	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、可用区灾备等外，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试，持续优化应急响应机制。

10 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。

11 版本历史

日期	版本	描述
2019年11月	1.0	首次发布
2021年3月	1.1	新增MAS《关于网络卫生的通知》的合规性说明。

