华为云墨西哥金融行业监管遵从性指导

文档版本 1.0

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，墨西哥财政和公共信贷部(SHCP)、国家银行和证券委员会 (CNBV)、墨西哥银行（Banxico）发布了一系列监管指令和指南，对墨西哥金融机构的网络安全、科技外包管理等方面提出了相关要求。

华为云作为云服务供应商，致力于协助金融客户遵从监管要求，持续为金融客户提供遵从金融行业监管要求的云服务及业务运行环境。本文将针对墨西哥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遵从监管要求。

1.2 适用的墨西哥金融监管要求简介

墨西哥金融体系的监管实体主要包括墨西哥银行（Banxico）、财政和公共信贷部（SHCP）及其下属六个部门。

墨西哥银行（Banxico）： 为墨西哥中央银行，是墨西哥金融体系中最重要的机构，是该国所有银行的监管者和控制者。

财政和公共信贷部（SHCP）： 为墨西哥中央集权的政府机构，其负责人由墨西哥总统任命。其政府职能旨在从各种来源获取货币资源，为国家的发展提供资金。

国家银行和证券委员会（CNBV）： 属于SHCP下属的分支机构，具备技术自主权和执行权，负责在其职权范围内对墨西哥金融机构进行监督管理，维护和促进整个墨西哥金融体系的稳定发展，保护公众利益。

国家保险和债券委员会（CNSF）： 属于SHCP下属的分支机构，负责监督墨西哥保险业和担保业遵守相关的监管框架，帮助服务范围扩大到尽可能多的人员。

墨西哥银行、SHCP和CNBV共同颁发了针对信贷机构、金融科技机构及证券机构相关的法律及其配套通用规定：

- **信用机构法及其通用规定：** 包括《信用机构法》、《适用于信用机构法的通用规定》。

- **金融科技机构监管法及其通用规定：**包括《 金融科技机构监管法 》、《 金融科技机构监管法二级监管要求 》、《 金融科技机构监管法的通用规定 》。
- **证券市场法及其通用规定：**包括《 证券市场法 》、《 适用于证券交易所的通用规定 》、《 适用于经纪公司的通用规定 》、《 适用于证券存管机构的通用规定 》。

墨西哥银行、SHCP和CNSF共同颁发了针对保险机构及担保机构相关的法律及其配套通用规定：

- **保险与担保机构法及其通用规定**：包括《 保险与担保机构法 》、《 适用于保险与担保机构法的通用规定 》。

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。
- **ITF：**

  金融科技机构，即融资机构和电子支付基金机构。
- **技术基础设施：**

  ITF使用的操作系统、数据库、软件和应用程序。

2 华为云的认证情况

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

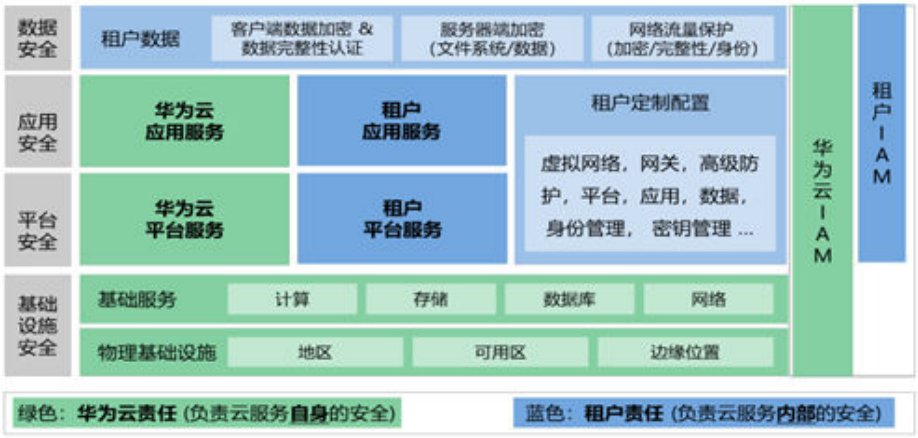
认证	产品介绍
网信办网络安全审查（中国）	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。
MTCS Level 3认证（新加坡）	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3 等级认证。
OSPAR认证（新加坡）	OSPAR是新加坡银行业工会（ABS）对外包服务提供商出具的审计报告。华为云通过了新加坡银行协会(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：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《信用机构法》及相关通用规定的要求

信用机构法及其通用规定共同阐述了墨西哥金融机构选择使用云服务时，墨西哥国家银行和证券委员会 (CNBV)对相关活动的监管方式及建议、以及金融机构需处理的事项。《信用机构法》为指令，具有法律效力，为高阶的管理要求，《适用于信用机构法的通用规定》为指南，是针对信用机构法指令的落地指导。

墨西哥金融机构在遵循《信用机构法》及其相关通用规定的要求时，华为云作为云服务提供商，可能会参与到要求所涉及的部分活动中，以下内容将总结《信用机构法》及其相关通用规定中与云服务提供商相关的控制要求，并阐述华为云作为云服务提供商，会如何帮助金融机构满足相关控制要求。

5.1 华为云如何遵从及协助客户满足《信用机构法》的要求

编号	控制域	具体控制要求	华为云的应答
46.2.1	第一节：关于通用规则	金融机构与第三方签订外包服务合同需遵守以下规定： 1. 遵守与提供的服务相关的技术和业务准则，以及在提供服务时保障银行系统用户信息的保密性的相关规定。 2. 金融机构应制定第三方提供服务时在控制程序方面的要求。 3. 金融机构应制定相应的监控程序和政策，以监控第三方履行合同的情况。其中应包括第三方有义务根据CNBV委员会以及机构的外部审计员的要求提供服务有关的记录、信息和技术支持。 4. CNBV委员会和金融机构有权在任何时候对第三方服务商进行审计、监督和监测，且金融机构有义务向CNBV委员会提供相关报告。CNBV委员会可根据对第三方的审计结果向金融机构提出意见或纠正措施。 5. 第三方的雇员以及离职员工也应遵守本条规定。 6. 第三方应配合金融机构选择其他外包服务提供商共同提供服务。 7. 若金融机构未能遵守本规定，CNBV委员会可在机构获得听证权利后，下令部分或全部、暂时或最终暂停通过有关第三方提供的服务或委托。	金融机构应在与第三方签订的合同中约定对第三方所提供服务的安全控制的要求，并制定第三方绩效监控政策监控第三方对服务合同的履行情况。 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，可根据金融机构的需求进行定制化。

编号	控制域	具体控制要求	华为云的应答
46.2.2	第一节：关于通用规则	1. 金融机构与第三方签订外包服务，不能免除金融机构或其董事、雇员遵守本法律条例的规定和相关通用规定的义务。 2. CNBV委员会可以通过金融机构要求外包服务商提供其服务相关的信息，包括书籍、记录和文件。	金融机构与第三方签订外包服务，但不能外包法律责任，金融机构或其董事、雇员均应按本法要求承担相应的责任。金融机构应配合CNBV委员会，向金融机构的外包服务商收集相关信息。 华为云会安排专人积极响应金融机构的要求，并提供相关材料。
126	单独章节：检查和监督	金融机构有义务向CNBV委员会提供检查和监督所需的支持，包括： 1. 提供数据、报告、记录、文件、信函以及其他所需文件。 2. CNBV委员会可进入其办公室场所和其他设施进行检查。	金融机构应配合CNBV委员会的检查工作。 华为云会安排专人积极配合金融机构或CNBV委员会发起的审计工作。

5.2 华为云如何遵从及协助客户满足《适用于信用机构法的通用规定》的要求

编号	控制域	具体控制要求	华为云的应答
318	第一节：通用规定	金融机构与第三方签订服务合同应遵守以下要求: 1. 提供报告说明选择第三方服务提供商的标准和政策。 2. 在服务合同或在第三方无条件接受的文件中规定： a) 接受机构的外部审计员、CNBV委员会或CNBV委员会本身指定的第三方机构访问外包服务商的物理场所，以核实机构所订的服务或委托是否允许金融机构遵守适用于它的法律规定。金融机构可以指定一名代表陪同访问。 b) 接受机构对上述合同约定的服务或委托进行审计，以核实是否符合适用于机构的规定。 c) 应机构的要求，向机构的外部审计员和CNBV委员会或其指定的第三方提供与服务相关的系统、记录、手册和文件。 d) 如果第三方服务提供商的企业宗旨或内部组织发生任何可能影响到合同所涉及的服务提供的变化，至少提前30日历日通知金融机构。 3. 有政策和程序来监督第三方的表现和合同履行情况。这种政策和程序应包括以下有关事项： a) 限制第三方分包服务的可能性。 b) 金融机构信息的保密性和安全性。 c) 机构和第三方的义务，监测第三方对合同的遵守的程序，不遵守可能产生的法律后果。	金融机构应将相关要求写入与第三方签订的合同。金融机构应制定第三方服务提供商的选择标准、监控第三方绩效和合同履行情况的机制。 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，可根据金融机构的需求进行定制化。华为云可能会随时自行修改或中止服务或修改或移除服务的功能。如果您订阅的服务发生重大变更或中止，我们会通过在我们的网站发布通知或其他方式通知您。

编号	控制域	具体控制要求	华为云的应答
		d) 解决与服务合同有关的争端的机制。 e) 业务连续性计划，包括发生灾害时的应急程序。 f) 制定准则，确保第三方定期接受与所签订的服务有关的信息。 g) 如果拟签约的服务或委托涉及技术或电信基础设施的使用，则应遵守本规定中规定的最低安全准则。 4. 每两年进行一次审计，以核实遵守本章以及最低安全准则规定的情况（如适用）。并向董事会和审计委员会汇报审计结果。 5. 规定总经理、审计委员会以及机构的内部审计员根据其权限监督外包服务商提供服务所使用的技术、信息处理基础设施的和信息的处理、控制和安全机制。 6. 制定准则，允许金融机构评估合同，以识别可能影响机构业务的情况，包括： a) 机构在发生突发事件时，有能力保持业务的连续性。 b) 寻找第三方来取代最初签约的一方的复杂性和所需的时间。 c) 在做出对机构本身的行政、财务、业务或法律状况有重大影响的决定时受到的限制。 d) 当其公司宗旨或内部组织的任何变化可能会影响作为合同所约定的服务的提供时，应至少提前30日历日通知机构。 e) 暂停服务可能对机构的财务、声誉和运作产生的影响。 f) 金融机构信息的脆弱性。	

编号	控制域	具体控制要求	华为云的应答
		7. 金融机构的总经理应负责审批第三方服务提供商的选择政策和标准。	
326	第三节：与第三方签订服务或委托合同	金融机构与第三方签订服务合同时，应在签约前向CNBV委员会说明与第三方约定的最低安全准则，并在签约前至少20个工作日送交CNBV委员会，金融机构需得到CNBV委员会同意后才可开展相关外包服务。	金融机构在计划与第三方签订服务合同前，需至少提前20个工作日向CNBV委员会提交相关材料并获取批准，提交的相关材料应说明利用第三方服务开展的业务类型，以及如何遵守本通用规定要求的最低安全准则。 华为云将配合金融机构提供相关上报材料。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。
327	第三节：与第三方签订服务或委托合同	326条所指的通知应由金融机构总负责人签署，如果服务涉及技术或电信基础设施的使用，通知还应包含一份技术报告，具体说明利用第三方提供的技术基础设施开展的银行业务或服务的类型，以及遵守本规定服务采购的最低安全准则。	

编号	控制域	具体控制要求	华为云的应答
328	第三节：与第三方签订服务或委托合同	如果第三方提供的服务部分或全部在国家领土之外或由国外居民提供或执行，金融机构应在签订合同前至少20个工作日向负责监督的CNBV委员会副主席申请有关授权，并提交下列文件： 1. 与之签订合同的第三方或委托代理人所居住的国家信息，其国内法对个人数据提供的保护措施，或者居住国与墨西哥签署了关于此类事项的国际协议。 2. 机构必须向CNBV委员会声明，他们将在位于墨西哥合众国的主要办事处至少保留与评估、审计结果和业绩报告有关的文件和资料。同样，当CNBV委员会要求时，他们应提供此类文件的西班牙语版本。 3. 金融机构在协议中说明签订服务或委托合同不会影响机构对本规定的遵守，并得到董事会或审计委员会的批准。	金融机构应按照相关要求制定与第三方的合同。当金融机构与墨西哥境外机构或与墨西哥境外居民签订外包服务合同时，应在签订合同前20个工作日向CNBV委员会申请并获得授权。金融机构在向CNBV委员会申请时，应按本通用规定的要求提供相关文件。 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，可根据金融机构的需求进行定制化，华为云会安排专人积极配合金融机构提供相关材料。
330	第四节：最后规定	1. 金融机构在任何时候都应对其授权的第三方提供的服务负责，以及对第三方发生的不遵守规定的情况负责。 2. 本规定不应影响第三方或委托代理人或其雇员因违反适用法律规定而可能承担的民事、行政或刑事责任。 3. 同样，本规定也应在机构与第三方或委托代理人之间签订的合同中确定。	金融机构应按照相关要求制定与第三方的合同。 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，可根据金融机构的需求进行定制化，例如在合同中说明双方在本法规定下的职责划分。

编号	控制域	具体控制要求	华为云的应答
332	第四节：最后规定	当CNBV委员会认为机构的财务稳定性、业务连续性或对公众利益的保护可能受到影响，或机构未能遵守本规定和其他适用规定时，CNBV委员会可在机构获得听证权利后，下令部分或全部、暂时或最终暂停通过有关第三方提供的服务或委托。除非在行使听证权时，金融机构提交一份规范化方案交由CNBV委员会审核，CNBV委员会在30个日历日内做出适当决定。	当CNBV委员会认为金融机构不满足本通用规定要求的场景时，金融机构应配合提交一份规范化方案交由CNBV委员会审核，必要时需暂停与相关第三方的合同。 华为云会安排专人积极配合金融机构提供相关材料。
333	第四节：最后规定	1. 机构应拥有一份清单，其中包含签约服务和业务的类型和特点，以及服务提供者或委托代理人的相关信息，并区分在本国境内或境外居住的人。 2. 机构应在本条提及的清单中注明其授权的服务提供者或委托代理人，并在必要时将名单提供给CNBV委员会审查。 3. 在不影响上述规定的情况下，机构应在财政年度结束后90个日历日内向CNBV委员会提交一份年度报告，详细说明机构根据其制定的程序进行审查的结果。	金融机构应制定并维护其供应商清单，清单中应包括服务提供商的基本信息。例如服务提供商所提供的服务清单、服务类型以及服务提供商所处地理位置。 华为云目前已陆续在全球部署多个地理区域（Region）和多可用区（AZ），可支持金融机构根据其需求选择数据存储位置。 如金融机构需向监管机构提交年度报告，华为云会安排专人积极配合金融机构提供相关材料。

编号	控制域	具体控制要求	华为云的应答
334	第四节：最后规定	机构在制定与第三方服务合同有关的政策时，应考虑以下内容： 1. 第三方执行措施或计划的能力，包括性能、可靠性、业务连续性。 2. 处理与提供的服务或委托有关信息时的完整性、准确性、安全性、保密性、安全性、及时性和可靠性，以及访问控制措施。 3. 金融机构用来评估合同遵守情况的方法。 4. 定期评估服务质量的标准和程序。 5. 第三方提供合同规定服务的连续性的能力，或金融机构在任何情况下都有其他选择，以减少机构运作的脆弱性。 6. 机构的风险容忍度。 7. 机构在综合风险管理中识别、衡量、监测、限制、控制、通报和披露本章所述服务可能产生的风险的能力。 8. 内部控制系统遵守本规定的能力。 9. 董事会应指定一名负责人，可以是内部审计员，负责监督、评估并定期向董事会报告服务提供者的业绩，以及对适用规定的遵守情况。 10. 董事会应至少每年审查一次第三方供应商的选择制度，并根据第三方的业绩评估结果进行修改。	金融机构应按照相关要求制定与第三方的合同。 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，可根据金融季候的需求进行定制化。 为了向客户提供持续、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。 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。

编号	控制域	具体控制要求	华为云的应答
附件52	技术支持服务采购的最低安全准则	金融机构采购技术支持服务时应考虑以下安全准则： 1. 安全方面 a) 确保采用以点对点加密方式传输敏感用户信息的措施。 b) 金融机构应设立一个独立于业务、审计和系统领域的安全官，安全官应负责管理访问控制，安全官拥有查阅被授权访问记录的权限，被授权人员的访问记录应保留。 2. 审计和监督 a) 金融机构应该至少每两年对第三方数据中心的基础设施的安全控制和运行情况进行一次审计。	金融机构应采用加密的方式传输用户的敏感信息，并设立一个独立的安全官，赋予该安全官查阅审计访问用户信息记录的权限，金融机构应至少每两年对第三方数据中心进行安全审计，检查第三方数据中心的安全措施的执行情况。 对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过如下方式提供： **虚拟专用网络（VPN）**：VPN用于在远端网络和VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云上，为租户提供端到端的数据传输机密性保障。通过VPN 在传统数据中心与 VPC 之间建立通信隧道，租户可方便地使用华为云的云服务器、块存储等资源，通过将应用程序转移到云中、启动额外的 Web 服务器来增加网络的计算容量，实现了企业的混合云架构的同时，也降低了企业核心数据非法扩散的风险。 目前，华为云采用硬件实现的 IKE（密钥交换协议）和 IPSec VPN 结合的方法对数据传输通道进行加密，确保传输安全。 **应用层TLS与证书管理：**华为云服务提供 REST 和 Highway方式进行数据传输，REST网络通道是将服务以标准RESTful的形式向外发布，调用端直接使用HTTP客户端，通过标准 RESTful形式对 API 进行调用，实现数据传输； Highway 通道是高性能私有协议通道，在有特殊性能需求场景时可选用。上述两种数据传输方式均支持使用传输层安全协议（TLS – Transport Layer Security）1.2版本进行加密传输，同时也支持基于 X.509 证书的目标网站身份认证。 **SSL证书管理服务（SCM）**则是华为云联合全球知名数字证书服务机构，为租户提供的一站式 X.509 证书的全生命周期管理服务，实现目

编号	控制域	具体控制要求	华为云的应答
			标网站的可信身份认证与安全数据传输。 华为云会安排专人积极配合金融机构发起的审计要求。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。

编号	控制域	具体控制要求	华为云的应答
附件64.2	信息安全事件报告	I. 机构信息 a) 机构的名称。 b) 首席信息安全官的全名，以及他/她的电话号码和电子邮件地址。 II. 在加密的数字媒体中附上信息安全事件的以下信息 1.信息安全事件的描述。 2.受影响的账户。 3.受影响账户的状态（被封锁、被暂停、被激活）。 4.受影响的网络区域（互联网、内部网络、管理网络等等）。 5.受影响的系统类型（文件服务器、网络服务器、邮件服务、数据库、工作站、移动设备等等）。 6.操作系统（注明版本）。 7.受影响组件的协议或服务。 8.本机构受影响系统的组件数量。 9.涉及的应用程序（指定版本）。 10.受损设备的信息（品牌、软件版本、固件等）。 11.信息安全事件对服务造成的影响。 12.以比索计算的损失金额。 13.以比索为单位收回的金额。 14.信息安全事件的状态（已解决或未解决）。 15.指出该信息安全事件是否已报告给任何当局。如果是这样，请注明授权和日期。 16.攻击来源的公共IP地址、电子邮件地址或域名。 17.使用的通信协议。 18.涉及网站。 19.检测到的恶意软件。	金融机构应按照本通用规定要求的信息安全报告内容，在发生信息安全事件时按照要求及时上报CNBV委员会。 华为云将配合金融机构提供相关上报材料，配合金融机构满足监管通知的工作。

编号	控制域	具体控制要求	华为云的应答
		20.详细说明为缓解信息安全事件所采取的行动，并提及负责实施这些缓解行动的人员。 21.说明缓解措施的结果。 22.在以后的类似情况下，采取行动尽量减少损失。 23.你认为应提请CNBV委员会注意的其他信息	

编号	控制域	具体控制要求	华为云的应答
附件67	业务连续性计划的最低要求	I. 在制定业务连续性计划之前，各机构应进行业务影响分析。 a) 确定对业务连续性不可或缺的关键流程。 b) 确定最低限度的资源（人力、后勤、物资、技术基础设施和任何其他性质的资源），以便在发生突发事件时，以及在这种突发事件结束时，维持和重建机构的服务和程序。 (c) 拟订与核查可能发生的业务紧急情况有关的相关设想，例如： i. 自然和环境灾害。 ii. 传染性疾病。 iii. 网络攻击或对计算机活动的攻击。 iv. 破坏行为。 v. 恐怖主义。 vi. 电力供应中断。 vii. 技术基础设施（电信、信息处理和网络）的故障或不可用。 viii. 人力、物力或技术资源的不到位。ix. 第三方提供的服务发生中断。 d) 根据为每个关键流程定义的情景，并通过风险委员会批准的方法评估突发事件的定量和定性影响。 e) 确定每个关键流程的恢复优先级。 f) 确定每个关键流程的恢复目标时间（称为RTO）。 g) 在适当的情况下，建立恢复目标点（RPO），作为每个关键流程的最大可容忍的数据损失。 h) 识别和评估与操作流程和与供应商签订的数据处理和传输服务有关的风险，以及	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。 为向金融机构提供持续、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ISO22301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，将业务中断对金融机构的影响程度作为判断关键业务的一个重要标准。为配合金融机构遵从监管要求，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。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，系统在遵循合规政策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。 此外，华为云作为云服务供应商，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云的**存储容灾服务（SDRS）**为弹性云服务器、云硬盘和**专属分布式存储（DSS）**等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到

编号	控制域	具体控制要求	华为云的应答
		与机构或其金融机构信息的保管和安全有关的风险。 i) 确定根据本节a）确定的关键流程的主数据中心的地理位置所带来的风险，以避免备用数据中心面临与主数据中心相同的风险。 II. 在制定业务连续性计划时，各机构应纳入以下战略： (a) 预防方面，应考虑以下事项： i. 评估机构的流程和服务以降低流程和服务本身的脆弱性对业务连续性的影响。 ii. 是否有必要的人力、财力、物力、技术和技术基础设施资源，以便在发生行动紧急事件时及时采取行动。 iii. 建立一个测试业务连续性计划的方案，至少每年更新一次，如果机构的技术基础设施、流程、产品和服务或内部组织发生了重大变化，则提前更新，并对业务连续性计划进行评估。 iv. 业务连续性培训计划。 v. 设计和实施业务连续性计划的沟通政策，应根据所述突发事件的性质及其不同的沟通对象，执行突发事件的通知。 vi. 登记、关注、跟踪和向有关人员传达对业务连续性计划进行测试所产生的结果的程序。 b) 突发事件，应包括以下内容： i.及时确定影响机构关键流程的突发事件的性质。 ii.控制突发事件对关键流程的影响。 c) 恢复，使机构的服务和程序恢复到最低服务水平并最终恢复正常。	容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

编号	控制域	具体控制要求	华为云的应答
		d) 评估，应包括收集和分析有关突发事件发展的相关信息，以及为预防、遏制和恢复突发事件而采取的行动和程序，以便在必要时对业务连续性计划做出调整。	

6 华为云如何遵从及协助客户满足《证券市场法》及相关通用规定的要求

墨西哥金融机构在遵循证券市场法及其相关通用规定的要求时，华为云作为云服务提供商，可能会参与到要求所涉及的部分活动中，以下内容将总结证券市场法及其相关通用规定中与云服务提供商相关的控制要求，并阐述华为云作为云服务提供商，会如何帮助金融机构客户满足相关控制要求。

6.1 华为云如何遵从及协助客户满足《证券市场法》的要求

编号	控制域	具体控制要求	华为云的应答
116	第一节：经纪人-交易商 第一部分：组织	经纪公司应在开展业务前30个工作日向CNBV委员会证明： 1. 经纪公司自身和签约的外包服务商提供服务所必须的基础设施和内部控制，若未成功证明CNBV委员会可能禁止其开展业务。	经纪公司应根据本法条在申请经营时提起30个工作日向CNBV委员会提供基础设施和内部控制的相关材料。 华为云将配合金融机构提供相关上报材料。
219	第二节: 经纪人的业务、活动和服务 第七部分：其他规定	经纪公司与第三方签订外包服务合同须先获得CNBV委员会的允许，并遵守相关的通用规定。	经纪公司应根据本法条在申请经营前获取CNBV委员会的批准。 华为云将配合金融机构提供相关上报材料并执行监管机构对于第三方外包服务提出的管理要求。

编号	控制域	具体控制要求	华为云的应答
220	第二节: 经纪人的业务、活动和服务 第七部分: 其他规定	经纪公司与第三方签订外包服务合同应遵守以下要求: 1. 向CNBV委员会提交说明云服务提供商提供的服务范围，风险以及供应商选择标准和程序的报告。 2. 制定检测云服务提供商业绩和合同履行情况的政策和程序。 a) 应考虑外包服务的质量和成本，明确绩效目标和衡量方式。 b) 分包的可能性和限制。 c) 信息的机密性和安全性。 d) 检测云服务提供商履行合同义务的程序。 e) 要求云服务提供商接受审计和监督，并在需要时提供与服务有关的记录、信息和技术支持。 f) 业务连续性计划和应急响应程序。 g) 若为国外的云服务提供商，则需云服务提供商书面签署遵守本法规的同意书。 h) 定期评估云服务提供商的绩效，以及遵守相关法规的情况，并提交董事会批准和核查。	金融机构应在与第三方签订的合同中约定对第三方所提供服务的安全控制的要求，并制定第三方绩效监控政策监控第三方对服务合同的履行情况。 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，可根据金融机构的需求进行定制化。
221	第二节: 经纪人的业务、活动和服务 第七部分: 其他规定	1. 经纪公司与第三方签订外包服务，不能免除经纪公司或其董事、雇员遵守本法律条例的规定和由此产生的通用规定的义务。 2. CNBV委员会可以通过经纪公司要求第三方提供其提供外包服务的信息，包括书籍、记录和文件。	金融机构与第三方签订外包服务，但不能外包法律责任，金融机构或其董事、雇员均应按本法要求承担相应的责任。金融机构应配合CNBV委员会，向金融机构的外包服务商收集相关信息。 华为云会安排专人积极响应金融机构的要求，并提供相关材料。

6.2 华为云如何遵从及协助客户满足《适用于证券交易所的通用规定》的要求

编号	控制域	具体控制要求	华为云的应答
33	第一节：技术基础设施的管理和控制	证券交易所应制定、记录和实施必要的政策和程序： 1. 技术基础设施的每个组成部分都能发挥其设计、开发或采购时所声明的功能。 2. 获取服务时已在生命周期的各个阶段考虑到信息安全问题，包括需求说明、设计、开发、测试、发布。 3. 证券交易所应根据不同的功能或传输的数据类型，将网络在逻辑上或物理上隔离成不同的域和子网络。 4. 证券交易所应对网络安全组件进行安全配置，考虑端口、最小特权原则、介质管理、访问控制、制造商更新和重新配置出厂设置等因素。 5. 证券交易所应在部署或变更前对组件进行测试，测试时禁止使用生产数据，或引入未授权的功能。 6. 具有使用许可证或授权书（如果适用）。 7. 建立访问控制、通信安全、信息安全管理等安全保护措施。包括： a) 建立用户识别和认证机制，确保仅允许授权的用户访问。访问控制中应包含特殊情况下的例外访问授权政策和程序。 b) 针对拥有较高权限的技术基础设施用户，如数据库和操作系统管理员，应建立特权账号管理制度。 c) 具有防止未经授权的用户进行访问的密码管理措施。	金融机构应制定技术基础设施的信息安全管理流程和机制，包括物理安全、软件生命周期安全管理、意识培训、数据全生命周期管理、访问控制、漏洞管理、业务连续性管理等领域，并确保外包服务提供商按照本通用规定的要求提供相应的外包服务。 华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编 码和测试、安全验收和发布、漏洞管理等环节，确保信息安全在信息系统开发生命周期中得到设计和实现。 华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分 区自我保护和容错恢复能力。华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS – Object - Based Storage）、运维管理区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能， 确定不同的攻击面以及不同的 安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。关于安全区域的详细介绍可参考**《华为云安全白皮书》**。 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

编号	控制域	具体控制要求	华为云的应答
		d) 证券交易所应对其信息进行分级分类，并对敏感信息加密。 e) 证券交易所应建立会话管理机制，自动关闭无人参与的会话，以及防止未经授权同时使用同一用户标识的会话。 f) 证券交易所应建立物理访问控制。 8. 技术基础设施具有备份机制和恢复程序。 9. 保留完整的审计日志，包括访问或尝试访问信息，以及技术基础设施用户进行的操作或活动记录。 10. 证券交易所应建立信息安全事件管理程序，并指定一个小组负责管理和执行。 11. 进行技术基础设施年度规划和审查，并制定更新计划。 12. 技术基础设施应执行自动控制措施或在没有自动控制措施的情况下进行补偿性控制，以减少手动或半自动控制程序的风险。 13. 建立控制措施以防止资产、账簿和记录被篡改或伪造。 14. 建立用来衡量内外部服务可用性水平和服务响应时间的程序。 15. 至少每年一次或在技术基础设施的任何部分发生变更时进行漏洞和威胁检测，以及对其技术基础设施的不同部分进行渗透测试。	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。 金融机构可通过华为云的**统一身份认证服务（IAM）**对使用云资源的用户账号进行管理。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。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（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。 金融机构可通过华为云的**漏洞扫描服务（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。 金融机构可通过华为云的**数据存储加密服务（DEW）**实现对数据的加密。目前，华为云的**云硬盘服务（EVS）**、**对象存储服务（OBS）**和 **镜像服务（IMS）**等多个服务均提供数据加密（服务端加密）功能供金融机构选择。此外，金融机构通过数据加密服务可对密钥进行全生命周期集中管理。华为云使用的硬件安全模块（HSM）为金融机构创建和管理密钥，HSM拥有FIPS140-2（2级和3级）的主流国际安全认证，满足用户的数据合规

编号	控制域	具体控制要求	华为云的应答
			性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取金融机构根密钥。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，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份的机制，保障了密钥的持久性。更多信息请参见**《华为云安全白皮书》**。 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（VPN）**、**云专线（DC）**、**云连接（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。华为云的**企业主机安全（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。 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。 华为云还为金融机构提供培训服务，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”。 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。

编号	控制域	具体控制要求	华为云的应答
37	第二节：业务连续性计划	证券交易所总经理应制定业务连续性计划，该计划及其修改应通过审计委员会提交给董事会批准。其中总经理应负责： 1. 制定培训计划，执行、持续更新和传播该计划。 2. 设计和实施业务连续性计划的沟通政策，并根据有关紧急情况的性质与金融机构、公众、CNBV委员会和其他主管当局及时沟通。 3. 当出现应急事件时，向CNBV委员会通报最新情况，并在应急事件结束后15个日历日内向CNBV委员会提交一份分析报告，说明导致业务出现应急事件的原因和造成的影响。 4.至少每年对业务连续性计划进行一次有效性测试，并保证每年对业务连续性计划的审核或更新。	金融机构应识别其关键业务流程，并制定业务连续性计划。金融机构应至少每年对业务连续性计划的有效性进行测试，将测试结果通报董事会和CNBV委员会，并根据测试结果和CNBV委员会的建议持续更新该计划。金融机构需制定评估突发事件影响性的方法，当出现突发事件时，金融机构需通报CNBV委员会，并说明该突发事件产生的原因以及造成的影响。 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。 如果金融机构在制定和执行其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。
38	第二节：业务连续性计划	证券交易所应制定评估突发事件的定量和定性影响的方法，并事先得到董事会的批准。审计委员会应每年核查该方法的有效性，根据报告结果进行修正。并向董事会和CNBV委员会报告该测试和评估的结果。	

编号	控制域	具体控制要求	华为云的应答
附件6	业务连续性计划的最低要求	I. 在制定业务连续性计划之前，各机构应进行业务影响分析。 a) 确定对业务连续性不可或缺的关键流程。 b) 确定最低限度的资源（人力、后勤、物资、技术基础设施和任何其他性质的资源），以便在发生业务紧急情况时以及在这种紧急情况结束时维持和重建证券交易所的服务和程序。 c) 拟定与可能发生的突发事件有关的方案，除其他外，考虑以下内容： i. 自然和环境灾害。 ii. 传染性疾病。 iii. 网络攻击或对计算机活动的攻击。 iv. 破坏行为。 v. 恐怖主义。 vi. 电力供应中断。 vii. 技术基础设施（电信、信息处理和网络）的故障或不可用。 viii. 人力、物力或技术资源的不到位。 ix. 第三方提供的服务发生中断。 d) 根据为每个关键流程定义的情景，评估突发事件的定量和定性影响。 e) 定义每个关键流程的恢复优先级。 f) 确定每个服务和流程的恢复时间目标（RTO）。 g) 考虑恢复目标点（RPO），理解为每项服务和流程可容忍的最大数据损失，考虑到在任何情况下都不能丢失那些已经输入的交易信息，并及时了解在突发事件发生时每个交易的状态。	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。 为向金融机构提供持续、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，将业务中断对金融机构的影响程度作为判断关键业务的一个重要标准。为配合金融机构遵从监管要求，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。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，系统在遵循合规政策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。 此外，华为云作为云服务供应商，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云的**存储容灾服务（SDRS）**为弹性云服务器、云硬盘和**专属分布式存储（DSS）**等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到

编号	控制域	具体控制要求	华为云的应答
		h) 识别和评估与操作流程和与服务供应商签订的数据处理和传输服务有关的风险，以及与证券交易所或经纪公司信息的保管和安全有关的风险。 i) 确定根据本节a ）确定的关键流程的主数据中心的地理位置所带来的风险，以避免备用数据中心面临与主数据中心相同的风险。 j) 考虑建立备用的数据处理和操作站点，这些站点应该能够在需要的基础上运行，并且不应该受到与主站点相同的风险。 II. 在制定业务连续性计划时，各机构应纳入以下战略： (a) 预防方面，应考虑以下事项： i. 评估机构的流程和服务以降低流程和服务本身的脆弱性对业务连续性的影响。 ii. 是否有必要的人力、财力、物力、技术和技术基础设施资源，以便在发生行动紧急事件时及时采取行动。 iii. 建立一个测试业务连续性计划的方案，至少每年更新一次，如果机构的技术基础设施、流程、产品和服务或内部组织发生了重大变化，则提前更新，并对业务连续性计划进行评估。 iv. 业务连续性培训计划。 v. 设计和实施业务连续性计划的沟通政策，应根据所述突发事件的性质及其不同的沟通对象，执行突发事件的通知。 vi. 登记、关注、跟踪和向有关人员传达对业务连续性计划进行测试所产生的结果的程序。	容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

编号	控制域	具体控制要求	华为云的应答
		b) 突发事件，应包括以下内容： i.及时确定影响机构关键流程的突发事件的性质。 ii.控制突发事件对关键流程的影响。 c) 恢复，使机构的服务和程序恢复到最低服务水平并最终恢复正常。 d) 评估，应包括收集和分析有关突发事件发展的相关信息，以及为预防、遏制和恢复突发事件而采取的行动和程序，以便在必要时对业务连续性计划做出调整。	

6.3 华为云如何遵从及协助客户满足《适用于经纪公司的通用规定》的要求

编号	控制域	具体控制要求	华为云的应答
117.2.7	第一节：内部控制 第六部分：整体管理	经纪公司应制定、记录和实施必要的政策和程序： 1. 技术基础设施的每个组成部分都能发挥其设计、开发或采购时所声明的功能。 2. 确保技术基础设施的完整性和充分维护。 3. 获取服务时已在生命周期的各个阶段考虑到信息安全问题，包括需求说明、设计、开发、测试、发布。 4. 金融机构应根据不同的功能或传输的数据类型，将网络在逻辑上或物理上隔离成不同的域和子网络。 5. 金融机构应对网络安全组件进行安全配置，考虑端口、最小特权原则、介质管理、访问控制、制造商更新和重新配置出厂设置等因素。 6. 金融机构应在部署或变更前对组件进行测试，测试时禁止使用生产数据，或引入未授权的功能。 7. 具有使用许可证或授权书（如果适用）。 8.建立访问控制、通信安全、信息安全管理等安全保护措施。包括： a) 建立用户识别和认证机制，确保仅允许	金融机构应制定技术基础设施的信息安全管理流程和机制，包括物理安全、软件生命周期安全管理、意识培训、数据全生命周期管理、访问控制、漏洞管理、业务连续性管理等领域，并确保外包服务提供商按照本通用规定的要求提供相应的外包服务。 华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节，确保信息安全在信息系统开发生命周期中得到设计和实现。 华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分区自我保护和容错恢复能力。华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS – Object - Based Storage）、运维管理区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。关于安全区域的详细介绍可参考**《华为云安全白皮书》**。 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、业务连续性等。 金融机构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

编号	控制域	具体控制要求	华为云的应答
		授权的用户访问。访问控制中应包含特殊情况下的例外访问授权政策和程序。 b) 针对拥有较高权限的技术基础设施用户，如数据库和操作系统管理员，应建立特权账号管理制度。 c) 具有防止未经授权的用户进行访问的密码管理措施。 d) 金融机构应对其信息进行分级分类，并对敏感信息加密。 e) 金融机构应建立会话管理机制，自动关闭无人参与的会话，以及防止未经授权同时使用同一用户标识的会话， f) 金融机构应建立物理访问控制。 9. 技术基础设施具有备份机制和恢复程序。 10. 保留完整的审计日志，包括访问或尝试访问信息，以及技术基础设施用户进行的操作或活动记录。 11. 金融机构应建立信息安全事件管理程序，并指定一个小组负责管理和执行。 12.进行技术基础设施年度规划和审查，并制定更新计划。 13. 技术基础设施应执行自动控制措施或在没有自动控制措施的情况下进行补偿性控制，以减少手动或半自动控制程序的风险。 14. 建立资产、账簿、记录和数字文件	管理。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。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（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。 金融机构可通过华为云的漏洞扫描服务（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。 金融机构可通过华为云的数据存储加密服务（DEW）实现对数据的加密。目前，华为云的云硬盘服务（EVS）、对象存储服务（OBS）和镜像服务（IMS）等多个服务均提供数据加密（服务端加密）功能供金融机构选择。此外，金融机构通过数据加密服务可对密钥进行全生命周期集中管理。华为云使用的硬件安全模块（HSM）为金融机构创建和管理密钥，HSM拥有FIPS140-2（2级和3级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取金融机构根密钥。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，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份的机制，保障了密钥的持久性。更多信息请参见**《华为云安全白皮书》**。 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（VPN）、云专线（DC）、云连接（CC）等服务，实现不同区域之间业务

编号	控制域	具体控制要求	华为云的应答
		被篡改或伪造的控制措施。 15. 建立用来衡量内外部服务可用性水平和服务响应时间的程序。 16. 至少每年一次或在技术基础设施的任何部分发生变更时进行漏洞和威胁检测，以及对其技术基础设施的不同部分进行渗透测试。	的互联互通和数据传输安全。华为云的企业主机安全（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。 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。 华为云还为金融机构提供培训服务，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”。 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。

编号	控制域	具体控制要求	华为云的应答
206	第二节：将服务外包给第三方	经纪公司与第三方签订服务合同应遵守以下要求。 1. 提供报告说明选择第三方服务提供商的标准和政策。 2. 在服务合同或在第三方无条件接受的文件中规定： a) 接受经纪公司的外部审计员和CNBV委员会访问物理场所，经纪公司可以指定一名代表陪同访问。 b) 由经纪公司或通过CNBV委员会自己指定的第三方对合同所涉及的服务进行审计 。 c) 应经纪公司的要求，向经济公司的外部审计员和CNBV委员会或CNBV委员会指定的第三方提供服务有关的账簿、系统、记录、手册，还应允许负责的人员可以访问与提供的服务有关的办公室和设施。 3. 有政策和程序来监督第三方的表现和履行其合同义务的情况。这种政策和程序应包括与以下有关事项： a) 经纪公司对服务所产生的数据的所有权。 b) 确保服务提供者定期接受与签约服务有关的充分培训。 c) 如果签约的服务涉及技术或电信基础设施的使用，则应遵守本规定附件12中规定的最低安全准则。	金融机构应按照相关要求制定与第三方的合同。 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。华为云也制定了线下合同模板，可根据金融机构的需求进行定制化。 华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。

编号	控制域	具体控制要求	华为云的应答
		4. 每两年进行一次审计，以核实遵守本章以及最低安全准则的程度（如适用）。并向董事会和审计委员会汇报审计结果。 5. 规定总经理、审计委员会以及经纪公司的内部审计员根据其权限监督外包服务商提供服务所使用的技术、信息处理基础设施的和信息的处理、控制和安全机制。	

编号	控制域	具体控制要求	华为云的应答
206.2	第二节：将服务外包给第三方	1. 经济公司应制定标准，与外包服务商签订合同应考虑： a) 机构在发生突发事件时，有能力保持业务的连续性。 b) 寻找第三方来取代最初签约的一方的复杂性和所需的时间。 c) 在做出对机构本身的行政、财务、业务或法律状况有重大影响的决定时受到限制。 d) 机构是否有能力保持适当的内部控制，以及在第三方暂停服务的情况下遵守监管要求。 e) 暂停服务将对机构的财务、声誉和运作产生的影响。 f) 金融机构信息的脆弱性。 2. 金融机构的总经理应负责审批第三方服务提供商的选择政策和标准。 3. 经纪公司应在与外包服务商签订合同的20工作日前，向监管CNBV委员会提交包括为有关服务对象的操作、技术或数据库管理过程的通知，并获取同意。	金融机构总经理是金融机构外包管理的主要责任人，金融机构应根据本通用规定制定外包管理机制，并确定与外包服务商签订合同的标准，并在与外包服务商签订合同前的20个工作日将相关资料提交给CNBV委员会获取同意。 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，可根据金融机构的需求进行定制化

编号	控制域	具体控制要求	华为云的应答
206.2.1	第二节：将服务外包给第三方	第206.2 所指的通知应由金融机构总负责人签署，如果服务涉及技术或电信基础设施的使用，通知应另外包含一份技术报告，具体说明利用第三方提供的技术基础设施开展的银行业务或服务的类型，以及遵守本规定服务采购的最低安全准则。	金融机构在计划与第三方签订服务合同前需向CNBV委员会提交相关材料并获取批准。 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。如客户申请，华为云将按需为客户提供相关的文件副本。 华为云将配合金融机构提供相关上报材料，配合金融机构执行监管通知。

编号	控制域	具体控制要求	华为云的应答
206.2.2	第二节：将服务外包给第三方	经纪公司应要求CNBV委员会授权与第三方签订外包服务合同，如果服务部分或全部在国家领土之外或由国外居民提供或执行，经纪公司应在签订合同前至少20个工作日向负责监督的CNBV委员会副主席申请有关授权，并提交下列文件。 1. 与之签订合同的第三方或委托代理人所居住的国家信息，其国内法对个人数据提供的保护措施，或者居住国与墨西哥签署了关于此类事项的国际协议。 2. 机构必须向CNBV委员会声明，他们将在位于墨西哥合众国的主要办事处至少保留与评估、审计结果和业绩报告有关的文件和资料。同样，当CNBV委员会要求时，他们应提供此类文件的西班牙语版本。 3. 经纪公司得到了董事会的批准，或得到了审计委员会或风险委员会的批准，并在各自的协议中说明签订服务或委托合同不会危及充分遵守适用于本机构的规定。	金融机构应按照相关要求制定与第三方的合同。当金融机构与墨西哥境外机构或与墨西哥境外居民签订外包服务合同时，应在签订合同前20个工作日向CNBV委员会申请并获得授权。金融机构在向CNBV委员会申请时，应按本通用规定的要求提供相关文件。 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，可根据金融机构的需求进行定制化。华为云将配合客户提供相关上报材料，配合客户执行监管通知的工作。

编号	控制域	具体控制要求	华为云的应答
206.2.4	第二节：将服务外包给第三方	当CNBV委员会认为机构的财务稳定性、业务连续性或对公众利益的保护可能受到影响，或机构未能遵守本规定和其他适用规定时，CNBV委员会可在机构获得听证权利后，下令部分或全部、暂时或最终暂停通过有关第三方提供的服务或委托。除非在行使听证权时，金融机构提交一份规范化方案交由CNBV委员会审核，CNBV委员会在30个日历日内做出适当决定。	当CNBV委员会认为金融机构不满足本通用规定要求的场景时，金融机构应配合提交一份规范化方案交由CNBV委员会审核，必要时可能暂停与相关第三方的合同。 华为云将配合金融机构提供相关上报材料，配合金融机构履行监管要求。

编号	控制域	具体控制要求	华为云的应答
206.2.5	第二节：将服务外包给第三方	经纪公司应拥有一份服务提供者的名单，其中至少应包括以下信息。 金融机构应拥有一份服务提供者的名单，其中至少应包括以下信息。 1. 服务提供者的名称、公司名称。 2、服务提供者的法律代表的姓名。 3. 说明与第三方签订的服务，包括第三方存储或处理的数据或信息（如有）。 4. 如果适用，与第三方提供的服务有关的系统信息，至少包括系统名称、版本和功能或目的。 5.与其他系统的接口及其目的，包括交换信息的细节。 6.开展该服务的完整地址，以及负责开展该服务的人员所在的位置。 7. 如果适用，合同系统的处理设备所在的主要数据中心的完整地址。 8. 在适用的情况下，处理设备所在的备用数据中心的完整地址。 9. 经纪人-交易商提交给CNBV委员会的通知的日期。 10. 获取批准签约服务的通知的编号和日期。	金融机构应制定并维护其供应商清单，该清单中应列明服务提供商的基本信息，包括服务提供者的名称、所提供的服务详情等信息。 华为云将配合金融机构提供相关上报材料，配合金融机构履行监管要求。

编号	控制域	具体控制要求	华为云的应答
206.2.6	第二节：将服务外包给第三方	经纪公司在制定与服务或委托合同有关的政策时，应考虑以下内容： 1. 第三方执行措施或计划的能力，包括性能、可靠性、能力、业务连续性。 2. 处理与提供服务或委托有关的产生的信息时的完整性、准确性、安全性、保密性、安全性、及时性和可靠性，以及访问控制措施。 3. 经纪公司可用来评估合同遵守情况的方法。 4. 定期评估服务质量的标准和程序。 5. 第三方提供合同规定服务的连续性的能力，或经纪公司在任何情况下都有其他选择，以减少经纪公司运作的脆弱性。 6. 经济公司的风险容忍度。 7. 经纪公司在综合风险管理中识别、衡量、监测、限制、控制、通报和披露本章所述服务可能产生的风险。 8. 内部控制系统遵守本规定的能力。 9. 董事会应指定一名负责人，可以是内部审计员或审计委员会，负责监督、评估并定期向董事会报告服务提供者的业绩，以及遵守与相应服务或交易有关的适用规则的情况。 10. 董事会应至少每年审查一次选择第三方的制度，并根据第	客户应按照相关要求制定与第三方的合同。 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，可根据金融机构的需求进行定制化。 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ISO22301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。 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。

编号	控制域	具体控制要求	华为云的应答
		三方业绩评估结果进行修改。	
附件12	金融机构采购时应考虑以下安全准则	1. 安全方面 a) 确保采用以点对点加密方式传输敏感用户信息的措施。 b) 金融机构应设立一个独立于业务、审计和系统领域的安全官，安全官应负责管理访问控制，安全官拥有查阅被授权访问记录的权限，被授权人员的访问记录应保留。 2. 审计和监督 a) 金融机构应该至少每两年对第三方数据中心的基础设施的安全控制和运行情况进行一次审计。	金融机构应采用加密的方式传输用户的敏感信息，并设立一个独立的安全官，赋予该安全官查阅审计访问用户信息记录的权限，金融机构应至少每两年对第三方数据中心进行安全审计，检查第三方数据中心的安全措施的执行情况。 对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过如下方式提供： **虚拟专用网络（VPN）**：VPN用于在远端网络和VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云上，为租户提供端到端的数据传输机密性保障。通过VPN 在传统数据中心与 VPC 之间建立通信隧道，租户可方便地使用华为云的云服务器、块存储等资源，通过将应用程序转移到云中、启动额外的 Web 服务器来增加网络的计算容量，实现了企业的混合云架构的同时，也降低了企业核心数据非法扩散的风险。 目前，华为云采用硬件实现的 IKE（密钥交换协议）和 IPSec VPN 结合的方法对数据传输通道进行加密，确保传输安全。 **应用层TLS与证书管理：**华为云服务提供 REST 和 Highway方式进行数据传输，REST网络通道是将服务以标准RESTful的形式向外发布，调用端直接使用HTTP客户端，通过标准 RESTful形式对 API 进行调用，实现数据传输； Highway 通道是高性能私有协议通道，在有特殊性能需求场景时可选用。上述两种数据传输方式均支持使用传输层安全协议（TLS – Transport Layer Security）1.2版本进行加密传输，同时也支持基于 X.509 证书的目标网站身份认证。 **SSL证书管理服务（SCM）**则是华为云联合全球知名数字证书服务机构，为租户提供的一站式 X.509 证书的全生命周期管理服务，实现目标网站的可信身份认证与安全数据传输。 华为云会安排专人积极配合金融机构发起的审计要求。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。

编号	控制域	具体控制要求	华为云的应答
附件18	业务连续性计划的最低要求	I. 在制定业务连续性计划之前，各机构应进行业务影响分析。 a) 确定对业务连续性不可或缺的关键流程。 b) 确定最低限度的资源（人力、后勤、物资、技术基础设施和任何其他性质的资源），以便在发生突发事件时以及在这种突发事件结束时维持和重建经纪公司的服务和程序。 c) 拟定与可能发生的突发事件有关的相关方案，至少要考虑以下几点： i. 自然和环境灾害。 ii. 传染性疾病。 iii. 网络攻击或对计算机活动的攻击。 iv. 破坏行为。 v. 恐怖主义。 vi. 电力供应中断。 vii. 技术基础设施（电信、信息处理和网络）的故障或不可用。 viii. 人力、物力或技术资源的不到位。 ix. 第三方提供的服务发生中断。 d) 根据为每个关键流程定义的情景，评估突发事件的定量和定性影响。 (e) 为每个关键流程的恢复优先级。 f) 确定每个服务和流程的恢复时间目标（RTO）。 g) 考虑恢复目标点（RPO），理解为每	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。 为向金融机构提供持续、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，将业务中断对金融机构的影响程度作为判断关键业务的一个重要标准。为配合金融机构遵从监管要求，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。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，系统在遵循合规政策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。 此外，华为云作为云服务供应商，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云的存储容灾服务（SDRS）为弹性云服务器、云硬盘和专属分布式存储（DSS）等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

编号	控制域	具体控制要求	华为云的应答
		个服务和流程可容忍的最大数据损失。 h) 确定和评估与供应商签订的操作流程和数据处理及传输服务有关的风险，以及与经纪商或其金融机构信息的保管和安全有关的风险。 i) 确定根据本节a ）确定的关键流程的主数据中心的地理位置所带来的风险，以避免备用数据中心面临与主数据中心相同的风险。 j) 考虑建立备用的数据处理和操作站点，这些站点应该能够在需要的基础上运行，并且不应该受到与主站点相同的风险。 II. 在制定业务连续性计划时，各机构应纳入以下战略： (a) 预防方面，应考虑以下事项： i. 评估机构的流程和服务以降低流程和服务本身的脆弱性对业务连续性的影响。 ii. 是否有必要的人力、财力、物力、技术和技术基础设施资源，以便在发生行动紧急事件时及时采取行动。 iii. 建立一个测试业务连续性计划的方案，该方案必须至少每年更新一次，如果经纪商的技术基础设施、流程、产品和服务或内部组织发生重大变化，则应提前更新，并对业务连续性计划进行评估。	

编号	控制域	具体控制要求	华为云的应答
		iv. 业务连续性培训计划。 v. 设计和实施业务连续性计划的沟通政策，应根据所述突发事件的性质及其不同的沟通对象，执行突发事件的通知。 vi. 登记、关注、跟踪和向有关人员传达对业务连续性计划进行测试所产生的结果的程序。 b) 突发事件，应包括以下内容： i.及时确定影响机构关键流程的突发事件的性质。 ii.控制突发事件对关键流程的影响。 c) 恢复，使机构的服务和程序恢复到最低服务水平并最终恢复正常。 d) 评估，应包括收集和分析有关突发事件发展的相关信息，以及为预防、遏制和恢复突发事件而采取的行动和程序，以便在必要时对业务连续性计划做出调整。	

6.4 华为云如何遵从及协助客户满足《适用于证券存管机构的通用规定》的要求

编号	控制域	具体控制要求	华为云的应答
23	第一节：关于技术基础设施的管理和控制	金融机构应建立制定、记录和实施必要的政策和程序： 1. 技术基础设施的每个组成部分都能发挥其设计、开发或采购时所声明的功能。 2. 获取服务时已在生命周期的各个阶段考虑到信息安全问题，包括需求说明、设计、开发、测试、发布。 3. 金融机构应根据不同的功能或传输的数据类型，将网络在逻辑上或物理上隔离成不同的域和子网络。 4. 金融机构应对网络安全组件进行安全配置，考虑端口、最小特权原则、介质管理、访问控制、制造商更新和重新配置出厂设置等因素。 5. 金融机构应在部署或变更前对组件进行测试，测试时禁止使用生产数据，或引入未授权的功能。 6. 具有使用许可证或授权书（如果适用）。 7. 建立访问控制、通信安全、信息安全管理等安全保护措施。包括： a) 建立用户识别和认证机制，确保仅允许授权的用户访问。访问控制中应包含特殊情况下的例外访问授权政策和程序。 b) 针对拥有较高权限的技术基础设施用户，如	金融机构应制定技术基础设施的信息安全管理流程和机制，包括物理安全、软件生命周期安全管理、意识培训、数据全生命周期管理、访问控制、漏洞管理、业务连续性管理等领域，并确保外包服务提供商按照本通用规定的要求提供相应的外包服务。 华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编 码和测试、安全验收和发布、漏洞管理等环节，确保信息安全在信息系统开发生命周期中得到设计和实现。 华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分 区自我保护和容错恢复能力。华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS – Object - Based Storage）、运维管理区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能， 确定不同的攻击面以及不同的 安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。关于安全区域的详细介绍可参考**《华为云安全白皮书》**。 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。

编号	控制域	具体控制要求	华为云的应答
		数据库和操作系统管理员，应建立特权账号管理制度。 c) 具有防止未经授权的用户进行访问的密码管理措施。 d) 金融机构应对其信息进行分级分类，并对敏感信息加密。 e) 金融机构应建立会话管理机制，自动关闭无人参与的会话，以及防止未经授权同时使用同一用户标识的会话。 f) 金融机构应建立物理访问控制。 8. 技术基础设施具有备份机制和恢复程序。 9. 保留完整的审计日志，包括访问或尝试访问信息，以及技术基础设施用户进行的操作或活动记录。 10. 金融机构应建立信息安全事件管理程序，并指定一个小组负责管理和执行。 11. 进行技术基础设施年度规划和审查，并制定更新计划。 12. 技术基础设施应执行自动控制措施或在没有自动控制措施的情况下进行补偿性控制，以减少手动或半自动控制程序的风险。 13. 建立控制措施以防止资产、账簿和记录被篡改或伪造。 14. 建立用来衡量内外部服务可用性水平和服务响应时间的程序。 15. 至少每年一次或在技术基础设施的任何部分发生变更时进行漏洞和威胁检测，以及对其技	金融机构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。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。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（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。 金融机构可通过华为云的漏洞扫描服务（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。 金融机构可通过华为云的数据存储加密服务（DEW）实现对数据的加密。目前，华为云的云硬盘服务（EVS）、对象存储服务（OBS）和镜像服务（IMS）等多个服务均提供数据加密（服务端加密）功能供金融机构选择。此外，金融机构通过数据加密服务可对密钥进行全生命周期集中管理。华为云使用的硬件安全模块（HSM）为金融机构创建和管理密钥，HSM拥有FIPS140-2（2级和3级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取金融机构根密钥。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，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份的机制，保障了密钥的持久性。更多信息请参见**《华为云安全白皮书》**。 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

编号	控制域	具体控制要求	华为云的应答
		术基础设施的不同部分进行渗透测试。	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（VPN）、云专线（DC）、云连接（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。华为云的企业主机安全（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。 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。 华为云还为金融机构提供培训服务，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”。 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。

编号	控制域	具体控制要求	华为云的应答
27	第二节：业务连续性计划	证券交易所总经理应制定业务连续性计划，该计划及其修改应通过审计委员会提交给董事会批准。其中总经理应负责： 1. 制定培训计划，执行、持续更新和传播该计划。 2. 设计和实施业务连续性计划的沟通政策，包括与金融机构和公众、与对手、与机构本身的不同行政和业务单位以及与CNBV委员会和其他主管当局根据有关紧急情况的性质及时沟通。 3. 当出现应急事件时，向CNBV委员会通报最新情况，并在应急事件结束后15个日历日内向CNBV委员会提交一份分析报告，说明导致业务应急的原因和造成的影响。 4.至少每年对业务连续性进行一次有效性测试，并保证每年对业务连续性计划的审核或更新。	金融机构应识别其关键业务流程，并制定业务连续性计划。金融机构应至少每年对业务连续性计划的有效性进行测试，将测试结果通报董事会和CNBV委员会，并根据测试结果和CNBV委员会的建议持续更新该计划。金融机构需制定评估突发事件影响性的方法，当出现突发事件时，金融机构需通报CNBV委员会，并说明该突发事件产生的原因以及造成的影响。 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。 如果金融机构在制定和执行其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。
28	第二节：业务连续性计划	金融机构应制定评估突发事件的定量和定性影响的方法，应事先得到CNBV委员会和墨西哥银行的批准。审计委员会应每年核查该方法的有效性，根据报告结果进行修正。并向CNBV委员会和墨西哥银行报告该测试和评估的结果。	

编号	控制域	具体控制要求	华为云的应答
附件1	业务连续性计划的最低要求	I. 在制定业务连续性计划之前，各机构应进行业务影响分析。 a) 确定对业务连续性不可或缺的关键流程。 b) 确定最低限度的资源（人力、后勤、物资、技术基础设施和任何其他性质的资源），以便在发生突发事件时以及在其终止时维持和重建证券存放机构的服务和程序。 c) 阐述与可能发生的运营突发事件有关的相关情景，至少考虑以下内容： i. 自然和环境灾害。 ii. 传染性疾病。 iii. 网络攻击或对计算机活动的攻击。 iv. 破坏行为。 v. 恐怖主义。 vi. 电力供应中断。 vii. 技术基础设施（电信、信息处理和网络）的故障或不可用。 viii. 人力、物力或技术资源的不到位。 ix. 第三方提供的服务发生中断。 d) 根据为每个关键流程定义的情景，评估突发事件的定量和定性影响。 e) 定义每个关键流程的恢复优先级。 f) 确定每个服务和流程的恢复时间目标（RTO）。 g) 考虑将恢复目标点（称为RPO）理解为每项服务和流程可容忍的最大数据损失。	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。 为向金融机构提供持续、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ISO22301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，将业务中断对金融机构的影响程度作为判断关键业务的一个重要标准。为配合金融机构遵从监管要求，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。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，系统在遵循合规政策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。 此外，华为云作为云服务供应商，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云的存储容灾服务（SDRS）为弹性云服务器、云硬盘和专属分布式存储（DSS）等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

编号	控制域	具体控制要求	华为云的应答
		h) 识别和评估与操作流程以及与供应商签订的数据处理和传输服务有关的风险，以及与机构存放证券或其金融机构的信息的保管和安全有关的风险。 i) 确定根据本节a）确定的关键流程的主数据中心的地理位置所带来的风险，以避免备用数据中心面临与主数据中心相同的风险。 j) 考虑建立备用的数据处理和操作站点，这些站点应该能够在需要的基础上运行，并且不应该受到与主站点相同的风险。 II. 在制定业务连续性计划时，各机构应纳入以下战略： (a) 预防方面，应考虑以下事项： i. 评估机构的流程和服务以降低流程和服务本身的脆弱性对业务连续性的影响。 ii. 是否有必要的人力、财力、物力、技术和技术基础设施资源，以便在发生行动紧急事件时及时采取行动。 iii. 建立一个测试业务连续性计划的方案，至少每年更新一次，如果机构的技术基础设施、流程、产品和服务或内部组织发生了重大变化，则提前更新，并对业务连续性计划进行评估。 iv. 业务连续性培训计划。 v. 设计和实施业务连续性计划的沟通政策，应根据所述突发事件的性质及其不同的沟通对	

编号	控制域	具体控制要求	华为云的应答
		象，执行突发事件的通知。 vi. 登记、关注、跟踪和向有关人员传达对业务连续性计划进行测试所产生的结果的程序。 b) 突发事件，应包括以下内容： i.及时确定影响机构关键流程的突发事件的性质。 ii.控制突发事件对关键流程的影响。 c) 恢复，使机构的服务和程序恢复到最低服务水平并最终恢复正常。 d) 评估，应包括收集和分析有关突发事件发展的相关信息，以及为预防、遏制和恢复突发事件而采取的行动和程序，以便在必要时对业务连续性计划做出调整。	

7 华为云如何遵从及协助客户满足《金融科技机构监管法》及相关通用规定的要求

国家银行和证券委员会 (CNBV)发布了金融科技机构监管法及其通用规定，该指南主要针对融资机构、电子支付机构提供的服务做出规定，以下内容将总结金融科技机构监管法及其通用规定中与云服务提供商相关的控制要求，并阐述华为云作为云服务提供商，会如何帮助金融机构客户满足相关控制要求。

7.1 华为云如何遵从及协助客户满足《金融科技机构监管法》的要求

编号	控制域	具体控制要求	华为云的应答
39	第一节：授权	申请第三方外包服务时，金融机构需获得CNBV委员会的授权，且必须附上以下材料： 1. 关于运营风险的控制措施和政策，提供证据表明他们为金融机构提供了安全、可靠和的技术支持，具有确保信息保密性、可用性和完整性以及防止欺诈和网络攻击的最低安全标准。 2. 与其他ITF或技术服务供应商签订的协议或合同清单，这些协议或合同是执行关键业务流程、数据库管理等活动所必需的。	金融机构在申请第三方外包服务前，需按本法要求提供相应材料，并获得CNBV委员会的授权。 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。

编号	控制域	具体控制要求	华为云的应答
54	第二节：关于金融科技机构的运作	1. 金融机构与第三方签订外包服务，不能免除金融机构或其董事、雇员遵守本法律条例规定的义务。 2. CNBV委员会可以通过金融机构要求第三方提供其提供的外包服务的相关信息，包括书籍、记录和文件。	金融机构与第三方签订外包服务，但不能外包法律责任，金融机构或其董事、雇员均应按本法要求承担相应的责任。金融机构应配合CNBV委员会，向金融机构的外包服务商收集相关信息。 华为云会安排专人积极响应金融机构的要求，并提供相关材料。

7.2 华为云如何遵从及协助客户满足《金融科技机构监管法二级监管》的要求

编号	控制域	具体控制要求	华为云的应答
15	第二节：关于内部流程中的技术基础设施	1. 金融机构应根据不同的功能或传输的数据类型，将网络在逻辑上或物理上隔离成不同的域和子网络，包括将生产环境与开发和测试环境隔离。 2. 金融机构应对网络安全组件进行安全配置，考虑端口、最小特权原则、介质管理、访问控制、制造商更新和重新配置出厂设置等因素。 3. 金融机构应建立应用程序中的安全机制，确保免受如代码注入、会话操纵、信息泄漏和访问权限的改变等攻击，包括第三方提供的应用程序也应采取相同机制。	金融机构负责按照本监管要求规定的网络安全管控进行网络域划分、网络安全配置等。同时，金融机构还应按照同等级别的网络安全要求，对第三方进行要求和管理。华为云从最初的网络架构设计、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。金融机构可以使用华为云提供的（VPC）服务，实现不同区域之间网络隔离。VPC可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络ACL和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。

编号	控制域	具体控制要求	华为云的应答
16	第二节：关于内部流程中的技术基础设施	1. 金融机构应对其接收、生成、存储或传输的个人信息和敏感信息加密。 2. 针对已建立安全机制保护的交易信息可免于加密。 3. 加密密钥应由金融机构首席信息安全官掌控。	金融机构应按照其数据分类策略和原则对个人数据、隐私数据或机密数据等需加密的数据进行加密管理。 目前，华为云云硬盘（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）功能供金融机构选择，这些服务都采用高强度的算法对存储的数据进行加密。华为云为金融机构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。华为云使用的硬件安全模块（HSM）为金融机构创建和管理密钥，HSM拥有FIPS140-2（2级和3级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取金融机构根密钥。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。更多信息请参见**《华为云安全白皮书》**。 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（VPN）**、**云专线（DC）**、**云连接（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。

编号	控制域	具体控制要求	华为云的应答
19	第二节：关于内部流程中的技术基础设施	金融机构应建立报废管理政策，确保丢弃或移除的存储部件或物理设备存储中存储的信息是不可恢复的。	金融机构应建立报废管理政策，删除即将丢弃或移除的存储介质中存储的信息，并确保删除的信息不可恢复。 在金融机构确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除金融机构与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。
20	第二节：关于内部流程中的技术基础设施	金融机构应使用工具检测基础设施中的计算机病毒和恶意代码，并定期更新检测策略。	金融机构应制定漏洞管理机制，对关键业务定期执行漏洞扫描，分析扫描的结果，并对漏洞进行修复。 华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描。对于所有获知的安全漏洞信息，华为云将对每个漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后对修复情况进行验证，持续跟踪确认风险得到消除或缓解。华为云在其官网公布已经发现的产品或服务的漏洞并进行预警，客户可查看安全公告以了解漏洞影响的范围，处置方式及威胁级别。 金融机构可通过华为云的**漏洞扫描服务（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。
21	第二节：关于内部流程中的技术基础设施	金融机构应至少每两个月或在发生重大变更、安全事件后对基础设施进行额外的测试。 金融机构应制定修复计划，以解决测试中发现的漏洞。并根据漏洞的严重程度决定优先顺序。漏洞制定修复计划应由首席信息官负责，金融机构应在发现漏洞的10个工作日内制定修复计划并交由CNBV委员会。	

编号	控制域	具体控制要求	华为云的应答
23	第二节：关于内部流程中的技术基础设施	电子支付机构应建立程序和机制，限制对物理连接端口和外围设备以及计算机或电信基础设施的访问，电子支付机构应确保第三方同样具备该政策。	金融机构应物理安全机制，以管理对物理设备的访问，并在与第三方签订的合同协议中明确这些要求。 华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。 在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。

编号	控制域	具体控制要求	华为云的应答
24	第二节：关于内部流程中的技术基础设施	金融机构应建立企业信息安全管理政策，应包括： 1. 基础设施如数据库、操作系统和软件的逻辑访问控制。 2.基础设施的账号和密码管理政策。 3. 跟踪和监测存储金融机构信息的系统的访问，包括允许审查对金融机构信息的访问、操作行为、无效的访问尝试等。 4. 不执行以上措施的金融机构，需事先获得CNBV委员会和墨西哥银行的授权。	金融机构应按照本监管要求制定企业内部的安全管理政策，包括基础设施的访问控制、密码管理、日志管理等。 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。华为云制定了密码策略及账号口令安全相关管理规范，对秘密鉴别信息的分配进行管理。新建系统中的账号缺省密码在首次使用前由用户进行更改，当用户需要重置密码时对其身份进行验证。 金融机构可通过华为云的**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，金融机构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（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。

编号	控制域	具体控制要求	华为云的应答
26	第三节：技术基础设施的通用规定	金融机构应依照最佳实践和国际标准建立通信加密机制，确保使用加密的通信协议保证点对点通信中的信息安全。 金融机构应采用最新的、无漏洞、密钥足够长的加密机制并获得墨西哥银行和CNBV委员会的批准。	金融机构应依照最佳实践和国际标准建立数据安全传输机制。 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（VPN）、云专线（DC）、云连接（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。

编号	控制域	具体控制要求	华为云的应答
28	第三节：技术基础设施的通用规定	金融机构与第三方签订开发信息系统的服务外包合同，应： 1. 记录其流程、功能和配置，包括其开发或获取方法，以及其变化、更新的记录和技术基础设施每个组成部分的详细清单。应至少在需求分析、设计、IT系统开发（购买）、系统功能验证、发布前漏洞测试和代码分析、系统变更、安全销毁等阶段实施信息安全控制措施。 2. 如果软件是由第三方开发的，金融机构应要求安装时验证其完整性和真实性。 3. 金融机构不同组件之间应包含认证机制。 4. 金融机构使用电子签名来保证信息的完整性和不可抵赖性，无论它是静态信息还是传输中的信息。 5. 管理访问技术基础设施的用户及其权限。 6.不同的计算机系统及组件之间使用加密通信协议。 7. 通过自动化工具，在每次更新计算机系统时对其安全性进行静态审查。	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或软件的全生命周期安全。 华为的开发测试过程均遵循统一的系统安全开发管理规范。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。 华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，确保云服务满足安全要求。测试在与生产环境隔离的测试环境中进行，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。

编号	控制域	具体控制要求	华为云的应答
33	第三节：技术基础设施的通用规定	金融机构应至少每年对技术基础设施的信息安全控制措施进行一次评估或审计。金融机构应向监管机构提交以下文件： 1. 具体说明技术基础设施的信息技术风险水平的报告。 2. 补救计划，以解决高风险问题。 3. 实施补救措施的证据。 4. 风险解除的证据。 金融机构应对于其签约的第三方服务提供商的技术基础设施进行评估和审计，并获取以下文件： 1. 至少每年一次在第三方开始提供服务之前进行的评估或审计的结果。 2. 补救计划，以解决高风险问题。 3. 风险解除的证据。 金融机构应在墨西哥银行和CNBV委员会要求其提供文件时提供相应的文件。	金融机构应建立风险评估框架，定期评估其技术基础设施的安全，包括外包安排相关的风险。 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。
34	第三节：技术基础设施的通用规定	金融机构应聘请外部技术人员，至少每两年对技术基础设施的不同系统和应用进行一次渗透测试。 金融机构应在测试完成后的20个工作日内向墨西哥银行和CNBV委员会发送一份报告说明测试的结论。 如果含有高风险问题，金融机构应在完成渗透测试后不超过20个工作日内向墨西哥银行和CNBV提交一份记录在案的补救计划，以纠正这些观察结果。 金融机构应在漏洞修复后不超过两个月的时间内再次进行渗透测试，以验证各自的漏洞已得到缓解。 金融机构应在手册中记录对测试结果进行风险分类的方法。	金融机构应按照本监管要求规定至少每两年对技术基础设施的不同系统和应用执行渗透测试及修复计划。金融机构应按照本通用规定的要求将渗透测试的结果和修复计划向CNBV委员会上报。 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。 金融机构还可通过华为云的漏洞扫描服务(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。 华为云将配合金融机构提供相关上报材料，配合金融机构执行通知监管的工作。

编号	控制域	具体控制要求	华为云的应答
40	第三章：业务连续性	1. 制定、审查并在必要时更新业务连续性计划。 2. 至少每年一次评估业务连续性计划的遵守情况，并向管理机构报告评估结果，视情况对其进行更新。 3.核查业务连续性计划的运作和充分性测试的执行情况，并至少每年一次向监管机构报告此类测试的结果。 4. 制定并向监管机构提交突发事件的管理方法。 5. 制定并向监管机构提交用于评估突发事件的定量和定性影响的方法。 6. 如果金融机构与第三方签订外包服务合同，金融机构应拥有证明第三方符合业务连续性的国际标准的文件。	金融机构应识别其关键业务流程，并制定业务连续性计划。金融机构应至少每年对业务连续性计划的有效性进行测试，将测试结果通报管理机构，并根据测试结果和监管机构的建议持续更新该计划。金融机构需制定评估突发事件影响性的方法，当出现突发事件时，金融机构需通报监管机构，并说明该突发事件产生的原因以及造成的影响。 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。 如果金融机构在制定和执行其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。

编号	控制域	具体控制要求	华为云的应答
41	第四章：共同信息安全和业务连续性安排	金融机构应记录在技术基础设施中发现的事件、故障或漏洞，其中至少应包括与发现的故障、操作错误、试图进行的计算机攻击和实际进行的攻击有关的信息，以及技术基础设施用户的信息丢失、被提取、被篡改、丢失或被不当使用。所提供的信息应至少包括事件发生的日期和事件的简要描述、持续时间、受影响的服务、受影响的金融机构和涉及的金额，以及实施的纠正措施。且相关信息应以金融机构确定的方式进行备份，并应至少保存10年。	金融机构应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志，并按照既定的规则对日志进行备份，备份信息应至少留存10年。 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，以确保支撑网络安全事件回溯和合规。该日志分析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。华为云有专门的内审部门，定期对运维流程各项活动进行审 计。 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。 华为云提供了多粒度的数据备份归档服务，以满足客户不同场景下的需求。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。

编号	控制域	具体控制要求	华为云的应答
42	第四章：共同信息安全和业务连续性安排	当信息安全事件发生时，首席执行官应 1. 立即通过电子邮件ifpe@banxico.org.mx和CiberseguridadCNBV@cnbv.gob.mx或认可的方式通知CNBV委员会相应的信息安全事件初步评估情况。 2. 金融机构在确认信息安全事件后的5个工作日内，通过电子邮件向CNBV委员会报告信息安全事件详细情况。 3. 在信息安全事件结束的15日工作日内将信息安全事件分析报告和处理措施递交给CNBV委员会。 4. 如果信息安全涉及敏感信息的提取、丢失、消除、更改或金融机构怀疑这些情况已经发生，应在信息安全事件发生或获悉后24小时内通知客户。	当发生信息安全事件时，金融机构应按照本通用规定的要求向CNBV委员会上报。 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。 华为云将配合金融机构提供相关上报材料，配合金融机构满足监管通知的工作。

编号	控制域	具体控制要求	华为云的应答
49	第五章：与第三方和委托代理人签订服务合同	金融机构应针对提供涉及个人信息或敏感信息传输、存储、处理的服务在与第三方签订外包服务合同时获得CNBV委员会和墨西哥银行的授权。授权申请应包含以下资料： 1. 对拟签约的服务过程进行详细描述。 2. 提供服务的合同草案，其中应说明预计订立合同的日期，金融机构和第三方的权利和义务，包括确定用于提供服务的知识产权，以西班牙语提供。并明确规定第三方需遵守的义务： a) 提供数据、报告、记录、会议记录簿、文件、信函以及其他所需文件。 b) 监管机构可进入其办公室、场所和其他设施进行检查。 c) 第三方对其公司宗旨的任何修改或可能影响到作为合同对象的服务的提供的任何其他变化发生前至少30个日历日通知金融机构。 d) 对在提供服务过程中接收、传输、处理的信息进行保密。 e) 第三方如果会进行服务分包，应通知金融机构。 f) 在第三方停止提供服务时，安全地转移、归还和处理合同规定的信息。 g) 保持全面的审计日志，其中包括访问或试图访问的日志记录，以及技术基础设施用户进行的操作或活动的详细信息。 h) 具有符合金融机构要求的访问控制机制。 i) 允许金融机构进行安全审查，或提供审查的证据。 3. 提供技术基础设施的文件，说明服务提供商提供的通信链路信息，包括服务提供商的名	金融机构应识别由第三方提供的且涉及个人信息或敏感信息纯属、存储、处理的服务，并在与第三方签订外包时获取CNBV委员会的授权。 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。如客户申请，华为云将按需为客户提供相关的信息安全管理体系副本。 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，客户可根据自身的需求自行选择不同区域服务，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（OMS）和主机迁移服务（SMS），将内容数据从华为云中迁移出去。 鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时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。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。 除非是为客户提供必要的服务，或者为遵守法律法规或 政府机关的约束性命令，华为云不会触碰客户数据。 为了更好的保护墨西哥公民的个人数据，华为云分析了自身关于墨西哥隐私法律法规的遵循性，更多信息请详见**《华为云墨西哥隐私遵从性说明》**。

编号	控制域	具体控制要求	华为云的应答
		称、带宽和提供的服务类型等。提供每项服务的完整地址，以及储存和处理信息的一级和二级数据中心所在地址。如果是云计算服务，应提供本规定第50条规定的信息。 4. 允许金融机构在其自己的基础设施中或在境内的第三方基础设施中保管所有交易的详细记录，以确保任何时候都能保持业务连续性。 5. 当第三方有权限访问金融机构的身份图像或生物识别信息时，该第三方应提供证据证明其采取了控制措施以确保该信息的保密性、完整性和可用性。 6.金融机构检测第三方遵守合同情况的机制。 7. 根据第三方提供的服务的重要性，以及合同遵守情况进行评估，并将评估结果向监管机构（视情况而定）或金融机构审计委员会报告。 8. 能够核实第三方拥有并执行个人数据保护的证据，能够证明金融机构能够遵守有关的法律规定。如果服务完全或部分在国家领土之外处理、提供或执行，金融机构应随附文件，证明第三方采取了对应的措施保护个人数据，或者这些国家已经与墨西哥签署了有关此类事项的国际协议。 9. 金融机构不会因为地理距离和语言而影响金融机构提供的业务的连续性。 10. 金融机构制定技术支持计划，以便在不考虑时区和工作日差异的情况下，解决问题和事件。 11. 如果第三方原籍国的任何当局要求第三方提供与其向金融机构提供的服务有关的信息，第三方应尽快依法通知该机构，并向金融机构提供其向该当局提供的信息的副本。墨	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》，其中说明了所提供服务的内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据金融机构的需求进行定制化。华为云可能会随时自行修改或中止服务或修改或移除服务的功能。如果您订阅的服务发生重大变更或中止，我们会通过在我们的网站发布通知或其他方式通知您。

编号	控制域	具体控制要求	华为云的应答
		西哥银行和CNBV委员会将在25个工作日内对本条所述的授权请求做出决定。	
50	第五章：与第三方和委托代理人签订服务合同	金融机构与第三方签订云计算服务外包合同，当第三方为外国企业时，可能因为外国当局的命令中断服务，处于该情况的金融机构需在其业务连续性计划中包括以下所示的机制之一，以保证它们将保持必要的计算和处理能力，在云服务中断的两小时内恢复业务。 1. 除主要云计算服务提供商，允许金融机构依赖其他云计算服务提供商提供的云服务。 2. 应允许有关机构拥有自己的基础设施。	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。
51	第五章：与第三方和委托代理人签订服务合同	金融机构与第三方签订服务合同需遵守以下规定： 1.第三方服务提供商至少每年进行内部或外部审计，或有证据表明签约的第三方进行了审计。 2. 说明技术基础设施和信息安全相应文件，包括： a) 说明合同所涉及的系统、设备和应用的技术特点。 b) 详细说明确保个人信息或敏感信息安全传输和存储的机制，包括加密协议的版本和技术基础设施的安全组件。 c) 说明第三方将在其设备或设施中储存的或其可能接触的个人信息或敏感信息的类型。 d) 关于控制和监测个人信息或敏感信息的访问的机制，以及为此目的建立的日志、数据库和安全配置的说明。	金融机构应根据本监管要求的要求与外包服务商签订服务协议。 华为云每年定期接受专业第三方审计机构的审核，并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。如客户申请，华为云将按需为客户提供相关的信息安全管理体系副本。

编号	控制域	具体控制要求	华为云的应答
52	第五章：与第三方和委托代理人签订服务合同	金融机构应拥有一份服务提供者的名单，其中至少应包括以下信息： 金融机构应拥有一份服务提供者的名单，其中至少应包括以下信息。 1. 服务提供者的名称、公司名称。 2、服务提供者的法律代表的姓名。 3. 说明与第三方签订的服务，包括第三方存储或处理的数据或信息（如有）。 4. 如果适用，与第三方提供的服务有关的系统信息，至少包括系统名称、版本和功能或目的。 5.与其他系统的接口及其目的，包括交换信息的细节。 6.开展该服务的完整地址，以及负责开展该服务的人员所在的位置。 7. 如果适用，合同系统的处理设备所在的主要数据中心的完整地址。 8. 在适用的情况下，处理设备所在的备用数据中心的完整地址。 9. 获取批准签约服务的通知的编号和日期。	金融机构应制定并维护其供应商清单，该清单中应列明服务提供商的基本信息，包括服务提供者的名称、所提供的服务详情等信息。 华为云将配合金融机构提供相关上报材料，配合金融机构履行监管要求。

编号	控制域	具体控制要求	华为云的应答
附件2	制定业务连续性计划的最低要求	金融基金机构在制定业务连续性计划之前，应开展以下工作。 I. 一项风险分析，即： a) 根据本规定第39条提及的方法，考虑与以下因素有关的风险：人（包括欺诈、诚信、培训）、流程、技术和外部（包括外部供应商）。 b) 识别、评估、监测和减轻与操作流程和与供应商签订的数据处理和传输服务有关的风险。 c) 确定根据业务影响分析确定为关键的流程的主要数据处理和操作中心的地理位置所带来的风险，以避免备用数据处理和操作中心同时面临与主要数据处理和操作中心相同的风险。 d) 评估是否有必要建立备用的数据处理和操作场所或服务，在适当的情况下，这些场所或服务应能在需要时运作，并且不会同时受到与主要场所相同的风险。 II. 一项业务影响分析，即： a) 包含全部的服务和流程，确定那些关键的和被认为对业务连续性不可或缺的服务，包括与服务供应商签订的服务。 b) 确定最低限度的资源（人力、后勤、物资、技术基础设施和任何其他性质的资源），以便在发生业务紧急情况时以及在紧急情况结束时维持和重建金融机构的服务和程序。 c) 拟定与可能发生的紧急情况有关的相关方案，考虑以下内容： i. 自然和环境灾害。 ii. 传染性疾病。 iii. 网络攻击或对计算机活动的攻击。 iv. 破坏行为。	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。 为向金融机构提供持续、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，将业务中断对金融机构的影响程度作为判断关键业务的一个重要标准。为配合金融机构遵从监管要求，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。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，系统在遵循合规政策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。 此外，华为云作为云服务供应商，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云的**存储容灾服务（SDRS）**为弹性云服务器、云硬盘和**专属分布式存储（DSS）**等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾

编号	控制域	具体控制要求	华为云的应答
		v. 恐怖主义。 vi. 电力供应中断。 vii. 技术基础设施（电信、信息处理和网络）的故障或不可用。 viii. 人力、物力或技术资源的不到位。ix. 第三方提供的服务发生中断。 d) 根据为每个关键流程定义的情景，评估突发事件的定量和定性影响。 e) 定义每个关键流程的恢复优先级。 f) 确定每个服务和流程的恢复时间目标（RTO）。对于被认为是关键的过程，恢复时间不应超过两小时。 g) 在适当的情况下，建立恢复目标点（RPO），作为每个关键流程的最大可容忍的数据损失。 h) 识别和评估与操作流程和与供应商签订的数据处理和传输服务有关的风险，以及与机构或其金融机构信息的保管和安全有关的风险。 III. 业务连续性计划应根据本附件第二节提及的影响分析，说明在发生突发事件时应优先恢复的流程。 IV. 业务连续性计划应至少包括以下行动。 a) 预防，至少应包括确定与以下有关的活动和程序： i. 评估机构的流程和服务以降低流程和服务本身的脆弱性对业务连续性的影响。 ii. 是否有必要的人力、财力、物力、技术和技术基础设施资源，以便在发生行动紧急事件时及时采取行动。 iii. 建立一个测试业务连续性计划的方案，至少每年更新一次，如果机构的技术基础设施、流程、产品和服务或内部	站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

编号	控制域	具体控制要求	华为云的应答
		组织发生了重大变化，则提前更新，并对业务连续性计划进行评估。 iv. 业务连续性培训计划。 v. 登记、关注、跟踪和向有关人员传达对业务连续性计划进行测试所产生的结果的程序。 b) 突发事件，应包括以下内容： i.及时确定影响机构关键流程的突发事件的性质。 ii.控制突发事件对关键流程的影响。 iii.根据本规定第43条，向墨西哥银行和CNBV委员会通报操作上的意外情况。 c) 恢复，使机构的服务和程序恢复到最低服务水平并最终恢复正常。 d) 评估，应包括收集和分析有关突发事件发展的相关信息，以及为预防、遏制和恢复突发事件而采取的行动和程序，以便在必要时对业务连续性计划做出调整。	

编号	控制域	具体控制要求	华为云的应答
附件4	信息安全事件报告	I. 机构信息 a) 机构的名称。 b) 首席信息安全官的全名，以及他/她的电话号码和电子邮件地址。 II. 在加密的数字媒体中附上信息安全事件的以下信息 1.信息安全事件的描述。 2.受影响的账户。 3.受影响账户的状态（被封锁、被暂停、被激活）。 4.受影响的网络区域（互联网、内部网络、管理网络等等）。 5.受影响的系统类型（文件服务器、网络服务器、邮件服务、数据库、工作站、移动设备等等）。 6.操作系统（注明版本）。 7.受影响组件的协议或服务。 8.本机构受影响系统的组件数量。 9.涉及的应用程序（指定版本）。 10.受损设备的信息（品牌、软件版本、固件等）。 11.信息安全事件对服务造成的影响。 12.以比索计算的损失金额。 13.以比索为单位收回的金额。 14.信息安全事件的状态（已解决或未解决）。 15.指出该信息安全事件是否已报告给任何当局。如果是这样，请注明授权和日期。 16.攻击来源的公共IP地址、电子邮件地址或域名。 17.使用的通信协议。 18.涉及网站。 19.检测到的恶意软件。	金融机构应按照本通用规定要求的信息安全报告内容，在发生信息安全事件时及时上报CNBV委员会。 华为云将配合金融机构提供相关上报材料，配合金融机构满足监管通知的工作。

编号	控制域	具体控制要求	华为云的应答
		20.详细说明为缓解信息安全事件所采取的行动，并提及负责实施这些缓解行动的人员。 21.说明缓解措施的结果。 22.在以后的类似情况下，采取行动尽量减少损失。 23.你认为应提请CNBV委员会注意的其他信息	

7.3 华为云如何遵从及协助客户满足《适用于金融科技机构监管法的通用规定》的要求

编号	控制域	具体控制要求	华为云的应答
61	第五节：业务连续性计划	金融机构应制定业务连续性计划，并任命专员负责该计划。包括： 1. 制定培训计划，执行、持续更新和传播该计划。 2. 设计和实施业务连续性计划的沟通政策，包括与金融机构和公众、与对手、与机构本身的不同行政和业务单位以及与CNBV委员会和其他主管当局根据有关紧急情况的性质及时沟通。 3. 向CNBV委员会通报在公众应急事件，且事件出现持续时间超过30分钟，金融机构需在确认事件发生的60分钟内发送电子邮件给contingencias@cnbv.gob.mx和supervisionfintech@cnbv.gob.mx 或其他认可的方式通知CNBV委员会应急事件的现状。 4. 批准风险管理负责人根据这些规定提交的定量和定性分析方法。	金融机构应任命专员按照本通用规定的要求建立业务连续性计划，并制定保证其关键业务连续的RTO、RPO指标。 华为云提供了线上的《华为云服务等级协议》，其中规定了所提供服务的服务水平，以及华为云的职责。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。

编号	控制域	具体控制要求	华为云的应答
62	第五节：业务连续性计划	金融机构应明确负责业务连续性计划的风险管理的员工的职责，包括： 1. 界定并提交管理机构批准用于评估突发事件的定量和定性影响的方法 2. 每年核查方法的有效性，将其估计值与实际情况进行比较，并进行必要的修正。 3. 编制、审查并酌情更新或建议更新业务连续性计划，并至少每年一次或由监管机构决定更频繁地提交给监管机构批准 4. 至少每年一次或在集体融资机构的技术基础设施、流程、产品和服务或内部组织发生可能影响恢复战略的重大变化时测试业务连续性计划的功能和充分性 5. 制定程序，以登记、关注、跟踪并向其职能受到突发事件影响或与执行业务连续性计划有关的人员传播上一节提到的测试或在发生突发事件的情况下执行计划本身产生的结果、事件或意见。 6. 至少每年一次向监管机构报告本条第四节中提到的测试结果 7. 评估业务连续性计划的范围和有效性，并将评估结果报告给管理机构和负责关键业务程序的领域，必要时确定更新和加强计划所需的调整。 8. 如果金融机构与第三方签订外包服务合同，金融机构应拥有证明第三方拥有按照国际标准颁发的关于其保持服务连续性的能力的有效证明的文件。	金融机构应明确业务连续性的主要负责员工，并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。 为向金融机构提供持续、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，将业务中断对金融机构的影响程度作为判断关键业务的一个重要标准。为配合金融机构遵从监管要求，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。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，系统在遵循合规政策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。 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
63	第六节：信息安全	金融机构应建立信息安全领域的内控制度，并指定其总经理为负责人，确保第三方提供的服务符合： 1. 技术基础设施的每个组成部分都能发挥其设计、开发或采购时所声明的功能 2. 获取服务时已在生命周期的各个阶段考虑到信息安全问题，包括需求说明、设计、开发、测试、发布。 3. 金融机构应根据不同的功能或传输的数据类型，将网络在逻辑上或物理上隔离成不同的域和子网络，包括将生产环境与开发和测试环境隔离。 4. 金融机构应对网络安全组件进行安全配置，考虑端口、最小特权原则、介质管理、访问控制、制造商更新和重新配置出厂设置等因素。 5. 金融机构应在部署或变更前对组件进行测试，测试时禁止使用生产数据，或引入未授权的功能。 6. 金融机构的应用程序中应包含执行过程中免受攻击或入侵，如代码注入、会话操纵、信息泄漏、访问权限的改变等安全机制，包括第三方提供的应用程序。 7. 具有使用许可证或授权书（如果适用）。 8.建立访问控制、通信安全、信息安全管理等安全保护措施。包括： a) 建立用户识别和认证机制，确保仅允许授权的用户访问。访问控制中应包含特殊情况下的例外访问授权政策和程序。 b) 针对拥有较高权限的技术基础设施用户，如数据库	金融机构应制定技术基础设施的信息安全管理流程和机制，包括物理安全、软件生命周期安全管理、意识培训、数据全生命周期管理、访问控制、漏洞管理、业务连续性管理等领域，并确保外包服务提供商按照本通用规定的要求提供相应的外包服务。 华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编 码和测试、安全验收和发布、漏洞管理等环节，确保信息安全在信息系统开发生命周期中得到设计和实现。 华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分 区自我保护和容错恢复能力。华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS – Object - Based Storage）、运维管理区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能， 确定不同的攻击面以及不同的 安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。关于安全区域的详细介绍可参考**《华为云安全白皮书》**。 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。 金融机构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。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，

编号	控制域	具体控制要求	华为云的应答
		和操作系统管理员，应建立特权账号管理制度。 c) 具有防止未经授权的用户进行访问的密码管理措施，并强制要求每90天或更短时间内更改密码，提供给外包服务商的密码则应至少每年进行更改，或当外包服务商停止提供服务时应立刻更改密码。 d) 金融机构应对其信息进行分级分类，并对敏感信息加密。 e) 金融机构应建立会话管理机制，自动关闭无人参与的会话，以及防止未经授权同时使用同一用户标识的会话。 f) 金融机构应建立物理访问控制。 9. 技术基础设施具有备份机制和恢复程序。 10. 保留完整的审计日志，包括访问或尝试访问信息，以及技术基础设施用户进行的操作或活动记录，对储存关键信息的组件的审计记录保存三年。其他审计记录保留期至少为六个月。 11. 金融机构应建立信息安全事件管理程序，并指定一个小组负责管理和执行。 12. 进行技术基础设施年度规划和审查，并制定更新计划。 13. 技术基础设施应执行自动控制措施或在没有自动控制措施的情况下进行补偿性控制，以减少手动或半自动控制程序的风险。 14. 建立控制措施以防止资产、账簿和记录被篡改或伪造。 15. 建立用来衡量内外部服务可用性水平和服务响应时间的程序。	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。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（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。 金融机构可通过华为云的漏洞扫描服务（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。 金融机构可通过华为云的**数据存储加密服务（DEW）**实现对数据的加密。目前，华为云的**云硬盘服务（EVS）**、**对象存储服务（OBS）**和 **镜像服务（IMS）**等多个服务均提供数据加密（服务端加密）功能供金融机构选择。此外，金融机构通过数据加密服务可对密钥进行全生命周期集中管理。华为云使用的硬件安全模块（HSM）为金融机构创建和管理密钥，HSM拥有FIPS140-2（2级和3级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取金融机构根密钥。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，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份的机制，保障了密钥的持久性。更多信息请参见**《华为云安全白皮书》**。 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（VPN）、云专线

编号	控制域	具体控制要求	华为云的应答
		16. 金融机构应集中收集和监控日志或其他信息，从而自动检测和拦截可能导致安全事件或事故。 17. 建立技术基础设施配置信息防泄漏的控制措施。如IP地址、防火墙规则以及硬件和软件版本信息。	（DC）、云连接（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。华为云的**企业主机安全（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。 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。 华为云还为金融机构提供培训服务，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”。 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。
67	第六节：信息安全	当信息安全事件发生时，首席执行官应 1. 立即通过电子邮件CiberseguridadCNBV@cnbv.gob.mx或认可的方式通知CNBV委员会相应的信息安全事件初步评估情况。 2. 金融机构在确认信息安全事件后的5个工作日内，通过电子邮件向CNBV委员会报告信息安全事件详细情况。 3. 在信息安全事件结束的15日工作日内将信息安全事件分析报告和处理措施递交给CNBV委员会。 4. 如果信息安全涉及敏感信息的提取、丢失、消除、更改或金融机构怀疑这些情况已经发生，应在信息安全事件发生或获悉后48小时内通知客户。	当发生信息安全事件时，金融机构应按照本通用规定的要求向CNBV委员会上报。 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。 华为云将配合金融机构提供相关上报材料，配合金融机构执行监管通知的工作。

编号	控制域	具体控制要求	华为云的应答
68	第六节：信息安全	金融机构应记录在技术基础设施中发现的事件、故障或漏洞，其中至少应包括与发现的故障、操作错误、试图进行的计算机攻击和实际进行的攻击有关的信息，以及技术基础设施用户的信息丢失、被提取、被篡改、丢失或被不当使用。所提供的信息应至少包括事件发生的日期和事件的简要描述、持续时间、受影响的服务、受影响的金融机构和涉及的金额，以及实施的纠正措施。且相关信息应以金融机构确定的方式进行备份，并应至少保存10年。	金融机构应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志，并按照既定的规则对日志进行备份，备份信息应至少留存10年。 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，以确保支撑网络安全事件回溯和合规。该日志分析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。华为云有专门的内审部门，定期对运维流程各项活动进行审 计。 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。 华为云提供了多粒度的数据备份归档服务，以满足客户不同场景下的需求。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。

编号	控制域	具体控制要求	华为云的应答
86	第八章：将服务外包给第三方	金融机构应在与第三方签订合同的授权申请中附上以下内容： 1. 提供服务的合同草案，其中应说明预计订立合同的日期，金融机构和第三方的权利和义务，包括确定用于提供服务的知识产权，以西班牙语提供。 2. 在审计过程中： a) 提供数据、报告、记录、文件、信函以及其他所需文件。 b) 监管机构可进入其办公室、场所和其他设施进行检查。 c) 第三方如果会进行服务分包，应通知金融机构。 d) 保持全面的审计日志，其中包括关于访问或试图访问以及技术基础设施用户进行的操作或活动的详细信息。 e) 允许金融机构进行安全审查，或提供审查的证据。 3. 提供技术基础设施的文件,说明与服务提供商连接的通信链路信息，包括服务提供商的名称、带宽和提供的服务类型等。 a) 提供每项服务的完整地址，以及储存和处理信息的一级和二级数据中心所在地址。如果是云计算服务，应提供本规定第50条规定的信息 b) 第三方应用程序或系统的相互关系方案，包括金融机构自己的系统。 c) 承包服务的业务连续性机制。 4. 金融机构应针对云计算服务提供额外描述，包括： a) 云的类型，无论是公有云、私有云还是混合云。	金融机构应识别由第三方提供的且涉及个人信息或敏感信息纯属、存储、处理的服务，并在与第三方签订外包时获取CNBV委员会的授权。 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。如客户申请，华为云将按需为客户提供相关的信息安全管理体系副本。 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，客户可根据自身的需求自行选择不同区域服务，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（OMS）和主机迁移服务（SMS），将内容数据从华为云中迁移出去。 鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时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。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。 除非是为客户提供必要的服务，或者为遵守法律法规或 政府机关的约束性命令，华为云不会触碰客户数据。 为了更好的保护墨西哥公民的个人数据，华为云分析了自身关于墨西哥隐私法律法规的遵循性，更多信息请详见**《华为云墨西哥隐私遵从性说明》**。 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》，其中说明了所提供服务的内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据金融机构的需求进行定制化。华为云可能会随时自行修改或中止服务或修改或移除服

编号	控制域	具体控制要求	华为云的应答
		b) 信息将被储存和处理的具体区域。 c) 在公有云或与其他金融机构共享基础设施的虚拟化方案中，描述将用于保证敏感信息的保密性、完整性和可用性的控制机制。 5. 墨西哥银行和CNBV委员会将在25个工作日内对本条所述的授权请求做出决定。	务的功能。如果您订阅的服务发生重大变更或中止，我们会通过在我们的网站发布通知或其他方式通知您。

编号	控制域	具体控制要求	华为云的应答
87	第八章：将服务外包给第三方	金融机构根据CNBV委员会许可的条款与第三方签订外包服务协议需遵守以下条款： 1. 提供与数据库和计算机系统的操作流程和管理有关的服务的第三方同意第86条的规定，并保留各自的合同。 2. 金融机构至少每年对签约服务进行内部或外部审计，或有证据表明签约的第三方进行审计。 3. 金融机构至少在其总部保存与评价、审计结果和（如适用）相应的补救计划有关的文件和资料，以及提供服务的第三方的业绩报告。 4. 金融机构应建立变更管理，当第三方提供的系统、设备和应用或其技术特征进行了修改时应更新相关文件。 5. 关于技术基础设施和信息安全，还需提供以下文件： a) 第三方的系统、设备和应用的技术特点说明。 b) 详细说信息加密传输和存储的机制（如果适用）。 c) 包含集体融资机构和金融机构信息类型的详细资料，包括说明第三方将在其设备或设施中存储的敏感信息的类型。 d) 监测系统中敏感信息的访问机制，以及为此目的建立的日志管理和安全配置机制。	金融机构应按本监管要求要求制定合同和用户协议。 华为云也制定了线下合同模板，可根据金融机构的需求进行定制化。

编号	控制域	具体控制要求	华为云的应答
88	第八章：将服务外包给第三方	金融机构应拥有一份服务提供者的名单，其中至少应包括以下信息。 1. 服务提供者的名称、公司名称。 2、服务提供者的法律代表的姓名。 3. 说明与第三方签订的服务，包括第三方存储或处理的数据或信息（如有）。 4. 如果适用，与第三方提供的服务有关的系统信息，至少包括系统名称、版本和功能或目的。 5.与其他系统的接口及其目的，包括交换信息的细节。 6.开展该服务的完整地址，以及负责开展该服务的人员所在的位置。 7. 如果适用，合同系统的处理设备所在的主要数据中心的完整地址。 8. 在适用的情况下，处理设备所在的备用数据中心的完整地址。	金融机构应制定并维护其供应商清单，该清单中应列明服务提供商的基本信息，包括服务提供者的名称、所提供的服务详情等信息。 华为云将配合金融机构提供相关上报材料，配合金融机构履行监管要求。

8 华为云如何遵从及协助客户满足《保险与担保机构法》及相关通用规定的要求

墨西哥国家保险和债券委员会（CNSF）发布了保险与担保机构法及其通用规定，主要针对保险机构、担保机构和互助保险公司的经营和运作发布的具体监管规定。以下内容将总结金保险与担保机构法及其通用规定中与云服务提供商相关的控制要求，并阐述华为云作为云服务提供商，会如何帮助金融机构客户满足相关控制要求。

8.1 华为云如何遵从及协助客户满足《保险与担保机构法》的要求

编号	控制域	具体控制要求	华为云的应答
268	第九节： 对其他公司的投资和向第三方采购服务	金融机构与第三方签订外包业务服务合同需遵守以下规定： 1. 遵守与提供的服务相关的技术和业务准则，以及在提供服务时保障银行系统用户信息的保密性的相关规定。 2. 金融机构应制定第三方提供服务时操作和控制程序方面的要求。 3. 金融机构应制定相应的监控程序和政策，以确保能监控第三方履行合同的情况。其中应包括第三方有义务根据国家银行和证券委员会以及机构的外部审计员的要求提供服务有关的记录、信息和技术支持。 4. 国家银行和证券委员会和金融机构有权在任何时候对第三方服务商进行审计，监督和监测，且金融机构有义务向国家银行和证券委员会提供相关报告。国家银行和证券委员会可根据对第三方的审计结果向金融机构发出意见或纠正措施。 5. 第三方的经理和雇员，以及离职员工也应遵守本条规定。 6. 金融机构可能不同意由第三方独家提供的业务和服务。 7. 若金融机构未能遵守本规定或可能影响信贷机构业务连续性或保护公众利益的情况下，CNBV委员会可在机构获得听证权利后，下令部分或全部、暂时或最终暂停通过有关第三方提供的服务或委托。	金融机构应在与第三方签订的合同中约定对第三方所提供服务的安全控制的要求，并制定第三方绩效监控政策监控第三方对服务合同的履行情况。 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，可根据金融机构的需求进行定制化。

编号	控制域	具体控制要求	华为云的应答
269	第九节： 对其他公司的投资和向第三方采购服务	1. 金融机构与第三方签订外包服务，不能免除金融机构或其董事、雇员遵守本法律条例的规定和由此产生的通用规定的义务。 2. 国家银行和证券委员会可以通过金融机构要求第三方提供其提供外包服务的信息，包括书籍、记录和文件。	金融机构与第三方签订外包服务，但不能外包法律责任，金融机构或其董事、雇员均应按本法要求承担相应的责任。金融机构应配合国家银行和证券委员会，向金融机构的外包服务商收集相关信息。 华为云会安排专人积极响应金融机构的要求，并提供相关材料。

8.2 华为云如何遵从及协助客户满足《适用于保险与担保机构法的通用规定》的要求

编号	控制域	具体控制要求	华为云的应答
3.6.3	第3.6节：向第三方采购服务	金融机构与第三方签订服务外包合同应考虑： 1. 第三方机构有必要的技术、财务、行政和法律经验和能力来完成相应的服务。 2. 建立业务连续性和应急计划，以处理因第三方导致的紧急情况。 3. 界定数据库管理责任，并要求相关信息的保密性和安全性。 4. 确定第三方是否有内部控制制度，并要求第三方定期接受培训。 5. 限制第三方分包服务的可能性。	金融机构应将相关要求写入与第三方签订的合同。金融机构应制定第三方服务提供商的选择标准、监控第三方绩效和合同履行情况的机制。 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，可根据金融机构的需求进行定制化。

编号	控制域	具体控制要求	华为云的应答
4.10.16	第4.10节：关于使用电子手段签订保险和担保交易的规定	使用电子手段执行业务和提供服务的机构，应在通过这种电子手段传输、储存和处理信息方面采取安全措施或机制，以防止其被第三方所知。为此，各机构应遵守以下规定： 1. 在通过电子手段处理的敏感用户信息（如密码、个人识别号码（PIN）、任何其他认证因素）的传输过程中，对信息进行加密或使用加密的通信手段。 2. 金融机构应确保将加密密钥以及加密和解密系统安装在高度安全的设备中，如HSM（硬件安全模块），且具有防止未经授权访问和披露的管理措施。	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。 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（VPN）**、**云专线（DC）**、**云连接（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。

编号	控制域	具体控制要求	华为云的应答
4.10.17	第4.10节：关于使用电子手段签订保险和担保交易的规定	金融机构建立数据库、文件以及存储介质的访问控制，应遵守以下规定。 1. 只允许本机构被授权的人员访问数据库和文件，并记录每次访问的详情。 2. 远程访问通道应使用加密机制。 3. 制定安全程序，销毁含有敏感用户信息的存储介质。 4. 制定与通过电子手段传送和接收的信息有关的政策，并核实第三方是否遵守相应政策。 5. 未经授权的访问，将被追究法律责任，包括为金融机构提供服务的第三方。	金融机构应建立用户访问管理机制，对访问系统的行为进行权限限制和监督。 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。 金融机构可通过华为云的**统一身份认证服务（IAM）**对使用云资源的用户账号进行管理。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。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（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。 为配合客户遵从监管要求，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

编号	控制域	具体控制要求	华为云的应答
			限定只能访问本角色所管辖的设备。 在金融机构确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除金融机构与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。
4.10.18	第4.10节：关于使用电子手段签订保险和担保交易的规定	1. 如果经纪公司或为其提供服务的第三方保管的敏感信息被提取、丢失，或经纪公司怀疑有人未经授权获取这些信息，总经理或其指定的工作人员应在有关事件发生后的5个日历日内，以书面形式向CNBV委员会报告。 2. 经纪公司立即调查导致敏感信息被删除、丢失或未经授权访问的原因，调查的结果、进展、改进措施应在事件发生后三个月内送交CNSF委员会。 3. 事件发生或知晓后的3个工作日内，通过客户自己指明的通知方式将其信息可能被提取、丢失或被非法获取的情况通知客户。 4. 核实有关事件后立即向经纪公司的审计委员会和风险委员会通报。	金融机构应根据本通用规定的要求制定数据泄露响应流程，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，以及供应商导致的数据泄露如何响应。 为配合金融机构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，及时知会金融机构。

编号	控制域	具体控制要求	华为云的应答
4.10.20	第4.10节：关于使用电子手段签订保险和担保交易的规定	金融机构应记录在技术基础设施中发现的事件、故障或漏洞，其中至少应包括与发现的故障、操作错误、试图进行的计算机攻击和实际进行的攻击有关的信息，以及技术基础设施用户的信息丢失、被提取、被篡改、丢失或被不当使用。所提供的信息应至少包括事件发生的日期和事件的简要描述、持续时间、受影响的服务、受影响的金融机构和涉及的金额，以及实施的纠正措施。且相关信息应以金融机构确定的方式进行备份，并应至少保存10年。	金融机构应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志，并按照既定的规则对日志进行备份，备份信息应至少留存10年。 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，以确保支撑网络安全事件回溯和合规。该日志分析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。华为云有专门的内审部门，定期对运维流程各项活动进行审计。 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。 华为云提供了多粒度的数据备份归档服务，以满足客户不同场景下的需求。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。

编号	控制域	具体控制要求	华为云的应答
4.10.21	第4.10节：关于使用电子手段签订保险和担保交易的规定	1.金融机构应建立日志审计制度，包括： a) 对信息的访问记录： b) 访问时间。 2.金融机构的日志应至少存储180个自然日，并建立防止篡改的机制，以及访问控制程序。 3. 各机构必须定期审查本节中提到的日志，如果发现任何异常事件，必须向审计委员会和风险管理领域的负责人报告。	金融机构应建立用户访问管理机制，对访问系统的行为进行权限限制和监督。并定期执行日志审计。 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，以确保支撑网络安全事件回溯和合规。该日志分析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。华为云有专门的内审部门，定期对运维流程各项活动进行审计。 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。

编号	控制域	具体控制要求	华为云的应答
4.10.23	第4.10节：关于使用电子手段签订保险和担保交易的规定	金融机构应建立基础设施审查制度，其中应明确规定： 1. 至少每年或在此类基础设施发生重大变化时进行审查，至少包括： a) 用户认证机制。 b)基础设施的配置和访问控制。 c) 操作系统和软件所需的更新。 d) 基础设施和系统的脆弱性分析。 e) 识别对原始软件可能进行的未经授权的修改。 f) 与电子媒体相关的技术基础设施、系统和流程。 g) 对与电子服务有关的关键应用程序进行系统分析，以发现错误、未经授权的功能。 2. 金融机构应采用自动化手段检测和防止可能影响用户信息的保密性，完整性和可用性的事件和未经授权的访问。	金融机构应根据本通用规定的要求建立基础设施审查制度。 华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性。此外，独立第三方评估机构也提供独立保证，这些评估员通过执行定期安全评估和合规性审计或检查（例如SOC、ISO标准、PCIDSS审计）来评估信息和资源的安全性、完整性、机密性和可用性，从而对风险管理内容/流程进行独立评估。 华为云会安排专人积极配合客户发起的审计要求。

编号	控制域	具体控制要求	华为云的应答
12.1.6	第12.1节：关于与第三方的服务采购	金融机构必须在与第三方签订的外包服务合同中规定： 1. 信息的所有权，保密性条款和责任条款。 2. 知识产权。 3. 核查对合同条款的遵守机制。 4. 第三方的应急计划。 5. 第三方的培训计划。 6. 第三方必须遵守的技术、操作、控制程序和法律法规的要求。 7. 第三方需接受： a) 接受机构的外部审计员、CNSF委员会或CNSF委员会本身指定的第三方机构访问外包服务商的物理场所，以核实机构所订的服务或委托是否允许后者遵守适用于它的法律规定。 b) 应机构的要求，向机构本身的外部审计员和CNSF委员会或其指定的第三方提供与服务有关的系统、记录、手册和文件。它还应允许负责的人员可以访问与提供的服务有关的办公室和设施。 c) 如果第三方服务提供商的企业宗旨或内部组织发生任何可能影响到合同所涉及的服务提供的变化，至少提前45个日历日通知机构。	金融机构应按照相关要求制定与第三方的合同。 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，可根据金融机构的需求进行定制化。华为云可能会随时自行修改或中止服务或修改或移除服务的功能。如果您订阅的服务发生重大变更或中止，我们会通过在我们的网站发布通知或其他方式通知您。。

编号	控制域	具体控制要求	华为云的应答
12.1.7	第12.1节：关于与第三方的服务采购	金融机构必须在签订合同前确定第三方是否具有相关经验、技术、财务、行政和法律能力，以及必要的物质、财务和人力资源，以保证在提供此类服务时具备可靠性和安全性。	金融机构应在选择服务提供商前进行尽职调查，确保第三方服务提供商的可靠性和安全性。 华为云会安排专人积极配合客户发起的审计要求和尽职调查。 **技术能力：**华为云用在线提供云服务的方式，将华为30多年在ICT基础设施领域的技术积累和产品解决方案开放给金融机构。华为云具备全栈全场景AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现金融机构价值最大化。 **财务状况：**华为云是华为的云服务品牌，自2017年正式上线以来，华为云一直处于快速发展中，收入保持强劲增长态势。 **商业声誉：**华为云一如既往坚持“以金融机构为中心”，让越来越多的金融机构选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现大突破。 **适合金融机构的企业文化和服务政策：**华为云在产品和服务规划和阶段会根据金融机构业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足金融机构的需求。华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等金融机构提供端到端的云解决方案。
12.1.9	第12.1节：关于与第三方的服务采购	金融机构董事会批准的政策和标准必须规定可以对第三方进行审计。	金融机构应在制度中规定对第三方服务提供商的审计要求和程序，并获得董事会的批准。 华为云会安排专人积极配合金融机构发起的审计要求。金融机构对华为云的审计和监督权益会根

编号	控制域	具体控制要求	华为云的应答
12.1.10	第12.1节：关于与第三方的服务采购	第三方外包服务提供商必须接受CNSF委员会对金融机构和所签约服务的检查和监督。	据实际情况在与金融机构签订的协议中进行承诺。

9 结语

本文通过让客户了解华为云对墨西哥金融行业监管要求的遵从情况，让客户安全、放心地通过华为云的服务存储、传输和处理数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合墨西哥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墨西哥金融行业监管要求的遵从性。

10 版本历史

日期	版本	描述
2021年12月	1.0	首次发布