华为云阿根廷金融行业监管遵从性指南

文档版本 2.0

发布日期 2022-05-16

华为云计算技术有限公司

商标声明


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

注意

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 背景与发布目的

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，阿根廷共和国中央银行（BCRA）针对阿根廷金融机构如何进行科技风险管理、科技外包管理等方面提出了一系列监管要求、指南和通知。

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。本文将针对阿根廷金融机构在使用云服务时通常需遵循的监管要求和指南，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的阿根廷金融监管要求简介

阿根廷共和国中央银行（BCRA）是阿根廷主要的金融监管机构，负责监管、检查和监督阿根廷的金融机构。BCRA属下的金融和交易机构监管局（SEFyC）负责对阿根廷金融机构的跟踪、监督、分析、审计、合规检查等工作。

BCRA在2017年11月17日颁发了《COMMUNICATION“A”6375》（简称《“A”6375》），该法规针对使用了去中心化/外包服务的金融机构提出了相关管理要求，为金融机构提供了针对去中心化/外包活动的风险管理指导。

注：BCRA在2018年8月29日颁发了《COMMUNICATION“A”4609》（简称《“A”4609》），该法规定义了金融机构在信息资产、数据处理、操作流程、记录存储、数据库管理、系统变更、事件管理、技术文档、合规性等场景中需遵守的主要要求，但同时考虑到《“A”4609》中所有场景下的要求在《“A”6375》中均有体现，且《“A”6375》规定的要求更为全面、具体，故本遵从性指导将聚焦于《“A”6375》的监管要求。

BCRA在2017年11月3日颁发了《COMMUNICATION“A”6354》（简称《“A”6354》），后BCRA又对其进行更新、修订，于2017年11月17日颁发了《“A”6375》，对金融机构在将IT服务去中心化/外包给服务供应商时需遵循的要求进行了完善。

BCRA在2021年4月16日颁布了《COMMUNICATION“A”7266》（简称“A”7266），该法针对金融机构在网络事件应对和恢复方面制定了相关准则，旨在保护金融市场稳定，提供整个生态系统的网络恢复能力。

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。

- **客户**

  指与华为云达成商业关系的注册用户。

- **外包**

  指利用其他服务供应商履行通常全部或部分由金融机构自行履行的职能。

- **服务供应商**

  指通过订立合同，履行通常由金融机构自行履行的职能的其他法人，包括任何从原始服务供应商或分包商分包或转包服务的法人。

- **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。

2 华为云的认证情况

华为云继承了华为公司完备的管理体系以及IT系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全，主要包括：

全球性标准类认证

认证	产品介绍
ISO 20000:2011	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。
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。

认证	产品介绍
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。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。
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。
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认证的通过表明华为云在3D协议执行环境的过程、流程、人员管理等方面符合安全标准。

地区性标准类认证

认证	产品介绍
网络安全等级保护（中国）	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。
可信云金牌运维专项评估（中国）	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（中国）	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（中国）	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（中国）	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。

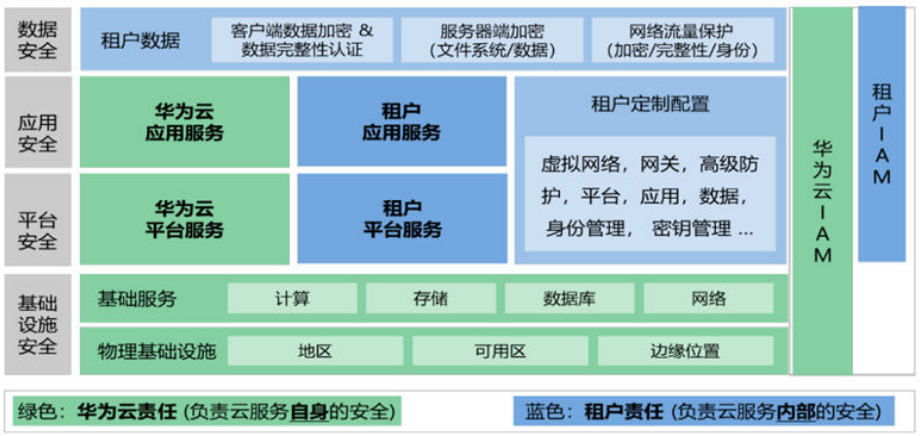
认证	产品介绍
网信办网络安全审查（中国）	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。
MTCS Level 3认证（新加坡）	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3 等级认证。
OSPAR认证（新加坡）	OSPAR是新加坡银行业工会（ABS）对外包服务提供商出具的审计报告。华为云通过了新加坡银行协会(ABS)关于控制外包服务提供商的目标和流程的指南（ABS指南），证明了华为云是符合ABS指南中规定的控制措施的外包服务提供商。
TISAX（欧洲）	TISAX（Trusted Information Security Assessment Exchange，可信信息安全评估交换）是德国汽车工业联合会（VDA）联合欧洲汽车工业安全数据交换协会（ENX）推出的汽车行业信息安全评估和数据交换安全标准。TISAX认证的通过，表明华为云已满足欧洲认可的汽车行业信息安全标准。

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

3 华为云安全责任共担

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

图 3-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

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

租户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

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

4 华为云全球基础设施

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

5 华为云如何遵从及协助客户满足 BCRA《“A”6375》的要求

《“A”6375》阐述了金融机构在将IT服务外包给第三方服务供应商（包括云服务供应商）时，金融机构需遵循的监管要求及在外包业务时需处理的事项。

金融机构在遵循《“A”6375》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《“A”6375》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。

5.1 通知和条件

《“A”6375》第2章要求金融机构在去中心化/外包活动时应事先通知监管机构并符合一定条件，对应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
2.1	事先通知	金融机构可以去中心化/外包不属于服务其客户和/或公众的活动（例如行政、IT服务、归档、打印等），但必须至少在此类活动开始前60天提前通知金融交易实体监管（SEFyC）。	当金融机构去中心化/外包不属于其客户和/或公众的活动时（如行政、IT服务、归档、打印等）时，应在此类活动开始前60天通知金融交易实体监管（SEFyC）。 华为云会配合金融机构提供通知所需材料。

编号	控制域	具体控制要求	华为云的应答
2.2	条件	去中心化/外包活动应遵守以下条件： ● 遵守与活动性质和类型相关的技术法规要求，合同或服务协议中明确规定相关的技术法规要求、金融交易实体监管（SEFyC）定期审核要求。 ● 金融机构必须实施统一访问点，以便能够主动、持续和永久地控制和监控所有IT外包活动和金融机构的数据。 ● 要求去中心化/外包IT服务的代理供应商至少每年一次对去中心化/外包活动进行内审，并且向金融机构总管理层提交审计报告，且此类审计报告也必须发送到系统外部审计管理部门。此外，代理人必须提交由外部审计员出具的关于其审查去中心化/外包活动的报告。 要求金融机构和其签约的第三方必须接受金融交易实体监管（SEFyC）指定的代理人履行其监督职能。	金融机构应识别与去中心化/外包活动相关的技术法规要求，并在与第三方签订的合同协议中明确这些要求。金融机构还应在合同中要求服务供应商至少每年一次对去中心化/外包活动进行内审和外审，并明确金融交易实体监管（SEFyC）有权对服务供应商进行监督。金融机构应实施统一访问点，以便能够控制和监控所有外包的IT活动和金融机构的数据。 华为云会遵从与金融机构签订的协议中约定的要求，华为云会安排专人积极配合金融机构和金融交易实体监管（SEFyC)/监管指定的代理人对华为云的审计和监督。金融机构对华为云的审计和监督权益会根据实际情况在与金融机构签订的协议中进行承诺。 此外，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。审计团队每年投入10+人力对全球范围运营的华为云至少开展1次，为期2个月的审计，重点关注华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上的风险。审计结果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。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。如有必要，金融机构可以通过官方渠道向华为云申请获取审计报告的副本。

编号	控制域	具体控制要求	华为云的应答
2.3	通知要求	金融机构在通知金融交易实体监管（SEFyC）去中心化/外包活动时，通知内容必须包括以下方面： ● 所涉及的每个活动的性质。 ● 活动的地址，或将要在活动中建立的信息系统管理和操作环境。 ● 活动的开始日期。 ● 外包合同的副本（若涉及将活动外包给第三方）。 ● 应遵守与活动性质和类型相关的技术法规要求。 ● 活动的合同或服务协议应明确规定参与的各方需接受并遵守相关技术法规要求，并且金融交易实体监管(SEFyC)定期审核参与的各方是否符合去中心化活动相关的技术法规要求。 ● 具备足够权限的人的签名。 所需文件必须按照金融交易实体监管(SEFyC)规定的“pdf”格式发送，原件保存在金融机构中，由金融交易实体监管(SEFyC)处置。金融机构的法定代表人必须正式声明，以电子方式发送的所有文件均为该金融机构保存文件的副本，由金融交易实体监管(SEFyC)处置，并详细说明其存放的位置。	金融机构应按法规要求通知金融交易实体监管（SEFyC），并提交去中心化活动相关信息清单及外包合同副本等材料。 华为云会配合金融机构提供所需材料。

5.2 统一访问点（PAU）

《“A”6375》第7.3章要求金融机构应定义统一访问点，通过该统一访问点，金融机构能够控制和监控IT外包活动和数据，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
7.3	统一访问点	要求阿根廷的金融机构应定义统一访问点，通过该统一访问点可以主动、持续和永久地控制和监控所有IT外包活动和数据。	阿根廷的金融机构应定义统一访问点，并通过该统一访问点控制和监控所有IT外包活动和数据。 金融机构可通过华为云的**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。

5.3 安全流程

《“A”6375》第7.2章要求金融机构应制定7个领域的安全流程及内容，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
7.2	安全流程	要求金融机构和服务供应商必须具有以下7领域详细的安全流程及内容： • 信息安全治理（ISG） • 安全意识和技能培训（AT） • 访问控制（CA） • 完整性和注册（IR） • 监视和控制（MC） • 事件管理（IM） • 运营连续性（CO） 要求金融机构将其IT组织架构、运营架构、和服务供应商之间的安全责任共担模型等信息告知BCRA。	金融机构应制定所要求的7个领域详细的安全流程及内容，并将其IT组织架构、运营架构和服务供应商之间的安全责任共担模型等信息告知BCRA。 华为云明确定义了与金融机构之间的安全责任共担模型，有关责任共担模型的具体内容请参见**《华为云安全白皮书》**。华为云也会积极配合金融机构执行BCRA上报工作。此外，华为云参照ISO27001构建了信息安全管理体系，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、以及业务连续性等。

5.4 情景矩阵

《“A”6375》第7.5章节概述了一个“情景矩阵”，该情景矩阵按照所处理的数据性质、数据类型以及所涉及的外包服务类别，描述了四种不同的IT外包情景，BCRA为每种情况制定了最低技术操作要求。下表总结了该情景矩阵，编号对应的具体技术操作要求详见本文档5.5章：

应用场景	情况	信息安全治理	安全意识和技能培训	访问控制	完整性和注册	监视和控制	事件管理	运营连续性
ESD001	客户数据：使用、开发、保存和传输，包括涵盖客户数据在内的金融交易数据。	RGS001 RGS002 RGS003 RGS004 RGS005 RGS006 RGS007	RCC001 RCC002 RCC005 RCC006 RCC007 RCC008 RCC010 RCC012 RCC013	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020 RIR021 RIR022 RIR023 RIR024	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD002	财务会计数据:使用、开发、保存和传输，包括或不包括数据。	RGS001 RGS002 RGS003 RGS004 RGS005 RGS006 RGS007	RCC001 RCC002 RCC005 RCC006 RCC007 RCC008 RCC010 RCC012 RCC013	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020 RIR021 RIR022 RIR023 RIR024	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004

应用场景	情况	信息安全治理	安全意识和技能培训	访问控制	完整性和注册	监视和控制	事件管理	运营连续性
ESD003	金融交易数据:使用、开发、保存和传输，不包括客户数据。	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD004	经营数据:使用、开发、保存和传输，不包括会计财务信息、客户或交易信息。	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023 RIR025	RMC003 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004

5.5 技术操作要求

《“A”6375》第7.7.1章要求金融机构应满足信息安全治理的技术操作要求，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
7.7.1	信息安全治理技术操作要求	RGS001：要求金融机构/服务供应商应定义完整、详细和清晰的IT服务相关角色、职责、金融机构与服务供应商之间的职责分担关系，遵守法规中定义的职责分离原则，并将上述信息告知BCRA。	金融机构应定义IT服务相关角色、职责、与服务供应商之间的职责分担模型，确保职责分离，并通知BCRA。 金融机构可通过华为云的**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。华为云明确定义了与金融机构之间的安全责任共担模型，金融机构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。 此外，华为云内部建立了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。

编号	控制域	具体控制要求	华为云的应答
7.7.1	信息安全治理技术操作要求	RGS002：要求金融机构/服务供应商必须建立处理其客户数据的角色和职责，且必须在IT外包协议中正式规定。	针对金融机构的客户数据，金融机构应建立相关数据处理的角色和职责，并在和服务供应商签订的协议中明确规定各自的角色和职责。 作为云服务供应商，华为云负责为金融机构提供安全的云服务相关基础设施、云平台以及软件应用，也就是负责平台安全，以帮助金融机构保护其内容数据。关于华为云与金融机构之间的数据安全责任界定等更多详细信息请参见**《华为云数据安全白皮书》**。
7.7.1	信息安全治理技术操作要求	RGS003：若涉及个人数据的收集和使用时，要求金融机构/服务供应商遵守与保护个人数据有关的国家法律法规（阿根廷第25,326号法律-个人数据保护法PDPL），且该要求必须在IT服务协议中正式定义。	金融机构应识别与个人数据保护相关法律法规，并评估自身的合规性。在采购服务供应商时，金融机构还应评估服务供应商对法规的遵从性，且在与服务供应商签订的协议中明确要求服务供应商必须遵从个人数据保护相关法律法规要求。 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，在遵从金融机构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、生态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、金融机构及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足金融机构的安全需求。华为云已识别并分析了PDPL法规要求，更多信息请详见**《华为云阿根廷PDPL遵从性说明》**。

编号	控制域	具体控制要求	华为云的应答
7.7.1	信息安全治理技术操作要求	RGS004：金融机构/服务供应商应建立并记录与IT服务协议参与者（包括第三方分包商）之间的信息交换协议，以及可以保证的技术和操作措施（包括格式，期限，责任方等），并向有关各方和BCRA提供有用、及时和完整的信息。	金融机构应与服务供应商签订协议，且协议中应包括详细的技术操作措施，以便向有关各方和BCRA提供有用、及时和完整的信息。 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，可根据不同金融机构的需求进行定制化。 此外，华为云内部也建立了完善的供应商管理机制，会对外包商以及外包人员进行严格的安全管理，并会定期对供应商进行审计和安全评估。

编号	控制域	具体控制要求	华为云的应答
7.7.1	信息安全治理技术操作要求	RGS005：若服务供应商/分包商涉及提供在境外处理、存储或传输金融机构数据的IT服务时，要求金融机构/服务供应商/所涉及的第三方提供必要的机制来验证该地点满足IT服务协议中明确的法律法规和合同协议要求。	金融机构应确定其数据类型以及数据存储、传输、处理的位置等信息，识别是否存在数据跨境场景，并分析相关法律法规要求，在与服务供应商签订的合同中明确要求服务供应商应提供机制来验证数据存储、传输、处理是否符合法律法规、合同协议要求。 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。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，在遵从金融机构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、生态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、金融机构及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足金融机构的安全需求。

编号	控制域	具体控制要求	华为云的应答
7.7.1	信息安全治理技术操作要求	RGS006：要求金融机构在IT服务协议中明确不得披露个人数据的义务，并将此类义务扩展至分包的第三方。	金融机构应在与服务供应商签订的协议中明确服务供应商不得披露个人数据的义务。 作为云服务供应商，华为云负责为金融机构提供安全的云服务相关基础设施、云平台以及软件应用，也就是负责平台安全，以帮助金融机构保护其内容数据。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，在遵从金融机构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、生态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、金融机构及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足金融机构的安全需求。华为云已识别并分析了PDPL法规要求，更多信息请详见**《华为云阿根廷PDPL遵从性说明》**。
7.7.1	信息安全治理技术操作要求	RGS007：要求金融机构/服务供应商在IT服务中记录、分配所有信息资产的所有权，以确定信息生命周期中每一方的运营责任。	金融机构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。 华为云为金融机构提供统一的管理界面，供金融机构查询并管理云服务。华为云的**企业主机安全（Host Security Service,简称HSS）**是服务器的贴身安全管家，可为金融机构提供资产管理功能，包括提供账号、端口、进程、Web目录和软件等安全资产信息的管理和分析。

《“A”6375》第7.7.2章要求金融机构应符合安全意识和技能培训技术操作要求，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
7.7.2	安全意识和技能培训技术操作要求	RCC001：要求金融机构/服务供应商应根据漏洞分析和事件管理的结果（包括但不限于对已报告、已发现和已发生事件的分析和管理）来制定安全意识和技能培训计划的内容并定期更新。	金融机构应制定完善的安全意识和技能培训管理机制，根据培训对象的职能和角色来制定培训内容，定期分析并更新培训内容，培训内容包括但不限于： ● 已报告、已检测和已发生的安全事件； ● 如何防止通过“社会工程”、“网络钓鱼”、“电话钓鱼”和其他具有类似特征的攻击来盗用个人数据和凭据； ● 保护身份认证凭证的措施； ● IT服务知识； ● IT服务的开发、获取、制造、实施、认证和安全性测试的技术。 金融机构还应建立有效的安全意识和技能培训沟通渠道，以处理相关投诉和问题。培训对象应覆盖特定活动流程所需的所有必要参与者。 作为云服务供应商，华为云会为金融机构提供培训服务和资源，包括帮助文档、使用手册、安全实施指南等，关于更多华为云为金融机构提供的培训服务和资源请参见官网“培训服务”。 此外，华为云内部也建立了人力资源管理框架，是建立在法律基础之上。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。华为云会至少每年一次对员工进行安全意识和技能培训，培训的形式包括但不限于现场演讲、视频网课、信息文档等，并定期更新培训内容。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。
7.7.2	安全意识和技能培训技术操作要求	RCC002：要求金融机构/服务供应商的安全意识和技能培训计划的内容包括：如何防止通过“社会工程”、“网络钓鱼”、“电话钓鱼”和其他具有类似特征的攻击来盗用个人数据和凭据。	
7.7.2	安全意识和技能培训技术操作要求	RCC005：要求金融机构/服务供应商的内部人员、IT服务管理人员、参与操作的第三方人员以及客户了解有效的沟通渠道，以处理相关流程中的投诉或问题。	
7.7.2	安全意识和技能培训技术操作要求	RCC006：要求金融机构/服务供应商的安全意识和技能培训的对象应满足以下要求： ● 根据每个培训对象在流程中的角色和职能，制定安全意识和技能培训内容。 ● 培训对象覆盖特定活动流程的所有必要参与者，包括但不限于：内部人员、IT服务管理人员、供应商和客户。	
7.7.2	安全意识和技能培训技术操作要求	RCC007：要求金融机构/服务供应商每年至少分析一次安全意识和技能培训计划，分析至少包括以下方面： ● 培训对象数量、培训对象分类以及培训内容； ● 培训内容必须涵盖已报告/已检测/已知的安全事件。	
7.7.2	安全意识和技能培训技术操作要求	RCC008：要求金融机构/服务供应商的安全意识和技能培训的内容包括:保护身份认证凭证的措施。	

编号	控制域	具体控制要求	华为云的应答
7.7.2	安全意识和技能培训技术操作要求	RCC010：要求金融机构/服务供应商的安全意识和技能培训的内容包括：IT服务知识。	
7.7.2	安全意识和技能培训技术操作要求	RCC012：要求金融机构/服务供应商的安全意识和技能培训的内容包括：IT服务的开发、获取、制造、实施、认证和安全性测试的技术，以确保内部或外部相关人员均受到适当的培训，以减少失败的操作。	
7.7.2	安全意识和技能培训技术操作要求	RCC013：要求金融机构/服务供应商必须为其安全意识和技能培训提供一种通信机制，以确保： ● 培训对象及时被通知； ● 培训对象可以查询并消除任何疑问。	

《“A”6375》第7.7.3章要求金融机构应满足访问控制领域的技术操作要求，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
7.7.3	访问控制技术操作要求	RCA049：要求金融机构/服务供应商保证他们或其任何供应商不会出于IT服务协议中规定的目的之外的目的来访问/处理/利用个人数据，也不得未经主要数据控制者的明示同意来访问/处理/利用个人数据。	金融机构作为产品或服务的购买方，应决定如何利用产品或服务存储和处理内容数据，包括其中可能的个人数据，因此金融机构负责内容数据的安全与合规。 作为云服务供应商，华为云会识别并保护金融机构的个人数据。从公司政策、流程、操作层面制定了隐私保护策略，并采取匿名化、数据加密、系统及平台安全防护等措施，全面保护金融机构个人数据的安全。华为云还负责在云服务中涉及到的基础平台及设施的安全，并确保华为云的应用安全、平台安全水平遵从适用的隐私保护法规要求。同时华为云为金融机构提供多种隐私保护技术及服务，包括访问控制和身份认证、数据加密、日志和审计等功能，帮助金融机构根据业务需求进行隐私保护。

编号	控制域	具体控制要求	华为云的应答
7.7.3	访问控制技术操作要求	RCA050：要求金融机构/服务供应商保证金融机构和BCRA在需要时可不受限制地访问与IT服务的处理、操作和程序相关的所有文档和信息。	针对IT服务的处理、操作和程序，金融机构应建立和留存相关文档和信息，并提供渠道以便监管机构在必要时访问文档和信息。金融机构还应向监管机构提供合规性审计报告，以验证IT服务环境安全控制的有效性。 如有必要，金融机构可以通过华为云的**统一身份认证服务(Identity and Access Management，简称IAM）**为监管机构创建一个临时用户账号，供监管机构访问IT服务的处理、操作和程序相关的文档和信息。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，必要时，金融机构需向监管机构提供IT服务的操作记录。 此外，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。如有必要，金融机构可以通过官方渠道向华为云申请获取审计报告的副本。

编号	控制域	具体控制要求	华为云的应答
7.7.3	访问控制技术操作要求	RCA051：要求金融机构必须确保服务供应商已通过独立评估、外部审核和国际标准认证，来实施并支持所提供IT服务的控制级别。	金融机构在采购服务供应商时，应查看服务供应商的认证和合规性报告，以评估和验证所提供IT服务是否满足要求。 华为云已获得众多国际和行业安全合规资质认证，包括ISO27001、ISO27017、ISO27018、PCI-DSS、CSA STAR等,并且每年会接受第三方的审计。如有必要，金融机构可以通过官方渠道向华为云申请获取审计报告的副本。华为云遵循国际标准建立信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。

编号	控制域	具体控制要求	华为云的应答
7.7.3	访问控制技术操作要求	RCA052：要求金融机构/服务供应商应对不兼容角色进行隔离，实施统一的身份管理策略，包括但不限于以下内容： • 数据加密机制和通信渠道； • 操作/应用平台的特权用户； • 紧急/临时用户； • 普通用户。 要求金融机构/服务供应商还必须确保密钥的生命周期、密钥的参数、规则、算法和软件应该是最新的并传达给相关方。	金融机构应建立用户访问管理机制，基于最小权限原则进行访问权限限制和监督，识别不兼容角色，确保职责分离。金融机构应做好数据分类，并进行风险分析，再根据风险分析结果，明确数据是否加密以及加密的措施。金融机构还应建立密钥管理机制，使金融机构数据的机密性和完整性不会受到损害。密钥管理措施包括：定期轮换密钥、制定详细的政策和程序管理密钥的生命周期以及密钥的备份等。 金融机构可通过华为云的**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。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。金融机构还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进行封装，使得金融机构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。对于传输中的数据，当金融机构通过互联网提供Web网站业务时，可以使用华为云联合全球知

编号	控制域	具体控制要求	华为云的应答
			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。针对金融机构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。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，除金融机构外的任何人无法获取密钥对数据进行解密，确保了金融机构云上数据的安全。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中的金融机构主密钥进行加密，该金融机构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。 此外，华为云内部的所有运维账号由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

编号	控制域	具体控制要求	华为云的应答
			位不同职责人员限定只能访问本角色所管辖的设备。

《“A”6375》第7.7.4章要求金融机构应满足完整性与注册技术操作要求，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
7.7.4	完整性与注册技术操作要求	RIR003：要求服务供应商提供的IT服务应记录所有活动并可追溯，能够确定“是谁（帐户、来源、目的地），是什么（活动、功能、交易），在哪里（服务、位置），什么时候（时间），以什么方式（事件模式、比率）”。	金融机构应对所有活动操作进行记录，记录的内容包括但不限于： • 用户ID； • 关键事态的日期、时间和细节，例如登录和退出； • 设备标识或位置（如可能），以及系统标识； • 网络地址和协议； • 系统成功及失败登录尝试； • 系统数据、文件及资源访问操作； • 系统配置修改； • 特权账号的使用。 金融机构还应建立日志数据的生命周期管理机制，确保可追溯所有活动的操作，日志的保留期限还应满足法规要求。同时，金融机构还应制定法证调查管理机制，防止对法律保护期间内的日志数据进行篡改，以支持安全事件的法证调查。 华为云的**云审计服务（Cloud Trace Service，简称 CTS）**为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。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

编号	控制域	具体控制要求	华为云的应答
7.7.4	完整性与注册技术操作要求	RIR023：要求金融机构/服务供应商应建立日志数据的生命周期管理机制，确保可追溯所有活动的操作，并遵守日志存储的法律和安全规定，对不可更改性和可访问性进行控制，以支持在发生安全事件和安全漏洞时的法证调查。	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。华为云内部已根据法规要求建立了法证调查管理机制，制定了规范的取证流程，以支持安全事件的法证调查。
7.7.4	完整性与注册技术操作要求	RIR010：要求服务供应商提供的设备和/或软件应基于以下阶段，确保满足开发生命周期要求： ● 需求分析； ● 采购/开发； ● 测试和批准； ● 实施； ● 运营和维护； ● 废弃和更换。 在开发生命周期过程中还必须考虑与（但不限于）以下内容相关的安全要求； ● 功能性安全需求； ● 输入数据类型和特征的验证； ● 功能和记录的颗粒度； ● 访问级别； ● 控制变更； ● 更新和补丁。	金融机构应在服务协议中明确规定服务供应商提供的设备和/或软件需满足的质量和安全要求，且金融机构应负责管理其所拥有的设备和/或软件的整个生命周期的安全。 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。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。为配合金融机构遵从监管要求，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，

编号	控制域	具体控制要求	华为云的应答
7.7.4	完整性与注册技术操作要求	RIR011：要求金融机构/服务供应商在IT服务交互中的设备和/或软件应经过批准，确保已对采购/制造/开发中定义的设计、功能、互操作性和安全性等进行了验证和部署。	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。
7.7.4	完整性与注册技术操作要求	RIR020：要求金融机构/服务供应商必须具有预防和纠正机制，以便在保护个人数据主体权利时响应个人数据主体的访问、修改和删除其个人数据的请求。	金融机构应决定如何利用产品或服务存储和处理内容数据，包括其中可能涉及的个人数据，金融机构负责内容数据的安全与合规。金融机构还应正确、全面地识别云端的个人数据，制定可保护个人数据的安全及隐私的策略并选择恰当的隐私保护措施，保障个人数据主体的权利。 作为云服务供应商，华为云负责为金融机构提供安全的云服务相关基础设施、云平台以及软件应用，以帮助金融机构保护其内容数据。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，在遵从金融机构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、生态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、金融机构及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足金融机构的安全需求。华为云已识别并分析了PDPL法规要求，更多信息请详见**《华为云阿根廷PDPL遵从性说明》**。

编号	控制域	具体控制要求	华为云的应答
7.7.4	完整性与注册技术操作要求	RIR021：要求金融机构/服务供应商在终止和/或无限期中断和/或重新定位服务的情况下，应建立信息资产的恢复机制，并确保信息安全和运营连续性。	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。 金融机构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，金融机构可通过两地互为冗余，如一地出现故障，系统在遵从监管要求的前提下自动将金融机构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，金融机构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。金融机构也可通过华为云的**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。 此外，华为云作为云服务供应商，为金融机构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，为金融机构持续有效提供服务，保证金融机构业务的开展。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
7.7.4	完整性与注册技术操作要求	RIR022：要求金融机构对计算机中使用的资源、信息及其所有者的当前身份进行核实，并在数据生命周期中指明删除参数、安全存储参数、验证参数。	金融机构应对其信息资产进行统一管理，定义信息资产的所有者，并建立数据全生命周期的安全管控措施，包括数据存储、删除等。 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，除金融机构外的任何人无法获取密钥对数据进行解密，确保了金融机构云上数据的安全。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中的金融机构主密钥进行加密，该金融机构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。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，金融机构首先做好数据分类，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。当金融机构使用云硬盘、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，确保金融机构只能访问到自己的数据。当金融机构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金融机构之间的协议约定，对存储的金融机构数据进行清除。

编号	控制域	具体控制要求	华为云的应答
			关于数据删除的详细信息请参见**《华为云数据安全白皮书》**。

编号	控制域	具体控制要求	华为云的应答
7.7.4	完整性与注册技术操作要求	RIR024：要求金融机构/服务供应商应建立存储加密和传输加密两种数据加密策略。	金融机构应确定如何配置环境和保护其数据，包括是否对数据进行加密（存储加密和传输加密）、确定所使用的安全功能/工具等。 金融机构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进行封装，使得金融机构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。对于传输中的数据，当金融机构通过互联网提供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。针对金融机构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。华为云为金融机构提供了**数据加密服务(Data Encryption Workshop，简称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，除金融机构外的任何人无法获取密钥对数据进行解密，确保了金融机构云上数据的安全。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）为金融机构创建和管理密钥，防止密钥明文暴漏在HSM之外，从而

编号	控制域	具体控制要求	华为云的应答
			防止密钥泄露，保护密钥安全。DEW还支持金融机构导入自有密钥作为金融机构主密钥进行统一管理，方便与金融机构已有业务的无缝集成、对接。同时华为云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。
7.7.4	完整性与注册技术操作要求	RIR025：要求金融机构应确保与其他第三方组织在数据的处理、存储、传输和恢复上是逻辑隔离的。必要情况下，服务供应商若要访问金融机构的设备/软件，必须获得金融机构的许可，并事先获得相关授权才可进行访问。	建议金融机构在数据生命周期的起始阶段就做好数据的区分和隔离。金融机构首先做好数据分类，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。 当金融机构使用云硬盘、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，确保金融机构只能访问到自己的数据。在金融机构自建存储的场景下，例如在虚拟机实例上安装数据库软件时，建议金融机构利用华为云的**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。华为云不会访问金融机构的云环境，除非在故障维护时，华为云会在得到金融机构的授权后（提供账号/密码）登陆租户的控制台或者资源实例以协助金融机构进行维护。

《“A”6375》第7.7.5章要求金融机构应满足控制和监督技术操作要求，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
7.7.5	控制和监督技术操作要求	RMC003：要求金融机构/服务供应商应对操作系统、数据库、通信链路、恶意代码检测/预防工具、网络安全设备、驱动程序和其他安全工具的安全配置、补丁更新等情况进行跟踪。跟踪内容包括但不限于： ● 特权和访问权限； ● 复制、保存和检索信息的过程； ● 设施/设备的可用性； ● 事件管理系统检测到的提示、警报和问题等。	金融机构应负责定义其运营模型，建立变更管理流程。可以使用服务供应商提供的工具来检测、跟踪其环境、资源的变化，以评估、审核对其环境、资源配置的变更。 金融机构可通过华为云的**云监控服务（Cloud Eye Service，简称CES）**、**弹性云服务器（Elastic Cloud Server，简称ECS）**、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。云监控服务目前可以监控多个云服务的相关指标，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。金融机构还可通过华为云的**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，以实现对其云上的业务进行多维度的安全检测。此外，华为云还为金融机构提供了**镜像服务（Image Management Service，简称IMS）**，IMS具有简单方便的镜像自助管理功能。金融机构可通过服务控制台或API对自己的镜像进行管理。华为云负责公共镜像的定期更新与维护向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息以便用户在部署测试、故障排除等运维活动时参考。 此外，为了保证华为云平台以及网络的安全、稳定运行，华为云内部采取了一系列管理措施，包括：漏洞分

编号	控制域	具体控制要求	华为云的应答
7.7.5	控制和监督技术操作要求	RMC004：要求金融机构应具备能够监控可疑事件或威胁的流程/工具，例如安装监控和分析网络威胁的系统，以便金融机构能够及时发现、预防和处理可疑事件或威胁： ● 预防。在确认操作之前，通过其他方法检测并触发与金融机构端的通知机制。 ● 反应。在确认可疑操作后，检测并触发与金融机构端的通知机制。 ● 假定。检测并假定由于客户对所进行的交易缺乏了解而导致的索赔或所涉及的金额的退款。	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
7.7.5	控制和监督技术操作要求	RMC006：从不同场景的IT服务操作记录中，要求金融机构/服务供应商应分析记录并对安全事件进行分类，定义时间限制和阈值、正常/意外行为的级别，并且根据每种安全事件分类建立行动计划和确定解决事件的时间限制。	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。 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。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（Cloud Trace Service，简称 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。 此外，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。华为云内部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

编号	控制域	具体控制要求	华为云的应答
			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。华为云内部还制定了信息安全事件管理规范，规定了安全事件的定级、升级规则以及不同级别事件的响应及解决时间限制等要求。
7.7.5	控制和监督技术操作要求	RMC014：要求金融机构/服务供应商应确定、记录和处理用于监控IT服务活动的资源、设施/设备和软件。	针对服务供应商提供的IT服务，金融机构应负责对IT服务定义运营模型，对IT服务活动进行监控和管理。 华为云的**云监控服务（Cloud Eye Service，简称CES）**可实现对金融机构自身云资源的使用情况和绩效的监控。华为云可以根据金融机构的需求按照SLA向金融机构提供服务报告，华为云也会安排专人负责金融机构方发起的尽职调查。华为云的云监控服务也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。 此外，为了保证华为云平台以及网络的安全、稳定运行，华为云内部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
7.7.5	控制和监督技术操作要求	RMC015：要求金融机构/服务供应商应针对所有关键业务定期执行漏洞测试和结果分析。	金融机构应对关键业务定期执行漏洞扫描和修复，并对结果进行分析。 金融机构可通过华为云的**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，以实现对其云上的业务进行多维度的安全检测。 此外，华为云内部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。

《“A”6375》第7.7.6章要求金融机构应满足事件管理技术操作要求，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
7.7.6	事件管理技术操作要求	RGI001：要求金融机构/服务供应商应至少每年一次执行风险分析和安全事件分析，并根据分析后的结果制定保护措施、安全意识和技能培训、日志管理机制、事件监控告警机制等。	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。金
7.7.6	事件管理技术操作要求	RGI002：要求应根据事件的类型/频率/模式等统计信息建立事件预警标识，并提供安全建议。	

编号	控制域	具体控制要求	华为云的应答
7.7.6	事件管理技术操作要求	RGI003：要求安全事件的管理可以以外包的方式执行，但必须与金融机构的人员进行协调。	融机构还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。 为配合金融机构遵从监管要求，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，根据安全事件对金融机构业务的影响程度进行事件定级，并根据安全事件的通报机制启动金融机构通知流程，将事件通知金融机构。当发生严重的安全事件，已经或可能对大量金融机构造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知金融机构。至少包括事件的描述、起因、影响、华为云已采取的措施、建议金融机构采取的措施等。在事件解决后，会根据具体情况向金融机构提供事件报告。 此外，华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云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（SIEM – Security Information and Event Management）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。华为云根据内部管理的要求，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

编号	控制域	具体控制要求	华为云的应答
7.7.6	事件管理技术操作要求	RGI005：要求针对检测到的事件应定期执行定级和逐步升级处理。	件响应人员，包括后备人员均需参与。测试场景将结合当下常见的网络安全威胁，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，若测试结果表明信息安全事件管理程序和流程等存在不足之处，将对相关文件进行更新。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。

《“A”6375》第7.7.7章要求金融机构应满足最低运行连续性技术操作要求，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
7.7.7	最低运行连续性技术操作要求	RCO001：要求提供必要的资源来创建、维护、更新和测试数据处理连续性计划。根据与服务供应商商定的要求、金融机构自身的要求和BCRA规定的要求，该计划必须具有可操作性。	金融机构应要求服务供应商制定业务连续性计划，特别是针对重大活动或影响广泛的活动，为此类活动分配足够的资源，符合金融机构自身业务连续性和法规要求。金融机构还应与关键服务供应商定期对业务连续性计划进行测试，并且必须以书面形式记录测试结果。 金融机构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，金融机构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的前提下自

编号	控制域	具体控制要求	华为云的应答
7.7.7	最低运行连续性技术操作要求	RCO002：要求金融机构/服务供应商应定义、记录、执行风险评估，以确定事件的影响（事件会干扰金融机构、服务供应商或分包的第三方的活动），包括但不限于： ● 确定关键资源，包括运营人员； ● 识别所有依赖项，包括流程，合作伙伴和分包的第三方； ● 发现对关键资源的威胁； ● 确定计划和非计划中断的影响，以及在不同中断时间下的影响程度； ● 建立最大可容忍的中断时间； ● 确定部分和全部恢复期； ● 确定关键资源的最大可容忍恢复时间； ● 估计业务连续性和最终恢复所需的资源以及备用地点。 此外，负责关键流程和资源的主要人员也应积极参与，以确保完全涵盖所有IT服务相关的人员。	动将金融机构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，金融机构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。金融机构也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。 此外，华为云作为云服务供应商，为金融机构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，为金融机构持续有效提供服务，保证金融机构业务的开展。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。
7.7.7	最低运行连续性技术操作要求	RCO003：数据处理连续性计划应包括但不限于以下内容： ● 根据每个确定的过程/资源/行动，进行手动和自动化的应急操作程序； ● 管理人员、供应商、服务应急资源和其他实物和逻辑资源的位置转移和运输； ● 进行恢复/还原已承诺资源的程序。	
7.7.7	最低运行连续性技术操作要求	RCO004：数据处理连续性计划应至少定期每年测试一次。测试应与计划内容保持一致且符合RCO002要求。测试还应定期以书面形式通知所有负责人员、组织以及过程的参与者。	

6 华为云如何遵从及协助客户满足 BCRA《“A”7266》的要求

《“A”7266》主要针对金融机构、提供支付账户的支付服务提供商以及金融市场基础设施。该准则主要包括一系列有效的网络事件响应和恢复实践，致力于提高整个金融生态的网络恢复能力。

金融机构在遵循《“A”7266》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《“A”7266》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。

6.1 治理

《“A”7266》第2.1章制定了有关网络事件响应和恢复的治理框架，对应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
2.1.1	文化	实体的管理层应创建一个组织环境，鼓励通过为此目的设立的渠道报告或升级网络事件，同时应考虑： 2.1.1.1 为实体的所有级别员工建立培训计划，鼓励积极主动的行为，接受网络事件发生的可能性，并从错误中学习。 2.1.1.2 推进积极的网络事件管理文化，并确保这些信息作为改善准备阶段的来源。 2.1.1.3 在网络事件响应与恢复活动的准备过程中，与供应商和第三方共同推进持续的、不间断的行动，以便及时应对不同情况。	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。如果客户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。 金融机构应当建立信息安全事件管理机制，其中应至少包括：事件管理流程中的角色和职责、员工培训计划及事件衡量指标。 华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收

编号	控制域	具体控制要求	华为云的应答
2.1.2	组织、角色、职能和责任	2.1.2.1 响应与恢复活动治理是组织整体治理的组成部分。这些准则的目标和优先级应与组织的总体风险管理保持一致，并且必须定义促进决策所需的角色、责任和程序。 2.1.2.2 组织的管理层负责定义网络弹性的目标，并负责实施相关政策、程序和控制措施。 2.1.2.3 针对应对网络事件时的协调和沟通，建议定义“协调员”的角色。该角色既可以是个人，也可以是团体。“协调员”必须有能力在网络事件发生期间，根据关键程度做出决策，发起某些活动并联系相关人员。 2.1.2.4 网络事件响应与恢复活动有助于确保金融服务的安全性和可靠性。实体的管理层不但可以通过提供支持来推动这些活动，还可以通过分配必要的预算来购置技术工具或在组织的各个层面实施意识、培训和沟通计划等。	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（SIEM – Security Information and Event Management）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。华为云已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。
2.1.3	活动的报告、衡量标准和责任	通过建立衡量标准来评估网络事件的影响，衡量响应和恢复活动的效率，并向当局报告，从而实现有效管理。根据事件的关键程度和/或优先级，定义关注的紧急程度和恰当的升级级别。例如，高度关键性的网络事件很可能需要向实体的管理层报告。	

6.2 规划和准备

《“A”7266》第2.2章提出了建立和维护组织响应网络事件的能力的具体措施，对应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
2.2.2	策略、渠道和沟通计划	2.2.2.1 应建立包括所有潜在的内部和外部的利益相关者的联系名单，并根据确定的情况和标准告知他们。 2.2.2.2 建议与参与者和每个确定的受众共同建立沟通策略。计划可以包括根据网络事件的类型，考虑恰当的或可用的沟通渠道所确定的报告内容模板。考虑到与之共享信息的受众，以及使相关人员了解情况的需要，为减少不确定性和增加信心，评估事件发生期间公布信息的顺序是可取的。	金融机构应梳理其利益相关方及相关方联系方式。金融机构还应制定事件沟通策略，用以明确事件发生后的沟通渠道、报告内容模板等。 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。

编号	控制域	具体控制要求	华为云的应答
2.2.3	事件评估的场景和标准	2.2.3.1 计划和程序应包括基于威胁情报支持的低概率和高影响事件的可能的场景的重要性。这些情景可以是： i）在测试业务连续性计划或响应和恢复计划期间进行评估，以及 ii）与外部各方、有关当局、服务供应商或第三方进行内部测试（如适用）。 2.2.3.2 RRCI活动的有效性可以在测试期间和应对实际事件时进行评估。建议独立的观察员参与，以保持客观的评估，并获得每个步骤的准确记录，以及网络事件期间和之后所采取的行动和决策的记录。	金融机构应当建立态势感知管理机制，确保网络中的信息及信息处理设施得到保护。 华为产品安全事件响应团队（PSIRT – Product Security Incident Response Team）于2010年正式成为国际应急响应论坛FIRST成员之一，通过该组织可实现与471个成员交流业界最佳实践和安全信息；华为PSIRT已经建立成熟的漏洞响应机制，针对云的自运营的特点，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，降低对租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，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。更多信息请参见**《华为云安全白皮书》**8.2漏洞管理。

编号	控制域	具体控制要求	华为云的应答
2.2.4	恢复的基础设施	根据实体的规模、复杂性和风险，有必要提供7*24小时监控或使用第三方安全服务，以实现识别、检测、响应和调查可能影响基础设施、服务和/或客户的网络事件的目标。	金融机构应对使用的云服务进行管理和监控，确保供应商可按照相关要求提供足够的资源和服务。 华为云的云监控服务（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。
2.2.5	灾难恢复与弹性基础设施	通过使用多样化的基础设施和关键系统的备份、灾难恢复站点或具有不同地理风险状况的替代站点，建立了恢复能力。这需要识别外部第三方的风险，评估并采用可用的缓解技术。	金融机构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的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。

编号	控制域	具体控制要求	华为云的应答
2.2.6	研究的能力与记录	适当的日志管理的开发包括收集与存储事件调查和分析所需的系统日志的工具。收集的“日志”的类型和保留期限必须根据信息的分类、现行的标准和法规事先确定。针对保存证据、分析控制故障、识别安全问题和与网络事件相关的其他原因，技术和取证能力是必要的。如果不具备此能力，那么可以雇佣第三方服务。从事取证工作的人员必须经过充分的培训，并遵循标准化的程序，以在调查期间保持证据、数据和系统的完整性。	金融机构应建立对敏感数据、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，作为云服务供应商，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。

编号	控制域	具体控制要求	华为云的应答
2.2.7	服务供应商	为确保在网络事件发生期间做出充分响应，有必要掌握与第三方、服务供应商约定的服务的细节，和协议的关键细节，例如服务供应商的联系信息，有效期以及商定的服务水平。另外，分包商的服务协议也需要审查。就服务的复杂性和规模而言，应评估供应商的网络事件，特别是其在第三方数据存储方面的网络安全实践的风险，和/或供应链管理或供应商系统中的软件的安全漏洞。	金融机构应确保其选定的服务供应商可按照合同及SLA约定提供服务。 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。目前，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。如有必要，金融机构可以通过官方渠道向华为云申请获取证书以及审计报告的副本。为配合客户遵从监管要求，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。华为云参照ISO27001构建了信息安全管理体系，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、以及业务连续性等。

6.3 分析

《“A”7266》第2.3章涉及与取证分析、确定网络事件的关键性和影响以及调查根本原因相关内容，对应控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.3.1	网络事件分类	2.3.1.1 需要事先定义网络事件分类规则，以便根据以下因素对网络事件进行分类：事件类型、威胁参与者、威胁媒介及其影响，以及事先建立的根据系统或服务的关键性对事件进行优先排序的评估框架。 2.3.1.2 对网络事件进行事先分析有助于确定及时关注的优先次序，分配资源以减轻影响，恢复服务以及允许以通俗的语言传达信息。设置关键程度等级旨在做出立即响应。此外，这种方法也允许在不完全了解事件的情况下进行初步关注。	金融机构应当对信息安全事件制定分类标准，并按照此标准对事件处理进行优先级排序。 华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云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（SIEM – Security Information and Event Management）系统如rcSight、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。至少包括事件的描述、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，会根据具体情况向客户提供事件报告。

编号	控制域	具体控制要求	华为云的应答
2.3.2	取证调查和分析	2.3.2.1 对于事件的取证调查，需要系统和设备的日志或审计日志。分析警报、指标（安全和系统）、调查和关联事件使响应团队能够确定事件的影响，并可能识别其来源。对于响应，还需从参与交互的计算机设备中检索数据，例如连接到网络的设备、正在运行的进程、用户会话、打开的文件、相关设备的配置和内存内容等。必须确保此类数据的完整性，以便进行恰当的分析。 2.3.2.2 在进行取证调查时，获取系统日志的系统必须是同步的。 2.3.2.3 为快速评估网络事件的威胁和原因，建议使用各种内部和外部信息来源。	金融机构应根据其风险偏好制定云上取证流程和控制措施，确保进行云上取证时保证数据的机密性、完整性和可用性。 华为云在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令。同时，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，确保了云上取证过程中，数据的机密性、完整性和可用性。此外，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，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

6.4 缓解

《“A”7266》第2.4章规定了降低网络事件对运营与服务的影响的缓解措施，对应控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.4.1	控制、隔离和消除	2.4.1.1 根据网络事件的类型部署控制措施，防止其在目标主体以及与之连接或相关的其他目标主体内部造成进一步的损害。获取关于当前网络威胁的信息，并分析潜在的影响，有助于确定控制措施，监测网络活动和决策。在发生事故的情况下，确保可以及时恢复。 2.4.1.2 在发生重大事故，决定关闭、断开或隔离部分系统或网络作为缓解措施，还是继续提供服务时，应考虑成本、对“业务”的影响、运营风险和其他因素。 2.4.1.3 在收集和保存证据后，必须删除攻击者引入的所有要素，如恶意代码和数据等。此外，必须纠正受影响的系统配置或更改。消除该事件的活动可以包括修补和检查漏洞等任务。	金融机构应制定网络安全风险评估机制，基于已收集到的网络威胁信息，分析潜在影响，确定预防措施。发生重大事件后，应及时应对和补救。 金融机构应按照其风险偏好对使用华为云服务进行风险评估，风险评估结果应记录在案，并按照风险评估的结果决定监控、管理华为云服务的机制（如评估周期）。 华为云将按需配合客户进行风险评估工作。

编号	控制域	具体控制要求	华为云的应答
2.4.2	“业务连续性”措施	根据网络事件的严重性，以及其后果或影响，业务连续性计划可以被启动。	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。如果客户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。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。为配合客户遵从监管要求，华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了恢复策略。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的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。

6.5 恢复

《“A”7266》第2.5章规定了以安全的方式将受影响的业务和服务恢复到正常状态所进行的活动，对应控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.5.1	确定优先次序	必须根据业务流程的关键程度确定恢复活动的优先次序，以便恢复数据与支持它们的系统。此外，强调更新内部和外部联系人名单的重要性。	金融机构应制定事件恢复策略。其中，应按照业务影响分析（BIA）的结果来制定业务恢复的优先级排序，并维护内外部联系人名单及联系方式。在事件恢复过程中，金融机构应对恢复过程进行监控。恢复完成后，应对其信息资产进行策略，确保其完整性没有被破坏。 华为云有专门的团队负责和客户的沟通联系，客户可以通过工单服务寻求华为云的帮助。
2.5.2	数据恢复	2.5.2.1 为满足数据恢复的业务要求，需要在自己的位置和第三方位置都获取必要的信息。当发生网络事件时，需要保证数据的完整性，即数据在恢复前没有被操纵或破坏。为确保数据的完整性、可用性和可读性，还需进行定期的恢复测试。 2.5.2.2 恢复活动最好有自动化的、记录在案的和经过测试的程序，从而减少人工恢复中可能出现的人为错误的风险。为恢复受影响的系统，通常会使用未被破坏的系统映像和快照，这些映像和快照必须定期检查、测试和安全存储，以减少损坏或破坏。 2.5.2.3 当无法恢复所有系统时，可以考虑部分恢复，并规定以较低的能力水平运行；确定系统重新安装和重新配置的关键里程碑，以确保有效恢复。	
2.5.3	监测	在恢复技术基础设施资产的过程中，监测网络、系统和服务供应商对于检测异常活动而言是重要的。在适当的情况下，根据它们的规模、复杂性和风险，最好在与供应商的服务协议中包含数据恢复期间的监控功能的内容。	

编号	控制域	具体控制要求	华为云的应答
2.5.4	验证	在系统和服务恢复正常运行之前，必须对恢复的IT资产的完整性进行验证，并确保它们不受损害、功能齐全并满足安全要求。	
2.5.5	记录活动	应尽可能记录从发现事件到最终解决期间的所有行动，以便于后续跟踪。一旦业务恢复，日志将有助于恢复所采取的操作，以复原事件发生前的条件，或在恢复操作不成功时排除故障。在恢复过程中使用的工具，如脚本、配置更改等，应该被记录下来，以便将来使用或改进当前的流程和/或系统。	

6.6 协调与沟通

《“A”7266》第2.6章规定了金融机构在网络事件的生命周期中应与内外部的利益相关者进行沟通协调，使其了解并关注网络事件，对应控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.6.1	及时升级	为及时处理事件，应根据关键性评估框架和预期的升级级别，及时向每个利益相关方报告事件。同样重要的是，在服务协议中规定与服务供应商的沟通。必须提供合理的保障措施，以确保在与内部领域和外部组织的沟通中提供完整和准确的信息。	金融机构应与服务供应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。在服务协议中，金融机构应与服务供应商约定信息安全的保障措施，用以确保金融机构的信息完整性和准确性。 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。

编号	控制域	具体控制要求	华为云的应答
2.6.2	网络事件的通知	2.6.2.1 有关网络事件的相关信息应根据相关监管框架规定的时限向当局报告。为支持有效和及时地报告网络事件，它们需要制定内部指南，说明不同类型的事件应该何时和向谁报告。为加强理解，可以提供不同类型的事件和报告的例子。 2.6.2.2 此外，应告知可能受网络事件潜在破坏影响的利益相关者，以便他们能够启动自己的响应和恢复计划。共享的信息应该是准确、及时、清晰和相关的；内部和外部利益相关者也应定期得到通知，但在紧急情况下应立即进行沟通。在恢复关键服务时也应告知条件或限制。每条信息都应说明期望收件人采取的行动，而且应事先确定频率。	金融机构应制定网络事件通知流程，流程中应包括通知和上报利益相关方（如数据控制者、数据主体、监管机构等）的要求和步骤说明。 为配合客户满足数据丢失和泄露事件上报利益相关方的要求，华为云设置 7*24 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。除此之外，华为云已建立了数据泄露事件处理机制，如有必要，华为云会按照适用法律法规的要求进行事件通报。
2.6.3	向公众通报网络事件	沟通策略需要事先确定，建议成立一个多学科的沟通团队，包括来自受影响的业务线、人力资源、新闻和沟通、法律、技术和网络安全的代表，以及事件协调员。根据事件的类型，可能会召集其他专家来协助。为避免沟通上的混乱，发言人需要整合专家和管理层的信息和各相关方面的信息，向媒体提供一致的最新信息和消息。应促进对传统媒体和社会媒体等沟通渠道的战略性使用。	
2.6.4	信息交流	2.6.4.1 建议各组织通过平台或以其认为合适的方式实施，共享有关网络威胁和网络事件、有效的网络安全战略和风险管理实践的信息。及时共享技术信息十分有益，例如泄露的迹象和被利用的漏洞，确保遵守保密协议所需的匿名性。 2.6.4.2 沟通渠道需要正规化，并确保共享信息的可用性、完整性和保密性。参与者还必须定期验证沟通渠道和联系人名单的可用性。	

6.7 持续改进

《“A”7266》第2.7章规定了基于经验改善应对网络事件的能力时应考虑的程序，对应控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
2.7.1	倡议	与其他参与者共享知识和技能，创建空间或论坛来讨论事件和针对网络安全漏洞和威胁的缓解策略，极其重要。同时，当局应共同努力促进信息和良好实践的交流。这种交流使参与者能够从信息中受益，有助于相互了解并提高响应和恢复能力。	在事件处理完成后，金融机构应对引起网络安全事件的漏洞和威胁进行分析，根据业务影响分析（BIA）的结果部署相应的管控措施。同时，金融机构应组织对本次事件应急响应处理过程进行总结汇报，分析本次事件处理的及时性和有效性，以及过程中取证分析的质量。
2.7.2	事后分析	一旦网络事件结束，应审查是否遵循了既定程序，所采取的行动是否有效，以及： i）对安全警报的反应速度， ii）确定事件影响及其严重程度的及时性， iii）取证分析的质量， iv）实体内部升级的有效性，以及 v）内部和外部沟通的有效性。	
2.7.3	演习	演习既可以是内部的，也可以是与第三方的，测试应急计划和危机管理，与供应商或同行的关系，以准备和改善各参与方之间的协作。这些演习包括不同的场景，以验证响应和恢复活动协调的有效性。为提高网络弹性，建议当局参与此类演习。	金融机构应制定事件应急计划和危机处理流程，并按照该计划和流程定期进行应急演练，用以提高金融机构的网络安全弹性，提高事件应急能力。 应急演练过程中如需华为云的参与，华为云会安排专人积极配合客户发起的演练需求。

7 结语

本文描述了华为云为客户提供的云服务如何遵从阿根廷金融行业的监管要求，并表明阿根廷共和国中央银行（BCRA）发布的重点监管要求，有助于客户详细了解华为云如何遵从阿根廷金融行业监管要求，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、构建和部署符合阿根廷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。

本文仅供参考，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阿根廷金融行业监管要求的遵从性。

8 版本历史

日期	版本	描述
2022年4月	2.0	合规要求更新
2021年5月	1.0	首次发布