华为云肯尼亚金融行业监管要求遵从性指南

文档版本 1.0

发布日期 2023-02-09

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

随着技术的发展，对云计算技术及服务的使用已经成为肯尼亚金融机构的常态。云计算为金融机构的发展带来巨大的便利的同时，网络安全事件也随之出现。为规范金融行业对于信息科技的运用，肯尼亚中央银行（CBK）、保险监管局（IRA），针对肯尼亚金融机构的网络安全、信息技术风险管理等方面发布了一系列监管规定。

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。本文将针对肯尼亚金融机构在使用云服务时通常需遵循的监管要求，详细阐述华为云将如何协助其满足监管要求。

1.2 适用肯尼亚的金融监管要求简介

肯尼亚中央银行（CBK）负责监督银行、信贷机构和支付运营商；保险监管局（IRA）负责管理和监督保险业。肯尼亚中央银行和保险监管局颁布了相关规定对金融机构提出要求。

- **《风险管理指南》（RISK MANAGEMENT GUIDELINES）：** 2013年1月，肯尼亚中央银行为所有机构提供关于风险管理体系和框架的最低要求指导方针。该指南覆盖风险管理框架、战略风险管理、信用风险管理、流动性风险管理、市场风险管理、操作风险管理、信息与通信技术风险、合规风险等
- **《IRA风险管理和内部控制准则 IRA/PG/11》（IRA Guidelines on Risk Management and Internal Controls IRA/PG/11）：** 2013年6月，保险监管局要求保险公司具备有效的风险管理和内部控制制度，作为整体公司管理框架的一部分，包括有效的风险管理、合规、和内部审计等。
- **《CBK审慎外包指引CBK/PG/16》（CBK Prudential Guidelines on Outsourcing CBK/PG/16 (Outsourcing Guidelines) which is applicable to banks）：** 2013年1月，肯尼亚中央银行发布《审慎原则》，《审慎准则》中提供了金融机构必须实施的基本标准，其中包括《CBK审慎外包指引CBK/PG/16》。其第四部分具体要求约束了内部控制和谨慎标准、外包金融服务的风险管理实践、监管和监督要求、金融服务的离岸外包等相关的安全要求。
  - **《网络安全指导说明》（GUIDANCE NOTE ON CYBERSECURITY）：** 2017年8月，肯尼亚中央银行明确各机构在制定和实施旨在减轻网络风险的战略、政策、程序和相关活动时应遵循的最低要求，主要覆盖风险管理、外包、信息通信技术、内部控制和公司治理等领域。

- **《支付服务提供商网络安全指南》（CBK Guidelines on Cybersecurity for Payment Service Providers (PSP Guidelines)）**：2019年11月，肯尼亚中央银行设定了支付服务提供商（PSP）应采用的最低标准，以制定有效的网络安全治理和风险管理框架。

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

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

- 服务提供商

  指使用第三方（公司集团内的关联实体或公司集团外的实体）持续开展现在或将来通常由该机构自己承担的活动。

- 业务连续性

  指企业的持续和不间断的运作状态。

- 业务连续性管理

  一种全面的业务方法，包括政策、标准、框架和程序，以确保在发生中断的情况下能够及时维持或恢复具体业务。它的目的是最大限度地减少业务、财务、法律、声誉和其他由中断引起的实质性后果。

2 华为云安全合规

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

全球性标准类认证

认证	描述
ISO20000-1:2011	ISO20000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。
ISO27001:2013	ISO27001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。
ISO27017:2015	ISO27017是针对云计算信息安全的国际认证。ISO27017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。
ISO22301:2012	ISO22301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。华为云已获得SOC 1 Type II, SOC 2 Type II和SOC 3 鉴证审计报告三项权威认证，其中SOC 2 五大控制属性审计全部通过，为全球首家，表明华为云平台的信息安全管理能力已达到国际公认的最高标准，能够为您提供世界一流的安全隐私保障及服务。

认证	描述
PCI DSS认证	支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discover、万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
CSA STAR金牌认证	CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
国际通用准则CCEAL3+	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。
ISO27018:2014	ISO27018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。
ISO29151:2017	ISO29151是国际个人身份信息保护实践指南。ISO29151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。
ISO27701:2019	ISO27701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。
BS10012:2017	BS10012是BSI发布的个人信息数据管理体系标准，BS10012认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
M&O认证	Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。
NIST网络安全框架(CSF)	NIST CSF由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
PCI 3DS认证	PCI 3DS标准，旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS的评估对象为3D协议执行环境，包括访问控制服务器、目录服务器或3DS服务器功能；以及3D执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估3D协议执行环境的过程、流程、人员管理等。

地区性标准类认证

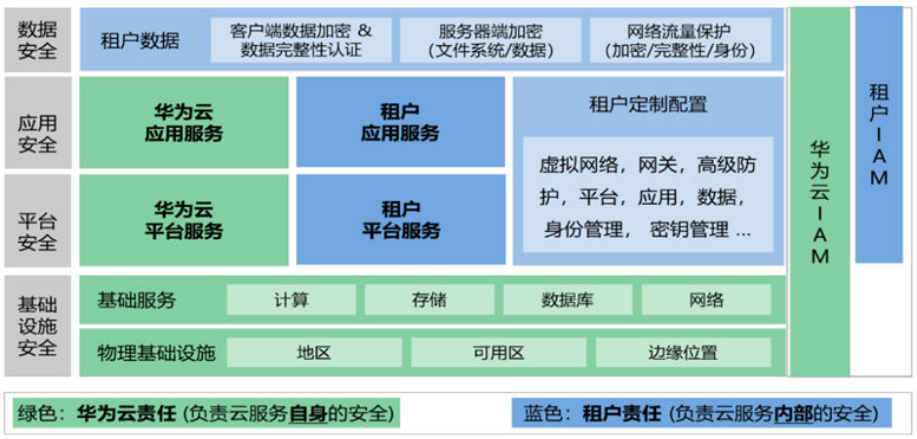
认证	描述
中国网络安全等级保护	网络安全等级保护是中华人民共和国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为中国各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡MTCS Level3 认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level3等级认证。
中国可信云金牌运维专项评估	金牌运维评估是面向已通过中国可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合中国权威云服务运营和维护保障要求的认证标准。
中国云服务用户数据保护能力认证	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。
中国工信部云计算服务能力评估	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关中国国家标准为依据的分级评估标准。
中国可信云评估	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。
中国网信办网络安全审查	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。

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

3 华为云安全责任共担

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

图 3-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（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遵从《 风险管理指南 》

肯尼亚中央银行在2013年1月发布了《 风险管理指南 》，该法规为所有机构提供关于风险管理体系和框架的最低要求指导方针。该指南覆盖风险管理框架、战略风险管理、信用风险管理、流动性风险管理、市场风险管理、操作风险管理、信息与通信技术风险、合规风险等。

金融机构在遵循上述规定时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与云服务供应商相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

5.1 政策和程序

编号	具体控制要求	客户关注点	华为云的内部实践
6.3.1关于外包的政策	董事会和高级管理层有责任了解与外包安排相关的运营风险，并确保制定有效的风险管理政策和实践，以管理外包活动的风险。 外包政策和风险管理活动应包括： (a) 确定活动是否可以外包和外包的程序。 (b) 在选择潜在服务供应商时进行尽职调查的程序。 (c) 外包安排的合理结构，包括数据的所有权和保密性，以及终止权。 (d) 管理和监测与外包安排相关风险的方案，包括服务提供商的财务状况。 (e) 在银行和服务提供商建立一个有效的控制环境。 (f) 制定可行的应急计划。 (g) 执行全面的合同和/或服务水平协议，明确外包商和银行之间的责任分配。	客户的高级管理层应制定外包风险管理政策，包括： (a)判断活动是否可外包，按照要求开展外包活动； (b) 选择服务供应商时进行尽职调查。 (c) 保证数据的所有权和保密性，以及终止权。 (d) 管理和监测与外包安排有关的风险的方案，包括服务提供商的财务状况。 (e) 与服务提供商之间具备一个稳定、安全的环境。 (f) 制定可行的应急计划；以及 (g) 执行全面的合同和/或服务水平协议，明确服务提供商和银行之间的责任分配。	华为云会安排专人积极配合金融机构的尽职调查。为了让用户享受安全可信的云平台和云服务，华为云按照全球各地权威的安全标准，从安全技术、安全制度、人员管理等各方面构建了完备的安全体系，并获得了国内外众多安全认证。华为在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。并贯穿在华为云招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。 华为云提供在线版本的**《 华为云服务等级协议 》**，明确了提供的服务的内容和级别，以及华为云的职责。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。华为云已获得ISO27001、ISO27017、ISO27018、SOC、CSASTAR等国际安全和隐私保护认证，并每年接受第三方审计。

5.2 衡量、监测和控制

编号	具体控制要求	客户关注点	华为云的内部实践
6.4.3控制与缓解	机构应该制定一个详细的业务连续性计划。必须确定恢复计划和业务恢复的优先次序，并对应急程序进行测试和实践，以便将严重运营风险事件引起的业务和运营中断降到最低。应定期评估恢复计划和事件响应程序，并在业务运营、系统和网络发生变化时进行更新。	客户应具备业务连续性计划，必须确定业务恢复的优先次序并进行应急演练。定期评估恢复计划和事件响应程序，并在业务运营、系统和网络发生变化时进行更新。	华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。
6.4.4 压力测试	机构应定期针对各种短期和长期的机构特定的运营风险压力情景进行压力测试，以确定潜在的运营风险来源，并确保机构在发生轻微和重大运营风险事件后做好继续经营的准备。机构应利用压力测试的结果来调整其操作风险管理战略、政策和立场，并制定有效的应急计划。	客户应定期进行压力测试，识别定位业务的脆弱环节，改进对风险状况的理解，监测风险的变动，并及时调整应急计划。	华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制

5.3 风险评估、测量和监测

编号	具体控制要求	客户关注点	华为云的内部实践
7.4.2 风险测量	机构应建立一套持续的风险衡量和监测机制。该机制应包括： 对ICT项目进行实施前和实施后的审查；定期对系统性能进行基准审查；有关ICT服务的事件和投诉报告；内部审计、外部审计的报告，以及CBK发现的问题报告；与供应商和业务部门的安排；定期审查服务水平协议（SLA）。 技术的新发展和新威胁对软件开发可能的影响。 及时审查业务领域的运营风险和管理控制。 定期评估信息技术外包项目的风险状况。	客户应建立风险管理和风险监控机制，审查ICT项目的实施工作、系统性能、有关ICT服务的事件和投诉报告、内部/外部审计的报告，以及CBK发现的问题、与供应商和业务部门的安排、服务水平协议（SLA）。定期评估信息技术外包项目的风险状况。	华为云开发并维护内部风险管理框架，识别、分析和管理已识别的风险。华为云至少每年进行一次正式风险评估，并制定了风险计算和分类的流程，以确定已识别风险的可能性和影响。每种风险相关的可能性和影响是独立确定的，应考虑每种风险类别。根据风险标准，将风险降低到可接受的水平包括解决时间，都应该由管理层制定、记录和批准。此外，华为云至少每月组织一次会议，讨论网络安全和隐私保护风险评估。华为云采取并记录相应的后续行动，以确保风险按照华为风险管理要求得到适当管理。 华为云制定了全面的物理安全和环境安全防护措施、策略和程序，运维团队定期对全球数据中心进行风险评估，确保数据中心执行严格的访问控制、安全措施、日常监控审计、应急响应等措施。此外，华为PSIRT和华为云的安全运维团队已经建立了成熟而全面的漏洞检测、识别、响应和披露计划和框架。华为云依靠该计划和框架来管理漏洞，确保无论是由华为技术还是第三方技术中发现的华为云基础设施和云服务、运维工具中的漏洞，都能在SLA内处理和解决。华为云致力于降低并最终避免漏

编号	具体控制要求	客户关注点	华为云的内部实践
			洞被利用对客户造成的业务影响。
7.8 审计跟踪	机构应制定一套政策和程序来控制所有生产系统中的活动记录，以支持有效的审计、安全取证分析和欺诈预防。日志记录可以在不同层次的软件和不同的计算机及网络设备上实现，这分为两大类。 1）事务日志是由程序软件和数据库管理系统生成的，它包含认证尝试、对数据和错误信息的修改。交易日志应根据该国家法律规定的信息保留政策进行保存。 2）系统日志由操作系统、数据库管理系统、防火墙、入侵检测系统和路由器等产生，包含认证尝试、系统事件、网络事件和错误信息。	客户可通过华为云统一身份认证服务可以更有效地细化管理特权账户。客户也可通过**云审计服务（Cloud TraceService，简称CTS）**作为辅助，CTS为客户提供云服务资源的操作记录，供用户查询、审计和回溯使用。	为配合客户满足合规要求，华为云相关系统的管理员登录系统时必须先经过双因子认证后，才能通过跳板机接入管理平面。所有操作都会记录日志并及时传送到集中日志审计系统。该审计系统有强大的数据保存及查询能力，确保所有日志保存时间超过180天，90天内可以实时查询。而且华为云有专门的内审部门，会定期对运维流程各项活动进行审计。

编号	具体控制要求	客户关注点	华为云的内部实践
7.9 加密技术	机构应具备采用加密技术的能力，以减少在信息和通信系统中或其传输过程中丢失机密信息的风险。应建立适当的加密设施管理程序，以确保使用中的加密设施应符合国际安全标准或要求。 负责加密设施管理的工作人员经过良好的培训和审查。这要通过专业和学术证明、独立推荐人的品行证明、良好行为证明来验证。 加密强度足以保护信息的保密性。有效和高效的密钥管理程序，特别是密钥的生命周期管理和证书的生命周期管理。	为配合客户满足保证数据机密性的要求，华为云提供服务端加密功能集成了**数据加密服务（Data Encryption Workshop，简称DEW）**的密钥管理功能，由DEW进行密钥全生命周期集中管理。DEW是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块（HSM）保护，并与许多华为云服务集成。用户也可以借此服务开发自己的加密应用。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，从而助力客户云上数据的安全。	华为云遵从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、可持续的数据安全保障体系。华为云为保护租户数据的存储安全采取了一系列的保护机制。 华为云建立了保护技术设备上的数据的加密策略与密钥管理机制，对加密级别、加密方法进行了规定。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： 1. 虚拟专用网络（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。目前，华为云采用硬 件实现的IKE（密钥交换协议）和IPSecVPN结合的方 法对数据传输通道进行加密。 2. 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。 以上数据传输方式均支持使用传输层安全协议TLS1.2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。 此外，华为云运维人员心对接客户VPC环境时，采用 安全传输协议HTTPS，以防止数据

编号	具体控制要求	客户关注点	华为云的内部实践
			在传输过程中发生泄露。
7.15 业务连续性管理	机构应根据其业务的性质、规模和复杂性做出适当的安排，以确保在信息和通信技术发生意外中断的情况下，能够继续运作并履行其监管义务。这些安排应定期更新和测试，以确保其有效性。	客户应制定业务连续性管理计划，并定期更新确保业务连续性管理的有效性。	华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。

编号	具体控制要求	客户关注点	华为云的内部实践
7.16 外包	1 ）风险分析 在订立对外包协议进行重大变更之前，机构应： 分析该安排将如何符合其信息和通信技术组织和报告结构；业务战略；整体风险状况；以及履行其监管义务的能力。 考虑这些安排是否允许其监测和控制与外包相关的运营风险。 对服务提供商的财务稳定性、专业知识和风险评估、设施和潜在的负债偿付能力进行适当的尽职调查。 考虑如何确保其业务从目前的协议安排顺利过渡到新的或变更后的外包协议（ 包括合同终止时的情况 ）；以及 考虑任何集中风险的影响，例如，如果几家公司都使用同一个服务提供商，可能产生的业务连续性的影响。 2 ）数据安全 机构应通过加强对与信息和通信技术相关的外包服务提供商的管理，采取措施，确保客户信息等敏感信息的数据安全，这些措施包括： 确保外包信息与服务提供商处理的其他信息之间有明确的区分。 服务提供商的员工应在 "需要知道 "和 "最低限度授权 "的基础上进行授权。 确保服务提供商保证其工作人员达到所要求的保密门槛。 确保在终止外包安排时，将所有相关的敏感信息从服务提供商的存储中删除。 3 ）应急计划 机构应确保其拥有适当的应急计划，以应对服务提供商服务的重大风险造成的损失。需要考虑的具体问题包括资源的重大损失、关键员工的更替、或服务提供商的财务危机，以及外包协议的意外终止。	客户应在使用外包服务之前进行风险分析、尽职调查；设置访问控制规则，保护用户敏感信息数据安全；具备应急计划、应急处置流程。	华为云会安排专人积极配合金融机构的尽职调查。为了让用户享受安全可信的云平台和云服务，华为云按照全球各地权威的安全标准，从安全技术、安全制度、人员管理等各方面构建了完备的安全体系，并获得了国内外众多安全认证。华为在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。并贯穿在华为云招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。 华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证与访问控制、权限管理、数据隔离、传输安全、存储安全、数据删除、物理销毁、数据备份恢复等方面，采用优秀技术、实践和流程，保证用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。更多详细信息请参见**《 华为云数据安全白皮书 》**第4部分。 华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务

编号	具体控制要求	客户关注点	华为云的内部实践
			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。

6 华为云如何遵从及协助客户遵从《 IRA 风险管理和内部控制准则 》

保险监管局在2013年6月发布了《 IRA风险管理和内部控制准则 》，该法规要求保险公司拥有有效的风险管理和内部控制制度，作为整体公司管理框架的一部分，包括有效的风险管理、合规、和内部审计等。

金融机构在遵循上述规定时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与云服务供应商相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

6.1 风险管理制度

编号	具体控制要求	客户关注点	华为云的内部实践
6.0 风险管理制度	6.2.6 识别、评估、监测、管理和报告风险的适当程序和工具（包括适当的模型）。此类流程也应涵盖应急计划、业务连续性和危机管理等领域。 6.10 应当要求保险公司记录风险管理系统的重大变更，并经董事会批准。变更的原因应记录在案，并提供给内部审计、外部审计和管理局，供其各自对风险管理系统进行评估。	客户应要求服务提供商应具备SLA，制定应急计划、业务连续性计划，保证业务的可用性。	华为云提供在线版本的**《 华为云服务等级协议 》**，明确了提供的服务的内容和级别，以及华为云的职责。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。华为云已获得ISO27001、ISO27017、ISO27018、SOC、CSASTAR等国际安全和隐私保护认证，并每年接受第三方审计。 华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。

6.2 风险缓解和控制

编号	具体控制要求	客户关注点	华为云的内部实践
7.0 风险缓解和控制	7.6 在设计有效的内部控制体系时，保险公司应至少考虑以下内容： 7.6.2 对其他关键业务流程和政策的适当控制，包括对重大业务决策和交易（包括集团内部交易）、关键的信息技术功能、雇员对数据库和信息技术系统的访问，以及重要的法律和监管义务。 7.6.3 必要时进行适当的职责分离，并进行控制以确保这种分离得到遵守。 7.6.4 明确界定的管理职责和责任制度，包括批准、设定限制和授权的文件。 7.6.7 定期检查所有控制措施的整体是否形成一个连贯的系统，以及该系统是否按预期运行的程序。 7.6.8 定期测试和评估（由内部或外部审计师等客观各方进行），以确定内部控制体系的充分性、完整性和有效性，以及其对董事会和管理层控制保险公司业务的效用。	客户应要求服务提供商具备严格的访问控制措施，防止未授权访问，定期检查系统架构、监控体系、压测机制等保证业务稳定性。	华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。 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。华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。 根据ISO27001标准，华为云构建了完善的信息安全管理体系，制定了华为云的整体信息安全战略，明确了信息安全管理机构的结构和职责、信息安全系统文件的管理方法、关键方向和目标，包括资产安全、访问控制、密码学、物理安全、运营安全、通信安全、系统开发安全、供应商管理、

编号	具体控制要求	客户关注点	华为云的内部实践
			信息安全事件管理和业务连续性。华为云全力保护客户系统和数据的不可侵犯性、完整性和可用性。此外，华为云专注于培养员工和外包人员的安全意识，并制定了适用的安全意识培训计划，定期进行培训。

7 华为云如何遵从及协助客户遵从《 CBK 审慎外包指引 CBK PG 16 》

肯尼亚中央银行在2013年1月发布了《 审慎原则 》，提供了金融机构必须实施的基本标准，其中包括《 CBK审慎外包指引CBK/PG/16 》。其第四部分具体要求约束了内部控制和谨慎标准、外包金融服务的风险管理实践、监管和监督要求、金融服务的离岸外包 等相关的安全要求。

金融机构在遵循上述规定时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与云服务供应商相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

编号	具体控制要求	客户关注点	华为云的内部实践
4.5.6 外包协议	4.5.6.1 外包安排应受明确的书面合同管辖，合同的性质和细节应与外包活动对受监管实体的持续业务的重要性相适应。 4.5.6.6 协议还应该指出各方之间法律关系的性质（如代理人、委托人或其他），合同的关键条款应当包括： b) 机构必须确保其可以获得与服务提供商的外包活动有关的所有文档、记录和信息。 c) 合同应规定机构对服务提供商进行持续监测和评估，以便立即采取任何必要的纠正措施。 e) 确保客户数据保密性的控制措施并确保服务提供商在违反安全规定和泄露客户相关机密信息时应当承担责任。 f) 确保业务连续性的应急计划。 g) 合同应规定，机构是否批准服务提供商在全部或部分外包活动中使用分包商。 h) 规定机构有权对服务提供商进行审计，无论是由其内部或外部审计员，还是由指定外部代表其行事的代理机构进行审计，且机构有权获得与为机构提供的服务有关的任何审计或审查报告或调查结果的副本。 i) 允许中央银行或其授权的人员在合理的时间内查阅该机构的文件、交易记录以及由服务提供商提供、储存或处理的其他必要信息的条款。 j) 制定条款，承认中央银行有权安排其一名或多名官员或雇员或其他人员对	客户与服务提供商所签订的用户协议中应包含： a关于外包活动有关的所有文档、记录和信息应提供给金融机构； b客户数据泄露，服务商应承担响应责任； c金融机构可以对服务商进行审计； d允许CBK查阅服务商提供、存储或处理的必要信息； e认同CBK安排人员对服务商及其在服务商注册的账户进行检查。	华为云会安排专人积极配合金融机构的尽职调查。为了让用户享受安全可信的云平台和云服务，华为云按照全球各地权威的安全标准，从安全技术、安全制度、人员管理等各方面构建了完备的安全体系，并获得了国内外众多安全认证。华为在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。并贯穿在华为云招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。 华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证与访问控制、权限管理、数据隔离、传输安全、存储安全、数据删除、物理销毁、数据备份恢复等方面，采用优秀技术、实践和流程，保证用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。更多详细信息请参见**《华为云数据安全白皮书》**第4部分。 华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。

编号	具体控制要求	客户关注点	华为云的内部实践
	银行的服务提供商及其账簿和账户进行检查。		
4.5.7 保密性和安全性	机构必须确保服务提供商的安全政策、程序和控制措施将使机构能够保护客户信息的保密性和安全性。机构应至少采取以下步骤，以确保客户的保密性问题得到解决。 a) 服务提供商的员工对用户信息的访问应限于为履行外包职能所需的信息领域。 b) 机构应确保服务提供商能够隔离并明确识别机构的客户信息、文件、记录和资产，以保护信息的保密性。 c) 机构应定期审查和监测服务提供商的安全实践和控制程序，并要求服务提供商披露安全漏洞。	客户应设置访问控制机制，服务提供商的员工仅能访问职能内的用户信息。 服务提供商应能够隔离机构的信息文件、记录和其他资产以保护信息的保密性。服务提供商应配合机构进行定期审查和检查服务的安全性，及时向用户披露安全漏洞。	华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证与访问控制、权限管理、数据隔离、传输安全、存储安全、数据删除、物理销毁、数据备份恢复等方面，采用优秀技术、实践和流程，保证用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。更多详细信息请参见**《华为云数据安全白皮书》**第4部分。

编号	具体控制要求	客户关注点	华为云的内部实践
4.5.8 业务连续性管理	机构应采取措施，评估并确保外包安排产生的相互依赖风险可以得到充分缓解，从而使机构在业务中断、外包意外终止或服务提供商清算的情况下，仍能以诚信和能力开展其业务。 a ）机构要求其服务供应商开发和建立一个强有力的框架，以记录、维护和测试业务连续性和恢复程序。机构需要确保服务提供商定期测试业务连续性和恢复计划，也可以考虑不定期地与其服务提供商进行联合测试和恢复演习。 d) 外包通常需要共享服务提供商的基础设施。机构应确保服务提供商能够隔离机构的信息、文件和记录以及其他资产。这是为了确保在不利的条件下，所有的文件、交易记录和给服务提供商的信息以及机构的资产，都能从服务提供商处移除，以继续其业务运作，或者删除、销毁或使其无法使用。	客户应要求服务提供商应制定BCP，并不定期的开展应急演练。 客户应该确保服务提供商能够隔离机构的信息文件、记录和其他资产；确保提交给服务提供商的文档、记录都可以从服务提供商收回，删除销毁、无法使用以便于机构业务继续运营。	华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。

编号	具体控制要求	客户关注点	华为云的内部实践
4.5.9 外包活动的监测和控制	4.5.9.1 机构应建立一个管理结构，以监测和控制其外包活动 4.5.9.2 随着外包关系和相互依存关系的重要性和复杂性增加，应采取更严格的风险管理方法。 4.5.9.4 机构应确保与服务提供商签订的外包协议包含解决其对外包活动的监督和控制的条款。 4.5.9.5 对材料外包进行有效监测和控制的结构将包括以下内容： c) 机构应至少每年一次审查服务提供商的财务和运营状况，以评估其继续提供外包服务的能力。这种尽职调查可以基于关于服务提供商的所有可用信息，应突出关注是否违反绩效标准、保密性和安全性以及业务连续性准备等方面。	客户应建立外包管理程序，对外包活动进行风险管理，应确保与服务提供商签订的外包协议包含解决其对外包活动的监督和控制的条款，至少每年对服务提供商进行一次尽职调查。	华为云提供在线版本的**《华为云服务等级协议》**，明确了提供的服务的内容和级别，以及华为云的职责。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。华为云已获得ISO27001、ISO27017、ISO27018、SOC、CSASTAR等国际安全和隐私保护认证，并每年接受第三方审计。 华为云会安排专人积极配合金融机构的尽职调查。为了让用户享受安全可信的云平台和云服务，华为云按照全球各地权威的安全标准，从安全技术、安全制度、人员管理等各方面构建了完备的安全体系，并获得了国内外众多安全认证。

8 华为云如何遵从及协助客户遵从《 网络安全指导说明 》

肯尼亚中央银行在2017年8月发布了《 网络安全指导说明 》，明确各机构在制定和实施旨在减轻网络风险的战略、政策、程序和相关活动时应遵循的最低要求，主要覆盖风险管理、外包、信息通信技术、内部控制和公司治理等领域。

金融机构在遵循上述规定时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与云服务供应商相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

编号	具体控制要求	客户关注点	华为云的内部实践
3.3外包	对外包协议进行适当的管理，包括对潜在的服务供应商进行尽职调查，签署书面外包协议并对服务的提供进行适当的监督。 根据合规性和风险评估来选择供应商。 确保所有计算资源的安全，包括注册、许可、合规和核验。 确保所有外包合同要求服务供应商遵守适用的法律和监管框架。 了解每个第三方产生的固有风险。 对机构的外包组合进行分析，以了解哪些对机构构成最大的相对风险。	客户应对服务提供商进行尽职调查，对外包服务进行适当监管，确保服务提供商符合合规要求。确保服务提供商使用的计算资源的安全性（如：软硬件为正版）；确保外包合同中明确服务提供商遵守当地法规以及满足监管要求。	为配合客户行使对云服务供应商的监管，华为云线上的**《华为云用户协议》**对客户和华为的安全职责进行划分，**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中与客户共同约定相应要求。更多详细信息请参见**《华为云用户协议》**。 华为云提供在线版本的**《华为云服务等级协议》**，明确了提供的服务的内容和级别，以及华为云的职责。华为云会安排专人积极配合金融机构的尽职调查。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。华为云已获得ISO27001、ISO27017、ISO27018、SOC、CSASTAR等国际安全和隐私保护认证，并每年接受第三方审计。

编号	具体控制要求	客户关注点	华为云的内部实践
4.0报告	b)各机构应在发生任何网络安全事件后24小时内通知肯尼亚中央银行，这些事件可能对该机构向其客户提供适当服务的能力、其声誉或财务状况产生重大和不利影响。	如金融机构发生网络安全事件，其服务能力、财务状况、声誉等产生了重大不利影响，金融机构应在24h内向肯尼亚中央银行报告。	华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。 为配合客户满足网络安全事件上报的要求，华为云设置7*24h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。

9 华为云如何遵从及协助客户遵从《 支付服务提供商网络安全指南 》

肯尼亚中央银行在2019年11月发布了《 支付服务提供商网络安全指南 》，设定了支付服务提供商（ PSP ）应采用的最低标准，以制定有效的网络安全治理和风险管理框架。

金融机构在遵循上述规定时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与云服务供应商相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

编号	具体控制要求	客户关注点	华为云的内部实践
3.2.4 事件响应和网络恢复能力	(ii) PSP应计划、应对、控制并能够从网络事件造成的破坏中迅速恢复，从而加强其网络复原力。因此，PSP应该有能力在面对攻击时操作关键业务功能，同时不断加强网络复原力。应涉及以下方面： a) 应对网络安全事件的内部流程。 b) 事件响应计划的目标。 c) 明确的角色、责任和决策权级别的定义。 d) 外部和内部沟通和信息共享。 e) 确定对信息系统和相关控制中任何已确定的弱点进行补救的要求。 f) 记录和报告有关网络安全事件和相关的事件响应活动；以及 g) 在发生网络安全事件后，对事件响应计划进行必要的评估和修订。	PSP应具备应急响应预案，提高信息安全事件的应急响应与处理能力，增强对突发事件的应变能力。预案中应具备：网络安全事件处理流程、响应计划、人员角色、责任等相关说明。	华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案。同时，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。 华为云每年对信息安全事件管理程序和流程进行培训和测试，所有的安全事件响应人员，包括后备人员均需参与。

编号	具体控制要求	客户关注点	华为云的内部实践
3.2.5 漏洞评估和渗透测试	每个PSP的网络安全计划应包括监测和测试，根据PSP的风险评估制定，旨在评估PSP的网络安全计划的有效性。监测和测试应包括持续监测和定期渗透测试和漏洞评估。在没有有效的持续监测，或其他系统持续检测信息系统中可能产生或显示漏洞的变化，PSP的应进行。 (i) 每季度对所有关键网络资产进行漏洞扫描。 (ii) PSP的年度渗透测试，至少涵盖每年根据风险评估确定的关键网络资产 (iii) 半年度脆弱性评估，包括对信息系统进行任何系统扫描或审查，合理设计，以根据风险评估确定PSP信息系统中公开已知的网络安全漏洞。	PSP应对业务系统进行持续监控，并定期进行渗透测试和漏洞扫描。 1. 每季度对重要业务系统/资产进行漏扫。 2. 每年度对重要业务系统/资产进行渗透测试。 3. 每半年对信息系统进行漏洞评估，包括主机扫描、WEB扫描等。	华为云建立了渗透测试与漏洞扫描管理规定，明确了华为云平台开展渗透测试的目的、频率以及应遵循的安全要求，规范渗透测试行为，确保渗透测试活动合规与受控。 华为云每半年都会组织内部以及外部具有一定资质的第三方进行对华为云平台范围内的所有的系统及应用进行渗透测试，并对渗透测试的结果进行跟进与整改，渗透测试报告及跟进情况会通过内部审计以及外部认证机构核查。

编号	具体控制要求	客户关注点	华为云的内部实践
3.4 外包	(i) 建立适当的外包协议管理框架，包括对潜在的服务供应商进行尽职调查，签署书面外包协议，并对服务交付进行充分监测。 (iv) 确保所有外包合同要求服务供应商遵守适用的法律和监管框架。 (vii) 强制要求其外包商在符合最佳实践的特定时间框架内报告安全事件/违规行为。通常以48小时为限。 (viii) 确保外包服务或基础设施至少符合PSP的非外包服务和基础设施相同的最低安全标准。 (ix) 确保服务水平协议充分包含安全性、服务可用性、性能指标和处罚等方面的规定。	允许银监会或其授权的人员在合理的时间内查阅机构的文件、交易记录以及由服务提供商提供、存储或处理的其他必要信息的条款	华为云会安排专人积极配合金融机构的尽职调查。为了让用户享受安全可信的云平台和云服务，华为云按照全球各地权威的安全标准，从安全技术、安全制度、人员管理等各方面构建了完备的安全体系，并获得了国内外众多安全认证。华为在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。并贯穿在华为云招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。 华为云作为云服务供应商，为金融机构客户提供其业务所依赖的云服务，因此除不可抗因素导致的外包中断或意外终止的情况外，华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 为配合客户行使对云服务供应商的监管，华为云线上的**《华为云用户协议》**对客户和华为的安全职责进行划分，的**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中与客户共同约定相应要求。更多详细信息请参见**《华为云用户协议》**。

10 结语

本文描述了华为云如何为客户提供遵从肯尼亚金融行业监管要求的云服务，并表明华为云遵守肯尼亚中央银行发布的重点监管要求，有助于客户详细了解华为云对肯尼亚金融行业监管要求方面的遵从性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署遵从肯尼亚金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

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

11 历史版本

日期	版本	描述
2023年2月	1.0	首次发布