华为云巴西金融行业监管遵从性指导

文档版本 1.0

发布日期 2020-12-16

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 概述

1.1 背景与发布目的

随着技术的发展，对云计算的使用已经成为巴西金融机构的常态。云计算为金融机构的发展带来巨大的好处，但它也为金融机构创造了一个复杂的环境。为规范金融行业对于信息科技的运用，巴西国家货币委员会（The National Monetary Council，简称CMN）和巴西中央银行（The Central Bank of Brazil，简称BCB）发布了一系列监管要求，针对巴西金融机构的网络安全、信息技术风险管理等方面提供了相关监管要求。另外，巴西政府的第8,771号法令针对执行数据处理活动的实体提出了数据安全准则，巴西金融机构同样需要遵守该法令要求。

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遵从金融行业标准要求的云服务及业务运行环境。本文将针对巴西金融机构在使用云服务时通常需遵循的监管要求，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的巴西金融监管要求简介

巴西国家货币委员会（CMN）

- **第4,658号决议（Resolution 4,658）**：该政策文件规定了受巴西中央银行许可的金融机构应遵守的网络安全政策，以及外包数据处理、数据存储和云计算服务的要求。

巴西中央银行（BCB）

- **第3,909号通函（Circular 3,909）**：该政策文件规定了巴西中央银行授权的支付机构应遵守的网络安全政策，以及外包数据处理、数据存储和云计算服务的要求。
- **第3,681号通函（Circular 3,681）**：该政策文件规定了巴西中央银行授权的支付机构应采用的程序，以进行风险管理、治理、保护支付账户中持有的资源以及满足适用于国家金融体系（SFN）机构的规范。

巴西政府

- **第8,771号法令（Decree 8,771）**：该政策文件提供了执行数据处理活动的实体应遵守的数据安全准则， 这些准则侧重于控制对个人数据的访问以及加密或等效保护措施的使用。

1.3 名词定义

- **华为云**

  华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。

- **服务提供商**

  根据外包安排向金融机构提供服务的实体以及实体的分支机构。

- **云计算**

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

- **客户内容数据**

  客户使用华为云服务过程中存储或处理的内容，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。

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

全球性标准类认证

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。
SOC审计	SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
PCI DSS认证	支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discover、万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。

认证	描述
CSA STAR金牌认证	CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
国际通用准则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。
ISO 27799:2016	ISO 27799标准为医疗行业和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。
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。
M&O认证	Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。
NIST网络安全框架(CSF)	NIST CSF由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
PCI 3DS认证	PCI 3DS标准，旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS的评估对象为3D协议执行环境，包括访问控制服务器、目录服务器或3DS服务器功能；以及3D执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估3D协议执行环境的过程、流程、人员管理等。

地区性标准类认证

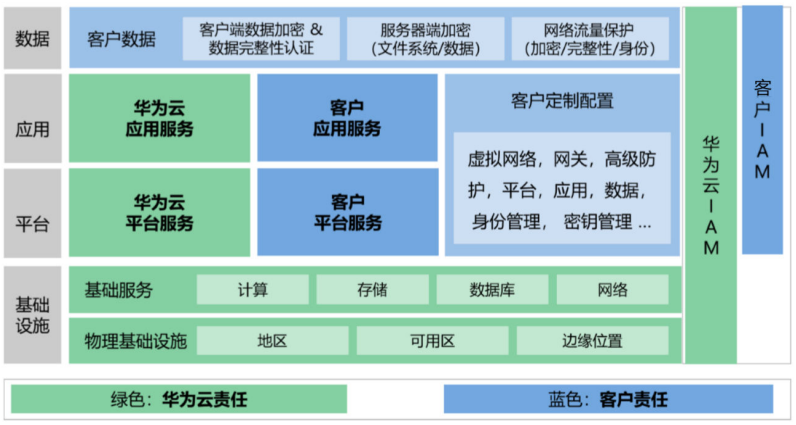
认证	描述
网络安全等级保护	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡 MTCS Level 3 认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3等级认证。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、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。

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-安全合规**”。

3 华为云安全责任共担模型

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

图 3-1 责任共担模型



基于责任共担模型，华为云与客户主要承担如下责任：

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

客户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对用户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，用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。

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

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。

5 华为云如何遵从及协助客户满足 CMN《第 4,658 号决议》和 BCB《第 3,909 号通函》的要求

巴西国家货币委员会于2018年4月26日发布了《第4,658号决议》，并于2019年9月26日进行了更新。该规定从网络安全政策、数据处理、数据存储和云计算服务的外包、通用要求等领域提出对**巴西中央银行许可的金融机构**的网络安全管理相关要求。

巴西中央银行于2018年8月16日发布了《第3,909号通函》，并于2019年11月13日进行了更新。该规定从网络安全政策、数据处理、数据存储和云计算服务的外包、通用要求等领域提出对**巴西中央银行授权的支付机构**的网络安全管理相关要求。

金融机构在遵循《第4,658号决议》和《第3,909号通函》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《第4,658号决议》和《第3,909号通函》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

注：《第4,658号决议》和《第3,909号通函》除适用对象不同之外，与云服务提供商相关的控制要求的条款编号以及内容基本一致。因此，针对华为云作为云服务提供商如何遵从及协助金融机构满足这些要求，在本章节进行合并阐述。

5.1 网络安全政策

原文编号	控制域	具体控制要求	华为云的应答
2、3	网络安全政策的实施	2.金融机构必须实施并维护旨在确保所使用数据和信息系统的保密性、完整性和可用性的原则和指南的网络安全政策。 3. 网络安全政策至少必须包括： I-机构的网络安全目标； II-为减少机构对事件的脆弱性和解决其他网络安全目标而采取的程序和控制； III-具体的控制措施，包括针对信息可追溯性的控制措施，旨在确保敏感信息的安全性； IV-与机构活动相关的事件记录，以及对事件起因和影响的分析以及对结果的控制； V-下列指引：a）制定反映业务连续性测试中考虑的事件的场景；b）定义了针对预防和处理事件的程序和控制措施，这些程序和控制应由处理敏感数据或信息或与机构的运营活动相关的第三方提供商采用；c）根据数据和信息的相关性对其进行分类。	客户应制定并实施网络安全政策，明确网络安全目标、信息安全措施、事件管理流程、业务连续性管理流程、数据分类标准等。作为云服务提供商，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。

原文编号	控制域	具体控制要求	华为云的应答
6、9、10	事件的行动和响应计划	6.金融机构必须制定事件的行动和响应计划，以保障网络安全政策的执行。 9.第2条所述的网络安全政策以及第6条所述事件的行动和响应计划必须得到董事会的批准，如果没有董事会，则须经高级管理层批准。 10. 网络安全政策和事件的行动和响应计划必须至少每年记录并修订一次。	客户应制定事件的行动和响应计划，并得到董事会的批准。另外，定期对网络安全政策和事件的行动和响应计划进行更新。作为云服务提供商： **（1）**华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理系统如ArcSight、Splunk对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。通知的信息至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，华为云会根据具体情况向客户提供事件报告。 **（2）**为应对云环境中复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，从而在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。同时，根据内部信息安全管理体系和业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。

5.2 数据处理、数据存储和云计算服务的外包

原文编号	控制域	具体控制要求	华为云的应答
12、14	服务供应商评估	12.金融机构在聘用数据处理、数据存储和云计算等相关服务之前，必须对第三方提供商能力进行验证，以确保: a)遵守现行法律法规； b)机构对将由第三方提供商处理或存储的数据和信息的访问权； c)第三方提供商处理或存储的数据和信息的保密性、完整性、可用性和恢复； d)遵守机构要求的认证，以履行拟承包的服务； e)机构可以获取第三方提供商聘请的专业独立审计师提供的报告，这些报告与合同服务中使用的程序和控制有关的报告； f)提供足够的资料和管理资源，以监控拟外包的服务； g)通过物理或逻辑控制，识别和分离与机构客户有关的数据；和 h)旨在保护机构客户数据和信息的访问控制的质量。 14. 聘用第12条所述服务的机构，对聘用服务的可靠性、完整性、可用性、安全性和保密性负责，并对现行法律法规的遵守负责。	客户在外包数据处理、数据存储和云计算等相关服务之前，必须对服务供应商的能力进行验证，包括数据安全、认证、报告的获取、服务监控、数据隔离、访问控制等方面。作为云服务供应商，华为云在上述方面的情况如下： **（1）适用法律法规的遵循：**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，参考业界优秀实践从组织、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，助力客户的安全需求。 **（2）客户的访问权：**客户拥有对其数据的所有权和控制权，华为云提供的产品和服务，可让客户确定其内容数据将存储在何处，并支持用户对华为云资源和数据的访问。 **（3）数据安全：**数据安全指对用户数据信息资产的机密性、完整性、可用性、持久性，以及可追溯性等方面的全面保护。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、权限管理、访问控制、数据隔离、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。 **（4）认证：**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，更多信息请参见本白皮书“2.华为云安全与隐私合规”。 **（5）报告的获取：**华为云目前获得了国际上多项权威的安全与隐私保护认

原文编号	控制域	具体控制要求	华为云的应答
			证，第三方测评公司也会定期对华为云展开保密性、安全充分性和合规性的审核并出具第三方审计报告。关于第三方审计报告的获取的要求，可以根据实际情况在客户签订的协议中约定。 **（6）服务监控：**华为云的**云监控服务（Cloud Eye Service，简称CES）**为用户提供一个针对**弹性云服务器（Elastic Cloud Server，简称ECS）**、带宽等资源的立体化监控平台。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。 **（7）数据隔离：**华为云各服务产品和组件从设计之初规划并实施了合理的隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。 **（8）访问控制：**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、访问控制列表来助力用户账户的安全。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，为用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。

原文编号	控制域	具体控制要求	华为云的应答
15	与监管机构的沟通	数据处理、数据存储、云计算等相关服务的外包，必须由金融机构与巴西中央银行进行沟通。 第1段 标题中提到的沟通必须包括以下信息： I-拟签约的第三方供应商名称； II-拟外包的相关服务； III-如果是国外承包时，则根据第16条第III项的规定，指定可提供服务和可储存、处理和管理数据的国家和每个国家的地区。	在外包数据处理、数据存储、云计算等相关服务之前，客户应与巴西中央银行进行沟通。沟通的内容包括服务提供商的公司名称，要聘用的服务，以及可提供服务和可存储、处理和管理数据的国家/地区的说明。金融机构客户向巴西中央银行发出的沟通是金融机构客户独立完成的一项行动，但金融机构客户可以利用华为云在官网和**《华为云用户协议》**中提供的信息来满足其要求。

原文编号	控制域	具体控制要求	华为云的应答
16	巴西境外的外包	外包境外提供的数据处理、数据存储和云计算相关服务，必须具备以下条件: I-巴西中央银行与可能提供服务的国家的监管机构之间存在信息交换协议； II-进行外包的机构必须确保提供本条所述服务不会对其自身的运作造成损害，也不会阻止巴西中央银行的行动； III-进行外包的机构必须在其签约之前定义可提供服务和可储存、处理和管理数据的国家和每个国家的地区；和 IV-进行外包的机构必须在合同不可能继续或合同终止的情况下准备业务连续性的备选方案。	对于在巴西境外提供的云计算服务，客户应查看巴西中央银行发布的与不同国家的**谅解备忘录（MoU）清单**。此列表显示了与巴西中央银行存在信息交换协议的监管机构。若未达成协议，客户应请求巴西中央银行的授权。另外，客户应保证外包服务不会阻碍对自身的运作和巴西中央银行的行动，并确定提供服务和数据处理所涉及的国家/地区，以及合同终止情况下的业务连续性安排。为配合客户满足监管要求，作为云服务提供商： **（1）**华为云不用客户数据做商业变现，在用户协议中明确表示除非是为用户提供必要的服务，或者为遵守适用的法律法规或政府机关的约束性命令，否则不会访问或者使用用户的内容。此外，华为云遵守巴西《通用数据保护法》所述的数据保护原则。 **（2）**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**”。 **（3）**在服务协议终止时，客户可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移服务（Server Migration Service，简称SMS）**，将内容数据从华为云中迁移出去，如迁移至本地数据中心。

原文编号	控制域	具体控制要求	华为云的应答
17	服务协议	数据处理、数据存储、云计算相关服务合同必须包括: I-指明可以提供服务和可储存、处理和管理数据的国家和地区; II-为传输和存储第I项所述数据而采取的安全措施; III-在合同生效期间,隔离数据和访问控制,以保护客户的信息; IV-合同终止时的义务: a)将第I项引用的数据转移给新的第三方提供商或进行外包的机构;b)在完成a项所述的数据传输及确认接收数据的完整性和可用性确认,由被替换的第三方提供商删除第I项中提及的数据; V-进行外包的机构可以访问: a)第三方提供商提供的信息,用于验证符合第I、III项;b)第12条第II项d、e项所述专业独立审计提供的证明和报告的有关资料;c)第12条第II项f项所述用于监控所提供服务的适当信息和管理资源; VI-如果分包服务被视为与进行外包的机构有关,第三方提供商有义务通知进行外包的机构; VII-允许巴西中央银行访问与提供服务相关的合同和条款、与所提供服务相关的文	客户应与服务提供商签订具有法律效力服务协议,并保证协议条款的合法性和适宜性。 为配合客户满足监管要求:华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**,其中规定了所提供服务内容和服务水平,以及华为云的职责。同时,华为云也制定了线下合同模板,可根据不同客户的需求进行定制化,客户及其监管机构对华为云的审计和监督权益,华为云会根据实际情况在与客户签订的协议中进行约定。

原文编号	控制域	具体控制要求	华为云的应答
		件和信息、存储的数据及其处理信息、数据和信息的备份以及数据和信息的访问代码； VIII-根据巴西中央银行的决定，进行外包的机构采取的措施；以及 IX-第三方提供商有义务随时向进行外包的机构通报可能影响所提供服务或遵守现行法律法规的限制。	

5.3 通用要求

原文编号	控制域	具体控制要求	华为云的应答
19	业务连续性管理政策	金融机构必须确保其依照现行法规实施的风险管理政策，包括与业务连续性有关的事项： I-第3条第IV项所提到的相关网络安全事件的处理； II-云计算服务相关数据处理、数据存储和外包中断时应遵循的程序，包括考虑更换第三方提供商和恢复机构正常运行的场景；和 III-第3条第V项a点中提及的业务连续性测试中考虑的事件场景。	请参见本文档**5.1 网络安全政策**下**“事件的行动和响应计划”**的相关内容。

原文编号	控制域	具体控制要求	华为云的应答
20	业务连续性管理程序	金融机构为符合现行法规而采取的风险管理程序，必须包括与业务连续性有关的事项： I-为减轻第3条第IV项所述相关事件的影响以及合同中相关数据处理、数据存储和云计算服务中断而采取的处理措施； II-第I项所述中断的活动或有关服务规定的恢复或恢复正常的期限；和 III-及时向巴西中央银行通报第I项中所述构成金融机构危机状况的相关事件和相关服务中断，以及恢复活动的程序。	客户应建立业务连续性管理机制，明确有关服务的恢复目标及最小恢复策略，制定危机管理流程，包括危机的响应、处置和通报。作为云服务提供商： **（1）**为向客户提供持续、稳定的云服务，华为云遵循ISO22301业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。 **（2）**华为云根据内部业务连续性管理体系的要求，定期开展风险评估，识别并分析支撑云服务持续运行的关键资源所面临的潜在风险。针对突出风险，华为云进一步考虑突发事件发生的场景，并制定应对各种突发事件场景的危机管理程序，以最大程度地降低突发事件的影响。危机管理程序中详细规定了突发事件的预警和报告流程、事件升级流程、应急预案启动的条件、事件进展的通报流程、内外部沟通流程等。 **（3）**为配合客户满足通知的要求，华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。根据内部的客户通知通报流程，在底层基础平台发生严重事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。

6 华为云如何遵从及协助客户满足 BCB《第 3,681 号通函》的要求

巴西中央银行于2013年11月4日发布了《第3,681号通函》。该规定从业务连续性计划、数据安全、漏洞管理、变更管理、问题管理、测试管理等领域提出对金融机构操作风险管理相关要求。

金融机构在遵循《第3,681号通函》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《第3,681号通函》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

原文编号	控制域	具体控制要求	华为云的应答
4(I)	业务连续性计划	关于操作风险，风险管理架构必须至少提供: I-为保障支付服务的连续性所采取的应急计划及其他机制。	客户应制定业务连续性计划保障支付服务持续运行。为向客户提供持续、稳定的云服务，华为云遵循ISO22301业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。华为云根据内部业务连续性管理体系的要求，定期开展风险评估，识别并分析支撑云服务持续运行的关键资源所面临的潜在风险。针对突出风险，进一步考虑突发事件发生的场景，并制定应对各种突发事件场景的危机管理程序，以最大程度地降低突发事件的影响。危机管理程序中详细规定了突发事件的预警和报告流程、事件升级流程、应急预案启动的条件、事件进展的通报流程、内外部沟通流程等。

原文编号	控制域	具体控制要求	华为云的应答
4(I)(II)	数据安全	II-储存、处理或传送的数据的安全保护机制； III -网络、电子站点、服务器和通信渠道的安全保护机制，以减少遭受攻击的脆弱性。	客户应建立数据安全管理机制，保障数据在存储、处理和传输过程的安全性。为保障客户安全地处理云上数据，华为云对数据生命周期的各阶段进行层层防护： **（1）数据创建：**华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据。客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，使客户内容数据存储在目标位置。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，使客户只能访问到自己的数据。 **（2）数据存储：**目前，**云硬盘（EVS）**、**对象存储服务（OBS）**、**镜像服务（IMS）**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，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，从而助力客户云上数据的安全。 **（3）数据使用：**华为云从数据访问控制、安全防护、审计等方面为客户提供了相关服务，协助客户对数据的使用和流转做到更加细粒度的管控。更多信息可参见《华为云数据安全白皮书》4.5。 **（4）数据传输：**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（VPN）、云专线服务、云连接等服务，实现不同区域之间业务的互联互通和数据传输安全。 **（5）数据归档：**华为云提供了多粒度的数据备份归档服务，以满足客户

原文编号	控制域	具体控制要求	华为云的应答
			不同场景下的需求。客户可以使用**对象存储服务（OBS）**的版本控制、**云硬盘备份（VBS）**、**云服务器备份（CSBS）**等功能，将云上的文档、硬盘、服务器进行备份。上述服务通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。 **（6）数据销毁：**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。
4(IV)	日志与监控	IV-监测、跟踪和限制访问敏感数据、网络、系统、数据库和安全模块的程序。	客户应建立对敏感数据、网络、系统、数据库和安全模块的监控机制。为配合客户满足监管要求，作为云服务提供商，华为云的**云审计服务（CTS）**为用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，使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，保障日志信息传输和保存的准确；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，华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以助力支撑网络安全事件回溯和合规。

原文编号	控制域	具体控制要求	华为云的应答
4(V)	漏洞管理	V-监控数据安全漏洞和最终用户的投诉。	客户应建立漏洞管理机制，监控数据安全漏洞和最终用户的投诉。为配合客户满足监管要求，作为云服务提供商： **（1）**华为云**漏洞扫描服务（Vulnerability Scan Service，简称VSS）**集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、弱密码检测五大核心功能，可自动发现网站或服务器暴露在网络中的安全风险，为云上业务提供多维度的安全检测服务。 **（2）**华为产品安全事件响应团队（PSIRT）已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对用户业务造成影响的风险。同时，华为PSIRT和华为云安全运维团队已经建立了漏洞感知、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，使基础设施、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能够在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用户业务的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对用户业务造成影响。

原文编号	控制域	具体控制要求	华为云的应答
4(VI)	变更管理	VI-审查安全措施和数据机密性，特别是在基础设施或程序变更之前。	客户应建立变更管理机制，在基础设施或程序变更之前，审查安全措施和数据机密性。华为云作为云服务提供商，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、变更窗口，并形成变更通告机制。该流程要求：在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，使变更委员会能够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。
4(VII)	问题管理	VII-编制报告，说明纠正已发现缺陷的程序。	客户应建立问题管理机制，及时处理并记录已发现的问题。华为云作为云服务提供商，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
4(VIII)(IX)	测试管理	VIII-进行测试，以确保采用的数据安全措施的稳健性和有效性； IX-开发、测试和生产环境的分离。	客户应建立测试管理机制，进行测试以确保采用的数据安全措施的健壮性和有效性。另外，应对开发、测试和生产环境进行分离。作为云服务提供商： **（1）**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。为配合客户满足合规要求，华为云通过制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。 **（2）**华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，使发布的云服务能够满足安全要求。测试在与生产环境隔离的测试环境中进行，以避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱敏，测试完成后需要进行数据清理。
4 Sole paragraph	服务协议	如果支付机构外包与所提供服务的安全性有关的职能，则相应的服务提供合同必须规定承包商必须： I-遵守本条的规定；和 II-允许支付机构访问有关所提供服务的数据和信息。	请参见本文档**5.2 数据处理、数据存储和云计算服务的外包**下**“服务供应商评估”**的相关内容。

7 华为云如何遵从及协助客户满足巴西政府《第 8,771 号法令》的要求

巴西政府于2016年5月11日发布了《第8,771号法令》。该规定从网络安全、记录、个人资料和私人通信的保护等领域提出了对数据保护相关要求。

金融机构在遵循《第8,771号法令》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《第8,771号法令》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

7.1 网络安全

原文编号	控制域	具体控制要求	华为云的应答
5	网络安全	负责传输、交换或路由活动的当事方必须应遵守适当提供服务和应用所必需的技术要求，其目的是保持其稳定性、安全性、完整性和功能性。 (1)上段提到的必要技术要求是来自： I-处理网络安全问题，例如对限制发送大量消息（垃圾邮件）和拒绝服务攻击； II-处理网络干扰的特殊情况，例如在主路由中断和紧急情况下的备用路由。	在处理网络安全问题和网络干扰的特殊情况时，客户应遵守必需的技术要求以保持其服务和应用的稳定性、安全性、完整性和功能性。作为云服务提供商，为配合客户满足监管要求： （1）华为云为客户提供两种防DDoS攻击服务：**Anti-DDoS流量清洗服务（简称Anti-DDoS）**和**DDoS高防（Advanced Anti-DDoS，简称AAD）**。Anti-DDoS是一种流量清洗服务，为客户的华为云内资源（弹性云服务器、弹性负载均衡），提供网络层和应用层的DDoS攻击防护，并提供攻击拦截实时告警，有效提升用户带宽利用率，保障业务稳定可靠。AAD则可服务于华为云和非华为云的主机，用户可以通过修改DNS解析或对外服务地址为高防IP，将恶意攻击流量引流到高防IP清洗，助力重要业务不被攻击中断。华为云的防DDoS攻击服务提供精细化的抵御DDoS攻击的功能，包括但不限于Ping Flood、 SYN Flood、UDP Flood、Challenge Collapsar、HTTP Flood 、DNS Flood。用户只需根据租用带宽及业务模型自助配置防护阈值，系统检测到攻击后就会实时通知用户并进行有效防御。 （2）华为云**Web应用防火墙服务（WAF）**是结合了华为多年攻防经验和一系列针对性优化算法的高级Web应用防火墙。采用正则规则和语义分析的双引擎架构对SQL注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意bot、webshell、CC等攻击实现实时的高性能防护。华为云WAF给用户提供简便的管理界面，用户可根据自身业务需要进行相关防护设置，亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。 （3）客户可以使用华为云提供的**弹性负载均衡（Elastic Load Balance，简称ELB）**服务，实现不同区域之间的负载平衡。ELB将访问流量自动分发到多台弹性云服务器，扩展应用系统对外

原文编号	控制域	具体控制要求	华为云的应答
			的服务能力，实现更高水平的应用程序容错性能。 **（4）**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。

7.2 记录、个人资料和私人通信的保护

原文编号	控制域	具体控制要求	华为云的应答
13	访问控制	连接和应用程序提供商在保管、存储和处理个人数据和私人通信时必须遵守以下安全标准指南： I-建立对数据访问的严格控制；通过对某些具有访问权限和具有专有访问权限的人规定责任； II-为记录的访问提供认证机制，例如使用双重认证系统，以确保负责数据处理的人员的个性化； III-创建连接和应用程序记录的详细访问日志。这些记录应包括访问的时间和持续时间、涉及的由公司指定的员工或负责人的身份以及被访问的文件； IV-使用记录管理解决方案，通过技术手段保证数据的不可侵犯性（如加密或等效保护措施）。	客户应建立访问控制管理机制，设定与职责匹配的用户权限，采用安全的身份认证和数据加密技术，并对用户访问通过日志进行记录。作为云服务提供商，为配合客户满足监管要求： （1）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。每一位华为云客户在华为云都拥有唯一可辨识的用户ID，此外，华为云还提供多种用户身份验证机制，包括账号密码、多因素认证等。 • IAM支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。 • IAM同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM默认启用多因子认证，保证用户账号安全。 • 如果用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，并访问用户的华为云资源。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。 （2）华为云的**云审计服务（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

原文编号	控制域	具体控制要求	华为云的应答
			全分析、合规审计、资源跟踪和问题定位等常见应用场景。 （3）华为云内部建立了运维和运营账号管理机制。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，华为云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。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。
16	安全标准披露	有关应用程序和连接提供商采用的安全标准的信息应以清晰易懂的方式向任何相关方披露，最好通过其网站披露，同时尊重商业秘密的保密权。	客户应向相关方披露其所采用的安全标准信息。作为云服务提供商： （1）华为云在官网上发布了其所提供产品的功能、安全特性以及使用到的标准技术的说明，具体请参见华为云官网“**帮助中心**”。 （2）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，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-安全合规**”。

8 结语

本文描述了华为云如何为客户提供遵从巴西金融行业监管要求的云服务，并表明华为云遵守巴西国家货币委员会（CMN）、巴西中央银行（BCB）和巴西政府发布的重点监管要求，有助于客户详细了解华为云对巴西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、构建和部署遵从巴西金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

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

9 版本历史

日期	版本	描述
2020年12月	1.0	首次发布