华为云南非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，南非共和国储备银行审慎监管局（PA）发布了一系列监管指令和指南，针对南非金融机构科技外包管理、云计算及数据离岸管理等方面提出了相关监管要求。另外，南非金融部门行为管理局（FSCA）（前身FSB）针对保险业务外包发布了相关的监管指令。

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。本文将针对南非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 适用的南非金融监管要求简介

当前，南非采取的是“双峰监管模式”，并赋予两个独立的监管机构行使金融部门的监管职责：

南非储备银行审慎监管局（PA）：

审慎监管局（PA）是设立在南非储备银行（SARB）的管理框架之内的一个独立机构，负责南非金融机构的审慎监管，其工作重点是维护和加强金融机构的金融安全和稳健，保障金融客户免受金融机构未能履行义务时所带来的风险。PA颁发了相关的指令及指南用来规范对南非银行、保险公司、合作金融机构以及合作银行审慎监管：

- D3/2018 **云计算与数据离岸外包指令（Cloud Computing and the Offshoring of Data）**（下文简称“D3/2018”）：规定了金融机构在选择云计算和/或数据离岸外包管理后的监管要求。本部指令应与G5/2018指导说明一起考虑。
- G5/2018 **云计算与数据离岸外包指南（Cloud Computing and the Offshoring of Data）**（下文简称“G5/2018”）：是针对D3/2018指令的指导说明，应与D3/2018指令一起考虑。
- G5/2014 **银行职能外包指南（Outsourcing of Functions within Banks）**（下文简称“G5/2014”）：说明了金融机构选择外包服务提供商产生的潜在风险，并提供了指南用于评估与外包相关的风险，以及适当的风险管理方案要素。

- D2/2019 **重大IT/网络事件报告（Reporting of Material Information Technology and/or Cyber Incidents）**（下文简称“D2/2019”）：规定了金融机构在发生重大IT事件或网络事件时上报PA的要求。
- G4/2017 **网络韧性（Cyber Resilience）**（下文简称“G4/2017”）：是针对金融机构网络韧性的管理要求，强调了安全有效的运营对维持和促进金融稳定与经济增长的重要性。

金融部门行为管理局（FSCA）：

负责提升和支持金融市场的效率和廉正，保障金融客户，推动公平对待金融客户。为规范金融机构的外包管理，本机构颁发了相关的指令及指南：

- **保险外包指令（Directive 159.A.i）**（下文简称“159指令”）：是针对保险公司（包括再保险公司）外包管理方面的立法要求。不论保险公司是否位于南非境内，或是保险公司的任何子公司，均应遵守本指令。

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。
- **云计算**

  被定义为一种模型，这个模型可以方便地按需通过网络访问一个可配置的共享计算资源（如网络、服务器、存储设备、应用和服务）。这些资源可以被迅速提供并发布，同时使管理成本及服务提供商的干涉最小化。
- **数据离岸管理**

  是指在南非国界之外存储和/或处理数据。
- **外包**

  定义为使用服务提供商（无论是公司集团内的关联公司还是第三方）来持续执行业务活动、服务、功能或流程，并且这些外包活动应由金融机构或金融机构代表承担最终责任。
- **内包**

  指职能和活动外包给某一金融机构集团所属的特定机构。
- **离岸外包**

  指金融机构将与南非业务相关的重要商业活动或职能外包给在南非境外从事外包活动的服务提供商（即无论公司的注册地，仅以处理活动的地理位置为准）。
- **重大业务活动或职能**

  指可能对金融机构的业务运营产生重要影响，或会破坏管理金融机构风险的有效机制的活动或职能。
- **重大事件**

  指业务活动、流程或功能的中断已经或可能对金融机构的业务、对客户的服务或更广泛的金融系统和经济造成严重和广泛的影响。
- **IT事件**

  定义为事态，它的发生或其影响都是作为金融机构正常运营非预期或非计划的，并且有可能扰乱金融机构IT系统或服务的正常运行。

- **网络事件**

  在信息系统中出现的任何可观察的事件(i)危及信息系统的网络安全或由系统处理、存储或传输信息的安全；或(ii)违反安全策略、安全流程或可接受的使用政策，无论是否由恶意活动造成。

2 华为云安全与隐私合规

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

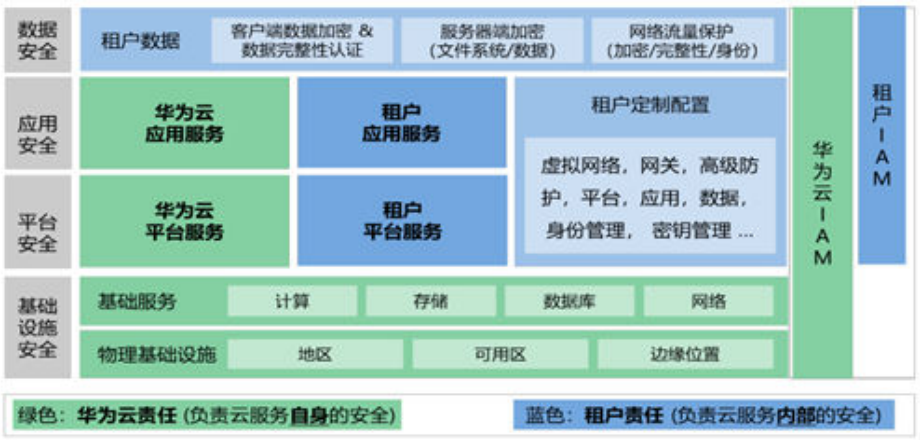
认证	产品介绍
网信办网络安全审查（中国）	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。
MTCS Level 3认证（新加坡）	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3 等级认证。
OSPAR认证（新加坡）	OSPAR是新加坡银行业工会（ABS）对外包服务提供商出具的审计报告。华为云通过了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

3 华为云安全责任共担模型

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要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 华为云如何符合 PA“云计算与数据离岸外包”的要求

“D3/2018”与“G5/2018”一同阐述了南非金融机构选择使用云服务或数据离岸外包服务时，南非审慎监管局（PA）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。“D3/2018”为指令，具有法律效力，为高阶的管理要求，“G5/2018”为指南，是针对“D3/2018”指令的落地指南。

南非金融机构在遵循“D3/2018”与“G5/2018”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“G5/2018”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这些控制要求。

5.1 数据策略和框架

“G5/2018”第4.1章要求金融机构应制定数据策略及框架，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
4.1.1	数据策略和框架	数据策略/框架应包括： 1）金融机构如何对数据进行分类； 2）数据可以存储在哪里（在哪个立法管辖区）； 3）各类数据（数据分类后）分别适用于哪种云存储服务和部署模型； 4）各类数据（数据分类后）分别适用于哪些安全要求和限制；和 5）与金融机构数据丢失和违规处理相关的流程。	客户应按照监管要求制定并实施数据管理策略。华为云建议客户在数据创建阶段首先做好数据分类，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，在数据生命周期的起始阶段就做好数据的区分与隔离。 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），可支持客户根据其需求选择数据存储位置。除了公有云服务，华为云还为客户提供私有云和混合云解决方案。华为云向客户提供一系列数据存储服务，包括**云硬盘（EVS）**、**对象存储服务（OBS）**等，服务遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，保证租户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。 华为云制定了完善的突发事件应 急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。

编号	控制域	具体控制要求	华为云的应答
4.1.2	资产登记	金融机构应对其所有信息资产进行登记，包括数据、IT应用、系统和流程。信息资产均应根据数据分类策略进行分类。还应注意数据所在的位置应符合数据留存要求以及信息安全要求。	客户应对其信息资产进行统一管理，其中应标注相应资产的分类，及其数据存储的物理位置（国家或地区），并识别该国家或地区发布的关于数据留存的要求和信息安全的要求。 华为云为客户提供统一的管理界面，供客户查询并管理其购买的华为云资源。客户也可使用华为云的**企业主机安全（HSS）**的资产管理功能对其资产进行统一管理。
4.1.4	通知上报	金融机构应有明确定义数据丢失和泄露流程，其中应包括通知和上报利益相关者的流程。	客户应制定数据泄露流程，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。

5.2 风险控制框架

“G5/2018”第4.4章要求金融机构应制定有效的风险控制框架，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.4.1	风险控制框架	1、金融机构应确保其审计计划和审计工作可以覆盖服务提供商提供的云服务或数据离岸管理服务。 2、说明当云服务、数据离岸管理服务或合规要求发生变化后（包括相关威胁和漏洞的变更），可能触发的额外审计工作。 3、金融机构在执行审计或评估工作时，应将金融机构和服务提供商相关IT控制均纳入到测试范围，验证控制的有效性。	客户应制定信息科技审计计划，并在执行审计工作时，将服务提供商提供的云服务或数据离岸管理服务相关的IT控制纳入其中。 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。

5.3 事前风险评估

“G5/2018”第4.5章要求金融机构在使用云计算或数据离岸管理服务前进行风险评估，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.5.1	风险评估	1、风险评估应识别所有涉及的风险，并确定是否已采取或实施了适当的控制措施，使其符合金融机构的风险偏好。 2、金融机构应识别、评估、管理、缓解和报告与云计算或数据离岸管理相关的风险，以确保服务提供商的运营及财务状况能够持续履行对所有利益相关方（包括客户和监管机构）的职责。 3、在使用云服务或数据离岸管理服务之前，金融机构应充分了解风险，并确保风险可管控。需要被考虑的因素包括连续性、数据保护以及审慎局和监管提出的合规要求，并且不应影响监管人员执行审慎职责的能力。 4、风险评估应被记录在案，并为管理层提供足够的信息以用于决策。 5、应指定责任人跟踪、处理与云服务或数据离岸管理服务相关的风险。 6、监控和管理外包关系的机制应根据风险评估的结果进行更新。 7、风险评估中应考虑使用云计算或数据离岸管理服务的可持续性，以及对恢复先前安排的影响。	客户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。 技术能力：华为云用在线提供云服务的方式，将华为30多年在ICT基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 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“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现大突破。在海外市场，华为云香港、俄罗斯、泰国、南非、新加坡大区相继开服。 适合金融机构的企业文化和服务政策：华为云在产品和服务规划和阶段会根据客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。华为云结合行业需求特点和华为丰富

编号	控制域	具体控制要求	华为云的应答
			的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。
4.5.2	合规要求识别	金融机构应考虑应由谁、在哪里、如何来提供服务。使用分包和涉及不同司法管辖区的情形应不影响金融机构对其所有利益相关方履行职责，包括数据留存的要求。	客户应识别其适用的司法管辖要求，并按照司法管辖要求（如：识别法律法规中对于数据留存的要求）决策应由哪家服务提供商、在哪些国家或区域、以何种方式提供服务。 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），可支持客户根据其需求选择数据存储位置及配置留存期限。

5.4 尽职调查

“G5/2018”第4.6章要求金融机构在使用云计算或数据离岸管理服务前进行尽职调查，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.6.1	尽职调查和选择	1、金融机构的高级管理层应与服务提供商就服务水平进行约定，并确保服务提供商有能力按照约定的服务水平提供服务。 2、在签订合同之前，还应该评估服务提供商在治理、风险和合规等方面的管理情况。 3、尽职调查需要考虑的因素包括所涉及的风险、范围、复杂性、业务活动或功能的重要性，以及服务提供商的声誉和行业地位。 4、所有的投资都应该遵循适当的治理流程，以确保战略是适合的以及业务是准备就绪的。 5、金融机构应维护一份供应商清单（服务良好的供应商），在选定云服务或数据离岸管理服务供应商时，在该清单中选取。同时，为支持金融机构的业务连续性，可在该供应商清单中选取可行的备选供应商。	客户应在选择服务提供商前进行尽职调查，特别是在治理、风险和合规管理方面的机制。客户应针对声誉良好的供应商制定一份供应商清单，并在该清单中选取服务提供商及备选供应商。 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内容和服务水平以及华为云的职责。同时，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。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。 技术能力：华为云用在线提供云服务的方式，将华为30多年在ICT基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 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“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监

编号	控制域	具体控制要求	华为云的应答
			控、基因、汽车制造等行业，华为云已实现大突破。在海外市场，华为云香港、俄罗斯、泰国、南非、新加坡大区相继开服。 适合金融机构的企业文化和服务政策：华为云在产品和服务规划和阶段会根据客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。
4.6.2	业务用例	1、金融机构应制定每一个迁移上云或使用数据离岸管理服务的业务用例。业务用例应该清楚地识别使用云服务或数据离岸管理服务是否可以支持金融机构的业务战略。 2、业务用例应该清楚地定义预期收益以及如何度量这些收益。 3、业务用例应包含成本收益分析。 4、业务用例应说明金融机构数据的处理策略，例如，数据分类和数据留存方面的策略要求。	客户应制定迁移上云的业务用例，其中应包括评估使用云服务是否满足自身的业务战略、使用云服务的预期收益和成本收益分析过程以及数据的处理策略。 华为云为客户提供上云迁移服务。华为云将基于客户提供的信息，与客户一同商定并确认具体业务目标及范围，通过需求分析为客户设计迁移方案并制定迁移计划和迁移演练等。

5.5 机密性、完整性和可用性

“G5/2018”第4.7章要求金融机构应确保其IT资产的机密性、完整性和可用性，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.7.3	信息安全评估	应从IT系统的重要性、所涉及的流程或活动的性质、数据的分类、涉及的服务提供商、数据位置和云部署模型等方面对信息安全控制进行定期的风险评估。	客户应建立风险评估框架，定期评估外包安排相关的风险。 华为云可配合并积极响应客户需求。此外，华为云内部也制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。
4.7.4	信息安全考虑	1、金融机构应在合同中要求服务提供商应遵循金融机构的安全管理要求。 2、金融机构应收集服务提供商已获得的认证。 3、金融机构应在合同中与服务提供商约定违反相关要求下的责任和惩罚，以及对于数据泄露事件的责任分担说明。	客户应定期对其外包服务供应商执行独立审计或专家评估，确保服务提供商按照不低于自身安全管理要求的前提下提供云服务。 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。 华为云提供了线上的**《华为云用户协议》**，其中规定了华为云的职责。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。

编号	控制域	具体控制要求	华为云的应答
4.7.5	保障和测试	1、与服务提供商签订的合同协议应规定金融机构将如何验证服务提供商是否遵循合同约定的信息安全要求。这可能包括但不限于，提供该服务提供商的认证/审计报告（包括NIST、CSA和ISACA发布的相关认证和审计报告）以及任何其他安全测试的需求，如漏洞扫描和渗透测试。 2、金融机构应收集服务提供商信息安全策略的副本，以确定该策略满足金融机构与服务提供商签订的服务水平协议(SLA)的要求。	客户应确保其选定的服务提供商可按照合同及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。为配合客户满足合规要求，华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。 华为云参照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
4.7.6	安全标准	服务提供商数据中心物理安全的管理要求不得低于金融机构数据中心物理安全的管理要求。	客户应要求服务提供商的物理安全管理机制不得低于金融机构的管理机制。 华为云已制定并实施了完善的物理和环境安全防护策略、规程和措施，满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中的 T3+ 标准。更多详细信息请参见**《华为云安全白皮书》**的“物理与环境安全”。

编号	控制域	具体控制要求	华为云的应答
4.7.7	访问权限	1、对云上的信息资产或离岸数据的访问权限应该根据金融机构的访问控制策略加以限制，例如，管理员对操作系统和数据库的访问限制。 2、使用服务提供商提供的云服务或数据离岸管理服务时，应制定并实施足够的用户访问权限控制，以限制服务提供商对金融机构数据、系统和基础设施的访问。这应该在细颗粒度和最小授权原则的基础上进行。金融机构对这些控制部署是否到位并有效运行负有最终责任。 3、金融机构有责任确保用户权限分配(入职时)、用户权限回收(中止时)和工作职能变更的流程均可以按照用户访问策略进行及时的管理和控制。	客户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。 客户可通过华为云的**统一身份认证服务（IAM）**对使用云资源的用户账号进行管理。IAM除了支持密码认证之外还支持多因子认证，客户可自主选择是否启用。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。为配合客户满足合规要求，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
4.7.8	加密	1、金融机构应根据云服务或数据离岸安排中涉及的数据分类来确定所需的加密级别。对于云计算，采用的云部署模型在确定适当的加密级别时也很重要。所有后续的加密考虑都应符合以下原则：加密水平应与数据的重要性和所涉及的风险相一致。 2、金融机构会使用不同的分类方法，但对于多租户、社区云或公有云环境中的任何个人数据、隐私数据或机密数据，金融机构应该考虑在传输和存储过程中对这些数据进行加密。 3、如果需要加密，数据应该在传输至云上或离岸之前进行加密，对于存储中和传输中的数据应使用相同级别的加密服务。 4、应根据金融机构的密钥管理策略和程序来限制对加密密钥的访问。在涉及服务提供商时，密钥管理也应使用与金融机构策略与程序的相同水平的控制来进行。 5、策略和程序应包括公钥基础设施、使用的加密协议设计和算法、对于安全密钥生成、恢复、交换和存储的适当的访问控制(如适用)。	客户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。如需上云，应在上云前考虑采用业内认可的加密算法和密钥管理机制对数据加密并妥善保管相关密钥。 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）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。华为云为客户提供了**数据加密服务（DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，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客户根密钥。DEW还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、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》**6.8.2数据加密（DEW）服务。 对于传输中的数据，当客户通过互联网提供 Web 网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给

编号	控制域	具体控制要求	华为云的应答
			Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。针对客户业务混合云部署和全球化布局的场景，可以使用华为云提供的**虚拟专用网络（VPN）**、**云专线（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
4.7.9	事件管理	1、应在云服务或数据离岸管理服务的合同协议中参考双方的事件管理流程规定各自的角色和职责。 2、事件管理流程应包括事件通知、事件响应、事件补救、事件文档化、事件时间安排、事件风险处理和升级、事件的正式关单管理。 3、与服务提供商签订的合同协议应明确事件的类型(例如数据泄露和安全违规事件)、事态以及每次事件后应采取的行动。 4、当金融机构的数据可能被南非境外机构抓取或访问时，应通知金融机构，即使是基于该国适当的法律程序。	客户应当建立信息安全事件管理机制，并在合同中明确双方在事件管理流程中的角色和职责。 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。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。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

编号	控制域	具体控制要求	华为云的应答
			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。 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。如：说明事件发生时双方的角色和职责划分。
4.7.10	云上多租户	金融机构应考虑制定安全配置基线，以防止与其他客户环境的交叉影响。	客户应就其云环境制定适当的安全配置基线。 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。客户可以使用华为云提供的**虚拟私有云（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
4.7.11	虚拟化环境	1、金融机构应了解服务提供商使用的虚拟化类型，并评估服务提供商环境中的安全级别是否足够，或者是否应通过额外的安全技术来增强。 2、作为定义和达成安全标准的一部分，应该定义用于加固虚拟化操作系统的安全配置基线（如果适用的话）。 3、协定的安全标准应可以进一步解决hypervisor漏洞管理、补丁管理和发布管理的问题，特别是在发现新的漏洞时。	客户需对所有系统制定安全配置基线，并定期进行基线检查。针对不符合安全配置基线的情况，需进行风险评估并制定补偿措施。 客户可使用华为云**企业主机安全（HSS）**对主机进行基线检查，包括检测系统口令复杂度策略、经典弱口令、风险账号，以及常用系统与中间件的配置，以识别不安全项目，预防安全风险。 华为云已制定虚拟化操作系统的安全配置基线，确保客户使用云服务时的安全。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。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对租户业务造成影响。

5.6 合规

“G5/2018”第4.8章要求了金融机构在使用云计算或数据离岸管理服务时应考虑的合规问题，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.8.1 4.8.2 4.8.3	问责制 合规情况 合同合规	1、金融机构对服务提供商提供的服务负有最终法律责任。金融机构应与服务提供商在合同中约定相关的合规要求，并且金融机构有责任提供证据，证明服务过程的合规。 2、金融机构应识别使用云服务或数据离岸管理服务时适用的各地的法律法规要求。 3、合同协议条款中应包括允许金融机构对云计算/数据离岸管理活动的执行方式进行修改，特别是金融机构为满足合规要求时。如果金融机构使用第三方进行云计算/数据离岸管理时，金融机构应确保与服务提供商就合规要求达成合同协议，以确保数据托管行为可以持续遵守适用的法律法规。	客户可以采取协议约束、审查监督等方式确保服务供应商的安全政策、程序和控制措施符合适用的法律法规的要求。 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，在遵从客户所在国家或地区的安全法规以及行业监管要求的基础上，参考业界最佳实践从组织、流程、规范、技术、合规、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足客户的安全需求。华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。为配合客户满足合规要求，华为云根据内部管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。另外，华为云有专门的团队对云服务的产品说明和操作手册进行维护，在国际站上将至少提供英文版的文档。同时，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。

5.7 业务连续性

“G5/2018”第4.10章要求金融机构应就使用云计算或数据离岸管理服务制定应急计划，以保障业务连续性，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.10.1	能力	1、在与服务提供商签订合同前，金融机构应评估服务提供商是否有足够的能力持续有效地提供云服务或数据离岸管理服务。金融机构还应考虑在可预见的未来，服务提供商可能必须提供的潜在增值服务，包括容量的相关指标，如存储容量、带宽需求、增加的用户数量和每秒需处理的交易需求。 2、在与服务提供商签订合同前，金融机构应考虑金融机构与服务提供商之间的通信基础设施是否足以持续管理当前和未来的需求。	客户应确保其服务提供商拥有足够的能力确保其业务的连续性及可能的扩容需求。 华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，进一步排除单点故障的风险。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。 为配合客户满足合规要求，华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对租户云服务的系统性能造成影响。同时，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。

编号	控制域	具体控制要求	华为云的应答
4.10.2	连续性和可恢复性	1、金融机构应该能够在合理的时间范围内，以及在法律和监管规定的时间范围内，从服务提供商的任何中断中恢复过来。 2、业务连续性要求，例如恢复时间目标和恢复点目标（RTOs和RPOs），应该通过业务影响评估来确定，并记录下来，如果涉及服务提供商，还应与服务提供商达成一致。 3、应制定灾难恢复计划和业务连续性计划，以确保金融机构业务的连续性，包括与事件恢复有关的事项、事件沟通的计划以及测试这些计划充分性和有效性的频率。 4、金融机构韧性应考虑使用云服务或数据离岸服务的影响。 5、金融机构在与服务提供商签订合同之前，应考虑服务提供商的业务连续性措施是否符合金融机构的要求。 6、金融机构应获得服务提供商业务连续性计划相关的审计报告或鉴证报告，包括灾难恢复测试、流程测试和控制测试，至少能证明其活动/功能是可管理的。 7、理想情况下，应要求服务提供商的业务连续性管理获得国际公认的认证或标准，如ISO 22301(业务连续性管理体系)。 8、在发生中断时，金融机构和服务提供商的角色和责任应在合同中明确定义。 9、应定期审查与外包活动有关的应急计划，且不少于一年一次。	客户应建立自身的业务连续性机制，并制定保证其关键业务连续的RTO、RPO指标。如果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。为配合客户满足合规要求，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，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

5.8 合同终止后的权利

“G5/2018”第4.11章要求金融机构应在合同中约定服务终止时有关互操作性的问题，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.11.1 4.11.2 4.11.4	计划终止合同协议互操作性	1、金融机构应避免出现服务提供商锁定的情形，且在退出云服务或数据离岸管理服务时，不会影响法律法规的遵守情况。 2、金融机构应与服务提供商在合同协议中明确双方在合同终止时双方的角色和职责。 3、合同协议中应包括：根据所涉数据的性质，金融机构的数据应及时、完全地删除并归还给金融机构、转移给其他服务提供商或被销毁。合同安排应包括足够的保证，在协议终止时，其数据被立即删除、转移或销毁。 4、金融机构应在外包活动给云服务提供商或数据离岸管理服务提供商之前考虑互操作性的问题。 5、金融机构应提前考虑由于选择的服务提供商无法满足合同义务时，如何将服务迁移至其它提供商的方案，并就该方案进行测试。 6、金融机构应就外包服务的环境制定应急计划，以在发生不可预见的事件时继续开展业务。	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，如迁移至本地数据中心。OMS和SMS支持国内外主流公有云厂商，SMS还支持国私有云平台虚拟机迁移、x86物理服务器迁移（覆盖约40种主流操作系统）。 在客户确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。

5.9 取证调查

“G5/2018”第4.12章要求金融机构在使用云计算或数据离岸管理服务时需明确的取证调查要求，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
4.12.1	适用性	1、金融机构应识别由于取证可能对云上数据/离岸数据产生的风险，并制定相应的控制措施，确保不低于金融机构的风险偏好。 2、确保云上或离岸管理中的数据在取证过程中的完整性。	客户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。
4.12.2	合同协议	金融机构应在合同里与服务提供商明确： 1）金融机构、监管机构和执法机关进行取证和调查的访问权限； 2）应部署相关控制以证明证据未被篡改； 3）明确双方在取证方面的角色和职责； 4）明确可以直接或使用哪些第三方工具进行取证； 5）明确双方在发现搜查、诉讼、证据保存和专家证言等方面的职责； 6）取证数据可被访问的期限； 7）规定服务提供商对金融机构数据保存的方式。	客户应按照相关要求制定与云服务提供商的合同。 华为云提供了线上的**《华为云用户协议》**，其中规定了华为云的职责。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。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。

5.10 合同协议

“G5/2018”第4.13章要求金融机构在使用云计算或数据离岸管理服务时应考虑的合同协议内容，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
4.13	合同协议	金融机构与服务提供商的合同中应明确： 1）金融机构数据的所有权问题，以及金融机构数据所有权如何受到托管国法律的影响； 2）数据仅可以存储在合同中明确的符合适用法律法规要求的地理位置； 3）哪些活动服务提供商可以进行分包，分包也需按照主合同进行； 4）服务提供商及其员工应对金融机构数据具有保密的义务，并按照最小授权原则为员工分配访问权限； 5）数据泄露时双方的角色和职责，以及数据泄露响应时实施的合作流程、以及泄露通知或其它的法律合规义务； 6）服务提供商不得妨碍金融机构满足其适用法律法规中对于数据留存相关的要求。	客户应按照相关要求制定与云服务提供商的合同。 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，可根据不同客户的需求进行定制化。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。

6 华为云如何符合 PA“银行职能外包”的要求

南非审慎监管局（PA）于2014年7月发布了“G5/2014”，主要用来帮助金融机构判断是否为“重大业务活动或职能”，以及该活动或职能外包后可能产生的风险。

南非金融机构在遵循“G5/2014”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“G5/2014”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这些控制要求。

编号	控制域	具体控制要求	华为云的应答
4.5	通知监管	金融机构应意识到云计算以及将重要的IT业务活动和功能离岸外包的重要性。 金融机构应在将重大业务活动离岸外包前通知南非金融监管机构。	客户应将使用云服务提供商或使用离岸外包服务识别为“重大业务活动或职能”外包，外包前需将外包活动通知南非The Office of the Registrar of Banks。 华为云将配合客户提供相关上报材料，配合客户满足监管通知的工作。 此外，为客户提供售后服务保障，华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由IM企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

编号	控制域	具体控制要求	华为云的应答
6.4	尽职调查和选择	金融机构应在签订外包协议之前，对潜在服务提供商进行评估，并进行必要的尽职调查。尽职调查需要包括的内容包括：业务背景和声誉，与其他人的合同安排冲突，战略与目标，费用结构和激励措施，财务业绩和状况，人力资源管理，事件报告和管理程序，信息安全，保险覆盖情况，司法管辖权问题和主权风险（跨境活动），法律法规遵从性，信息系统的管理，运营和内部控制，物理安全，公司负责人的资质、背景和声誉，分包商的依赖情况，韧性，以及风险管理。	客户应在签订外包协议前，对服务提供商进行评估，并进行必要的尽职调查。 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客户。华为云具备全栈全场景 AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 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“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、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客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。

编号	控制域	具体控制要求	华为云的应答
6.5	外包合同	1、外包合同或服务水平协议应在签署前获得金融机构法务审核，并确保包括以下内容：访问资产的途径，审计（包括审计权）和监督程序，业务中断和应急计划，服务开始和结束日期，信息的机密性、完整性、隐私性和安全性，客户投诉，违约安排和终止条款，争端解决安排，建立和监测绩效的标准，境外服务，激励薪酬审查，赔偿，保险，限制和责任，财务困难、灾难性事件和重大事件的通知，离岸安排，所有权和许可证问题，定价和费用结构，修正条款，定期审查规定，违约补救措施（包括提前退出选择），报告要求，提供、接收和保留信息的责任，遵守适用法律法规的责任，审查规定，监管机构的权利（包括不受限制地获取信息的权力），角色、权利和责任，拟提供的安排和服务的范围和性质，服务级别和业务绩效要求，和分包。 2、金融机构应在合同里规定服务提供商出现分包后的职责分配问题，包括由分包商引起的故障涉及的赔偿责任。金融机构理应在合理可行的范围内解决与管理与每个外包安排相关的风险有关的所有问题。所有法律文件应按照金融机构的法律文件管理程序。	客户应按照相关要求制定与云服务提供商的合同。 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，可根据不同客户的需求进行定制化。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。

编号	控制域	具体控制要求	华为云的应答
6.6	管理和监控关系	金融机构应确保拥有足够和适当的资源来随时管理和监控外包关系，并且指定具备专业知识的人员负责。监控内容包括服务提供商的系统是否得到有效的控制，供应商的财务问题，是否按照协议约定履行，问题的升级处理等，同时金融机构还需定期与供应商的高级管理人员保持适当的联系。	客户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。 华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。同时，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。此外，华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由IM企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

编号	控制域	具体控制要求	华为云的应答
6.7	应急计划和业务连续性	金融机构应针对任何职能的外包制定应急计划和预案，并且每年至少审查一次。应急计划应至少包括以下内容： 1）考虑备选服务提供商，以及业务切换到新服务提供商的流程； 2）制定寻求替代供应商的流程和程序，并确保该过程对业务影响最小； 3）确保金融机构拥有或能够随时获得所需的必要记录； 4）针对购买的服务或产品，制定了灾难恢复计划和业务连续性计划； 5）评估服务提供商的灾难恢复计划和业务连续性计划的充分性和有效性，并确定是否与自身计划一致； 6）记录金融机构应由谁来维护和测试服务提供商的业务连续性计划和应急计划； 7）定期获取测试证据，以证明服务提供商的业务连续性和应急计划是充分和有效的； 8）在签约的服务提供商无法执行任务的情况下，维持建立退出策略，包括可提供服务的服务提供商资源池； 9）金融机构应考虑，当决定取消外包功能或活动，金融机构进行自行管理时，应当考虑的要求。	客户应建立自身的业务连续性机制，并制定保证其关键业务连续的RTO、RPO指标。如果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。为配合客户满足合规要求，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，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。 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，如迁移至本地数据中心。

编号	控制域	具体控制要求	华为云的应答
6.9	信息的监督访问	金融机构与服务提供商签订的合同中，应包括在南非金融监管机构认为必要时，可对服务提供商进行现场检查的权利。如金融机构管理层意识到任何外包相关的功能和资料访问受限时，必须通知南非金融监管机构。	客户应按照相关要求制定与云服务提供商的合同。 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，可根据不同客户的需求进行定制化。如：南非监管对华为云现场检查的权利。
6.10	外包评估	1、金融机构管理层应确保金融机构拥有适当的流程以识别和处理与外包相关的风险，包括由金融机构内外部审计人员、或独立的第三方人员对服务提供商进行评估的流程。 2、金融机构管理层应确保有能力解决在服务提供商处进行调查时所引起的问题，并在需要时采取适当的措施。 3、金融机构的内审应确保重要外包业务活动符合金融机构的外包策略，并将评估结果上报金融机构董事会或审计委员会。南非金融监管机构可聘请外审或外部专家对金融机构的重大业务外包职能和活动进行评估（可能包括IT系统、数据安全、内部控制框架和业务连续性等领域），评估结果提供给南非金融监管机构，相关费用由金融机构提供。	客户应制定外包管理流程和机制，确保与外包相关的风险得到适当的识别和管控。同时，南非金融监管有权聘请外审或专家对客户的重大业务外包职能和活动进行评估，且评估费用由客户自身承担。 华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。同时，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。 如客户需进行监管上报的工作，华为云将配合客户提供相关材料。

7 华为云如何符合 PA“重大 IT/网络事件报告”的要求

南非审慎监管局（PA）于2019年9月发布了“D2/2019”，主要提出了金融机构在发生重大IT事件或网络事件时上报PA的要求。

南非金融机构在遵循“D2/2019”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“D2/2019”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这些控制要求。

编号	控制域	具体控制要求	华为云的应答
2.1	指令	1. 金融机构应建立和维护一套IT治理框架，确保关键业务功能、资源和基础设施均可得到充分管理和监督； 2. 金融机构应建立一个健全的事件管理流程，用来管理和报告IT及网络事件； 3. 发生重大IT或网络事件后，金融机构应在一天内通知PA（应填写“重大IT和网络事件报告”表格，并提交SARB-PA-ITIncidentReporting@resbank.co.za）； 4. 金融机构应在通知PA之日起14个日历日，向PA提交事件的根因分析和影响分析报告。	客户应制定一个完善的事件管理流程用来管理和报告IT及网络事件，客户应在流程中明确在发生重大IT事件或重大网络事件的一天内按照南非审慎监管局的要求上报PA，并在上报后的14个日历日内，向PA提交事件的根因分析和影响分析报告。 为配合客户满足重大IT事件和重大网络事件上报PA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。

8 华为云如何符合 PA“网络韧性”的要求

南非审慎监管局（PA）于2017年5月发布了“G4/2017”，该指南是在国际通用的《金融市场基础设施网络韧性指南》基础上对南非金融机构业提出的关于网络韧性方面的要求。

南非金融机构在遵循“G4/2017”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“G4/2017”中与云服务提供商相关的控制要求以及对应《金融市场基础设施网络韧性指南》中的具体指标，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这些控制要求。

编号	控制域	G4/2017控制要求	金融市场基础设施网络韧性指南具体指标	华为云的应答
2.3.3	恢复时间	金融机构的恢复时间目标应基于全面的业务影响评估，并考虑所有其他相关的法律和法规要求。此外，在设计韧性原则时应考虑高可用性和故障转移，以最大程度地减少对客户的影响。	6.2.2 应在2小时内恢复（即RTO为2小时）。应对财务系统最终设定的恢复目标进行规划和测试。FMI应设计和测试其系统和流程，以便在中断后两小时内安全恢复关键运行，并能够在中断当天结束前完成结算，即使在极端但合理的情况下也是如此。	客户应建立自身的业务连续性机制，并制定保证其关键业务连续的RTO、RPO指标，且财务系统的RTO应不低于2小时。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。 华为云为向客户提供持续、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。为配合客户满足合规要求，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

编号	控制域	G4/2017控制要求	金融市场基础设施网络韧性指南具体指标	华为云的应答
				现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。
2.3.4	安全测试	关于安全测试，特别是渗透测试，在使用第三方时，要求金融机构使用信誉良好的外部服务提供商进行此类测试，例如，可以通过认证或认可来证明这一点。	7.2.2 FMI应进行渗透测试，以识别可能影响其系统、网络、人员或流程的漏洞。为了深入评估FMI系统的安全性，这些测试应该模拟对系统的实际攻击。应定期在系统更新或部署时对面向互联网的系统进行渗透测试。在适用的情况下，测试可包括其他内部和外部利益相关方，如业务连续性、事件和危机应对团队中的利益相关方以及第三方如服务提供商和参与者。	客户应建立有效的安全测试机制，定期对关键信息系统进行安全测试。 为配合客户满足合规要求，华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。

编号	控制域	G4/2017控制要求	金融市场基础设施网络韧性指南具体指标	华为云的应答
2.3.5	态势感知	金融机构的态势感知必须包括适用于本地市场及其在南非运营的网络威胁情报。	8.2.1 识别潜在网络威胁。FMI应识别可能对其业务产生重大影响或在其生态系统内产生连锁效应的网络威胁，并定期审查和更新此类威胁的分析。 8.2.2 威胁情报管理流程。FMI需要建立收集和分析网络威胁情报的流程。 8.2.4 有效利用信息。FMI应确保使用网络威胁情报来实施网络韧性措施。FMI应基于网络威胁情报来制定风险缓解措施和培训计划的优先级。	客户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**

编号	控制域	G4/2017控制要求	金融市场基础设施网络韧性指南具体指标	华为云的应答
				安全白皮书》8.2漏洞管理。

9 华为云如何符合 FSCA“保险业外包管理”的要求

金融部门行为管理局（FSCA）于2012年4月发布了“159指令”，该指令是南非监管对保险公司（包括再保险公司）的外包管理的立法要求。

南非保险业在遵循“159指令”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“159指令”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，会如何帮助保险业客户满足这些控制要求。

9.1 内部审查和批准

“159指令”第7.5章要求保险业在计划外包时应考虑相关的外包风险，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
7.5	内部审查和批准	保险公司在决定外包前，应： 1）评估拟外包业务的成本收益及其潜在的固有风险； 2）评估保险公司的风险评估将如何被外包行为影响； 3）通过目标采购和选择程序确定潜在的服务提供商进行外包； 4）考虑首选服务提供商为多个保险公司提供多种外包服务所引起的潜在影响； 5）评估选定的服务提供商是否适合； 6）评估首选服务提供商的治理、风险管理及内控是否均符合适当的法律法规； 7）评估首选服务提供商的服务能力和财务状况； 8）对于拟外包的业务，制定一个合适的管理和监控流程； 9）制定适当的业务连续性计划，以确保在外包安排终止或无效的情况下，保险公司的保险业务能够持续运作。	客户应对其外包的业务以及首选服务提供商进行风险评估，识别潜在风险。 华为云可配合并积极响应客户 需求。此外，华为云内部也制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。

9.2 书面合同

“159指令”第7.6-7.7章要求保险业在计划外包时应考虑的合同协议内容，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
7.6 7.7	书面合同	保险公司应与其服务提供商签订书面合同，定义双方的权利、职责和期望，合同内容应至少包括： 1）说明供应商应当提供的服务水平协议及服务的标准； 2）要求服务提供商拥有适当的治理、风险管理和内控管理； 3）说明保险公司应可以监管服务提供商对于本合同的遵守情况； 4）说明保险公司可以可持续访问与外包流程、服务或活动相关的信息； 5）要求服务提供商遵守南非适用的法律法规，包括南非POPIA； 6）要求服务提供商对于保险公司和承保人的信息机密性、隐私性和安全性负责； 7）要求服务提供商提供应急流程。	客户应按照相关要求制定与云服务提供商的合同，并签订书面合同。 华为云制定了线下合同模板，可根据不同客户的需求进行定制化。华为云已识别并分析了POPIA法规要求，更多信息请详见**《华为云南非POPIA遵从性指南》**

9.3 管理和定期审查

“159指令”第7.9-7.11章要求保险业对外包相关的风险进行定期的审查，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
7.9 7.10 7.11	管理和定期审查	1、保险公司应确保外包服务提供商可以按照合同约定的服务水平和标准提供服务。 2、保险公司应定期评估服务提供商的治理、风险管理和内控管理，法规遵从情况及其服务能力和财务状况。	客户应确保服务提供商可按照合同和服务水平协议中的约定和标准提供云服务，并定期评估服务提供商的管理、合规及运营状况。 华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。同时，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。此外，华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由IM企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

9.4 涉及实质性职能和管理职能外包时的通知

“159指令”第8.1-8.2章要求保险业重要功能外包时应通知监管，相关控制要求及华为云的应答如下：

编号	控制域	具体控制要求	华为云的应答
8.1 8.2	涉及实质性职能和管理职能外包时的通知	1、保险公司如涉及管理职能、控制职能或实质性职能（含重要系统上云）的外包时，应将服务提供商的详细信息、外包相关的主要风险及风险缓解措施通知南非金融监管机构。 2. 在外包商出现任何重大事项，包括活动终止、重大的不履行事项，应及时通知南非金融监管机构。	客户如涉及将重要系统上云时，即为此条所管辖的范围（如公有云服务的中断，会对保险业客户的运营产生影响）。在将此类活动外包前，客户应将外包活动通知南非金融监管机构。 华为云将配合客户提供相关上报材料，配合客户满足监管通知的工作。

10 结语

本文描述了华为云如何为客户提供符合南非金融行业监管要求的云服务，并表明南非储备银行审慎监管局（PA）和金融部门行为管理局（FSCA）发布的重点监管要求，有助于客户详细了解华为云对于南非金融行业监管要求方面的合规性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合南非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南非金融行业监管要求的遵从性。

11 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