华为云印度尼西亚金融行业监管要求遵从性指南

文档版本 1.0

发布日期 2023-02-08

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
1.1 背景与发布目的.....1
1.2 适用的印度尼西亚的金融监管要求简介.....1
1.3 名词定义.....2
2 华为云安全合规.....3
3 华为云安全责任共担.....6
4 华为云全球基础设施.....7
5 华为云如何遵从及协助客户满足《No.38_POJK.03_2016 关于商业银行在使用信息技术时实施风险管理的规定》及其修正案.....8
5.1 信息技术实施的风险管理.....9
5.2 由银行或信息技术服务商提供的信息技术实施.....13
5.3 报告.....18
6 华为云如何遵从及协助客户满足《No.21/SEOJK.03/2017 关于商业银行在使用信息技术时实施风险管理的通知》.....19
6.1 信息技术管理.....19
6.2 信息技术开发和采购.....20
6.3 信息技术运营管理.....27
6.4 信息技术运营管理.....29
6.5 信息安全.....33
6.6 灾难恢复计划.....43
6.7 信息技术供应商管理.....45
7 华为云如何遵从及协助客户满足《No.4_POJK.05_2021 关于非银行金融机构在使用信息技术时实施风险管理的规定》.....47
7.1 识别、测量、控制和监控信息技术风险的充分性.....48
7.2 信息技术使用的内部控制制度.....52
7.3 非银行金融机构或信息技术服务商实施信息技术.....53
7.4 消费者个人数据的安全.....59
7.5 报告.....60
8 结语.....61
9 历史版本.....62

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印度尼西亚金融机构的常态。云计算为金融机构的发展带来巨大的便利的同时，也为金融机构创造了更为复杂的业务运营环境。为规范金融行业对于信息科技的运用，印度尼西亚金融服务管理局（OJK）针对印度尼西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。本文将针对印度尼西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 适用的印度尼西亚的金融监管要求简介

印度尼西亚金融服务管理局是印度尼西亚金融服务监管机构，负责监督和管理金融机构、非银行金融机构的信息科技风险管理，并颁布了相关规定来规范这一领域。

- **《No.21/SEOJK.03/2017 关于商业银行在使用信息技术时实施风险管理的规定》(Implementation of Risk Management in the use of Information Technology by Commercial Banks)**：2017年6月6日，印尼金融服务管理局发布了该规定，对商业银行实施IT技术提出的风险管理要求，涉及多个IT领域的要求，如业务连续性，数据安全、信息安全、供应商要求等。
- **《No.38/POJK.03/2016关于商业银行在使用信息技术时实施风险管理的规定》(Implementation of Risk Management in the use of Information Technology by Commercial Banks)**：2016年12月14日，印尼金融服务管理局发布了该规定，对商业银行实施IT技术提出的风险管理要求，涉及多个IT领域的要求，如业务连续性，数据安全、信息安全、供应商要求等。
  - **《关于对No.38/POJK.03/2016的修正案》(Implementation of Risk Management in the use of Information Technology by Commercial Banks)**：2020年6月18日，印尼金融服务管理局发布了该规定，对No.38/POJK.03/2016在数据中心和灾难恢复中心、公司机密信息、信息科技风险评估等领域的要求进行修订，提出进一步的要求。
  - **《No.4/POJK.05/2021关于非银行金融机构在使用信息技术时实施风险管理的规定》(Implementation of Risk Management in the Use of**

Information Technology by Nonbank Financial Services Institutions)：2021年3月9日，印尼金融服务管理局发布了该规定，对非银行金融机构实施IT技术提出的风险管理要求，涉及多个IT领域的要求，如信息安全、业务连续性、数据安全、境内交易处理、供应商管理等要

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

  根据外包安排向金融机构提供服务的实体以及实体的分支机构。

- 灾难恢复计划

  金融机构业务活动中无法避免自然界或人类造成的中断或损害，如地震、火灾、洪水、电力故障、技术故障、人为疏忽等。发生的中断或损害不仅影响到金融机构的技术能力，还会影响到银行的业务运行，尤其是对客户的服务。因此金融机构必须建立灾难恢复计划，以确保业务在中断或灾难发生时仍能继续运作，以保护利益相关者的利益，重点是数据恢复计划、关键应用系统和IT基础设施的运行。

- 内部审计

  有效的内部控制系统是金融机构管理的一个重要组成部分，可以协助金融机构管理层保护资产，确保提供可靠的财务和管理报告，并减少损失、违规和违反审慎方面的风险。IT内部审计作为内部控制系统的一部分，需要独立、客观地评估IT的实施情况，以提高风险管理、内部控制和良好治理的效率和效果，包括对数据中心、灾难恢复、应用程序等审计。

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。
PCI DSS认证	支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discover、万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。

认证	描述
CSA STAR金牌认证	CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
国际通用准则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

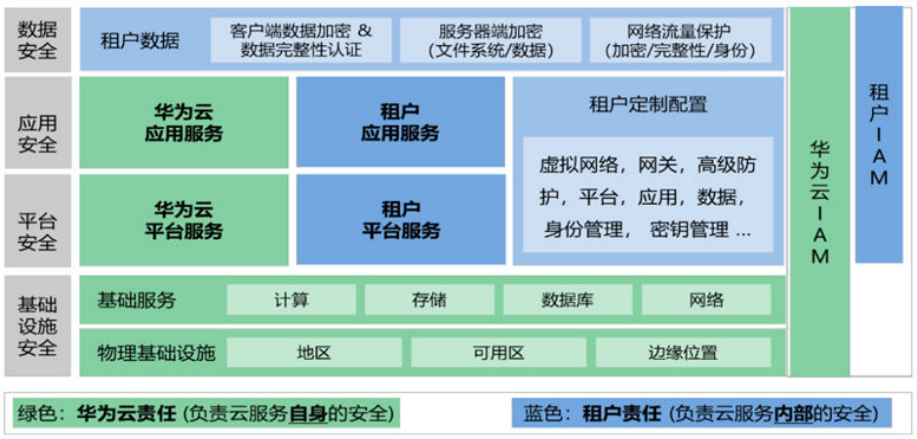
认证	描述
中国网络安全等级保护	网络安全等级保护是中华人民共和国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为中国各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡MTCS Level3 认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level3等级认证。
中国可信云金牌运维专项评估	金牌运维评估是面向已通过中国可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”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。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。
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满足《 No.38_POJK.03_2016 关于商业银行在使用信息技术时实施风险管理的规定 》及其修正案

印尼金融服务管理局在2016年12月14日发布了《 No.38_POJK.03_2016 》，该规定对于金融机构的信息科技风险管理提出了多个方面的要求，如业务连续性，数据安全、信息安全、供应商管理等。

基于对信息技术利用效率和风险管理等要求，印尼金融服务管理局在2020年6月18日发布了《 关于对No.38_POJK.03_2016的修正案 》，该修正案对《 No.38_POJK.03_2016 》有关数据中心和灾难恢复中心的规定进行了修订。

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 信息技术实施的风险管理

编号	具体控制要求	客户关注点	华为云的内部实践
第8条	(1) 银行必须拥有第2条第(2)款b项中提到的信息技术政策、标准和程序 (2) 信息技术的政策、标准和程序至少包括以下方面： a. 管理 b. 开发和采购 c. 业务信息技术 d. 通信网络 e. 信息安全 f. 灾难恢复计划 g. 电子银行业务， h. 信息技术服务提供商，以及， i. 向银行提供信息技术服务 （3）银行必须确定可容忍的风险限度，以确保第2节（2）款中提到的与信息技术有关的方面将以最佳方式运行。	客户应制定网络安全政策和程序，并获得组织负责人或代表的批准，分发给组织的内外部相关组织。	华为云作为云服务提供商，确保各项云技术的安全开发、配置和部署以及所提供云服务的运维运营安全。华为云参照ISO27001、ISO27017、ISO27018、SOC、CSASTAR的要求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，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。 在业务流程方面，安全保障活动融入研发、供应链、市场与销售、工程交付及技 术服务等各主业务流程中。安全作为质量管理体系的基本要求，通过管理制度和技术规范来确保其有效实施。华为通过内部审计和接受各国政府安全部门、第三方独立机构的安全认证和审计等来监督和改进各项业务流程。2004年起，华为的安全管理体系通过了BS7799-2/ ISO27001 认证。华为云在公司级的业务流程基础上，大胆地将已在华为全面采用的安全周期管理（SDL – Security Development Lifecycle）集成于当前适合云服务的 DevOps 工程流程和技术能力，形成有华为特色的DevSecOps 方法论和工具链，既支撑云业务的敏捷上线，又确保研发部署的全线安全质量。

编号	具体控制要求	客户关注点	华为云的内部实践
第11条	在开发和获取信息技术的过程中，银行必须采取控制措施，生成保密和集成的系统和数据，以支持实现银行目标，包括： a. 建立和实施一致的信息技术开发和采购的程序和方法； b. 在系统开发中实施项目管理； c. 在系统的开发和采购的过程中进行充分的测试，包括与用户工作部门进行的联合测试，以确保系统和用户要求的准确性和一致性，以及一个系统与另一个系统的兼容性； d. 采用适当的文件记录系统的开发及其维护； e. 进行应用系统变更管理； f.确保银行的信息技术系统能够完整地显示信息；	客户应明确应用网络安全的标准，在应用安全开发的生命周期中实施安全标准。 客户应确保其应用开发流程遵循安全系统开发生命周期的方法。	● 项目管理框架 华为云制定了完整的项目管理方法，实施基于CCM5/CMMI、ISO 9001:2000和PMI框架的实践，使合格的项目管理专业人员在全球成功实施项目。 ● 系统开发生命周期和设计安全 华为云追求新的DevOps流程，具有快速持续迭代能力，集成了华为安全开发生命周期(SDL)。此外，逐步形成高度自动化的新安全生命周期管理方法和流程，称为DevSecOps，与云安全工程能力和工具链一起确保DevSecOps的顺利灵活实施。华为云对开发环境进行分层管理，并实施物理隔离、逻辑隔离、访问控制、数据传输通道审批和审计等保护措施。 为满足客户合规要求，华为云严格遵守华为发布的安全编码规范。此外，我们还引入了静态代码扫描工具的每日检查，生成的数据将输入云服务持续集成/持续部署（ CI/CD ）工具链，通过使用质量阈值进行控制和云服务产品质量评估。源代码在编译前由变更经理审查和批准。开发人员无法批准和编译代码。在任何云产品或云服务发布前，必须完成静态代码扫描告警清除，有效减少因代码延长上线时间的相关问题。所有云服务在发布前都通过了多次安全测试。测试环境与生产环境隔离，避免使用生产数据或敏感生产数据进

编号	具体控制要求	客户关注点	华为云的内部实践
			行测试，并在使用后需要清除。
第15条	(1) 银行必须设置灾难恢复计划。 (2) 银行必须确保第(1)款所述的灾难恢复计划能够有效实施，以便在银行使用的信息技术设施发生灾难和/或中断时，银行的业务连续性能够继续运行。 (3) 银行有义务根据业务影响分析的结果，在一年内至少对所有重要的应用程序和基础设施进行一次灾难恢复计划的测试，并让信息技术用户参与其中。 (4) 银行有义务在1年内对灾难恢复计划进行至少1次的审查。	金融机构应建立自身的业务连续性机制，并制定保证其关键业务的RTO、RPO指标。 客户可以依赖华为云数据中心集群的区域和可用区架构，实现业务系统的容灾和备份。按规则在全球部署数据中心。	华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。 华为云根据内部业务连续性管理体系的要求，制定了完善的恢复策略，以支撑云服务持续运营的关键业务。 客户通过两个地方拥有灾难数据备份中心。如果发生故障，系统会自动从受影响区域传输客户应用程序和数据，在满足合规策略的前提下，确保业务连续性。华为云还部署了全球服务器负载均衡中心。客户应用可以在数据中心实现N+1部署。即使一个数据中心发生故障，它也可以将流量负载均衡到其他中心。

编号	具体控制要求	客户关注点	华为云的内部实践
第19条	(1) 银行必须有针对银行自身或信息技术服务供应商信息技术使用的内部审计准则。 (4) 银行必须向金融服务管理局提交： a. 第(3)款中提到的审查结果附有改进建议，并作为审查报告一部分；以及 b. 按照有关执行内部审计职能的标准的规定，信息技术的内部审计结果作为执行报告和内部审计要点的一部分。	客户应接受独立的网络安全审计，以确定符合公认的审计标准和网络安全框架。 客户的网络安全审计应根据其组织内部的审计手册和审计计划进行。	华为内部审计团队直接向董事会和公司高层管理者汇报，严格的审计活动在推动网络安全流程和标准落地，保障结果交付上起着关键的作用。 华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。审计团队每年投入10+人力对全球范围运营的华为云至少开展1次，为期2个月的审计，重点关注华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上的风险。 审计结果向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。

5.2 由银行或信息技术服务商提供的信息技术实施

编号	具体控制要求	客户关注点	华为云的内部实践
第20条	(1) 银行应组织实施信息技术。 (2) 第(1)款所指的信息技术的实施可由银行本身和/或信息技术服务提供商进行。 (3) 如果银行的信息技术的实施是由第(2)款所指的信息技术服务提供商进行的，银行应： f. 定期监测和评估信息技术服务提供商的业绩、声誉和提供服务的连续性。 g. 在需要时向内部审计员、外部审计员和金融服务管理局提供获取数据和信息的途径。 h. 及时向金融服务管理局提供对数据库的访问，包括对当前数据和过去数据的访问；以及 i. 确保信息技术服务提供商： 1.根据组织信息技术的需要，拥有在学术上和/或专业证书支持的可靠性的专家。 2.充分执行信息技术控制原则，由独立方进行的审计结果证明。 3.向银行的内部审计员、银行任命的外部审计员、金融服务管理局和/或其他各方提供访问权限，根据监管规定，法律和法规授权进行检查，以便在需要时及时获得必要的数据和信息。 4.声明在金融服务管理局和/或其他依法被授权进行检查的各方对所提供的服务活动进行检查时没有异议。 5.作为关联方，维护所有信息的安全，包括银行机密和客户的个人数据。 6. 只能根据银行的批准进行部分活动的转让（分包），并有书面文件为证。 7. 向银行报告任何可能导致重大财务损失和/或破坏银行顺利运作的重大事件。 8. 通过有关银行向金融服务管理局提交由独立审计师定期对数	客户与其服务供应商签订的合同中应清楚列明所提供的服务内容和水平，以及服务供应商在合约下的网络安全责任和义务。 客户应对其外包政策和流程的网络安全要求仅定期的衡量和评估。 客户的网络安全审计应根据其组织内部的审计手册和审计计划进行。	华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。华为内部审计团队直接向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。严格的审计活动在推动网络安全流程和标准落地，保障结果交付上起着关键的作用。此外，华为云建立了完备的供应商选择机制和管理机制，除了对供应商的绩效进行日常监督和管理之外，也会定期对供应商进行风险评估。针对审计发现的问题，组织内会进行再评估，如果问题对金融机构的业务会造成重大影响，华为云会告知金融机构。 华为云对外提供了统一的沟通接口，负责收集并处理客户侧的投诉，以及向金融客户同步监管机构发布的通告。 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。

编号	具体控制要求	客户关注点	华为云的内部实践
	据中心、灾难恢复中心和/或基于信息技术的交易处理的实施情况进行的信息技术审计的结果。 9.提供经过测试和充分的灾难恢复计划。 10.愿意在协议期结束前终止协议的可能性（提前终止）；以及 11.按照银行与信息技术服务提供商之间的服务水平协议，履行服务水平。 (4)银行使用第(3)款所述的信息技术服务提供商必须基于书面协议，该协议至少包含信息技术服务提供商组织和/或执行第(3)款所述事项的意愿。		

编号	具体控制要求	客户关注点	华为云的内部实践
第21条	(1) 银行必须在印度尼西亚境内的数据中心和灾难恢复中心放置电子系统。 (2) 只有获得金融服务管理局的批准，银行才能将电子系统放置在印度尼西亚境外的数据中心和/或灾难恢复中心。(4) 第(2)款中提到的金融服务管理局的批准可以在如下条件进行。 b. 提交国家风险分析的结果。 d. 确保仅在符合印度尼西亚法律和法规规定且有银行和信息技术服务供应商之间的合作协议证明的情况下披露有关银行的机密信息。 e. 确保与信息技术服务供应商的书面协议包含法律选择条款。 f. 提交印度尼西亚境外的信息技术服务供应商的监管机构不反对管理局服务金融服务局可以对信息技术服务供应商进行审查的声明书。 h. 确保将电子系统置于印度尼西亚境外的计划给银行带来的益处超过银行承担的负担；	为保证业务连续性，客户需建立灾难恢复计划，系统应部署在印尼境内的数据中心和灾难恢复中心。若客户将该系统部署于境外，则需提交其他国家风险分析结果、供应商审查声明书等材料并在与供应商签订的协议中包含法律选择条款，以获得金融服务管理局的批准。	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和多可用区的模式，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。客户可根据自身需求选择可用区进行系统部署。若客户选择将电子系统部署于境外可用区，华为云可以安排专人积极配合客户提供相关证明以获取金融服务管理局的批准。 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。 基础设施高可用 ● 华为云依赖数据中心集群的二地三中心架构实现数据中心本身的容灾和备份，数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。同时，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。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，即便在一数据中心故障的情况下，也可以将流量负载均衡到其他中心。

编号	具体控制要求	客户关注点	华为云的内部实践
			● 华为云能够在多个地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。另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。 ● 用户可充分利用这些地域和可用区，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（包括自然灾害和系统故障）系统都能连续运行。 云安全合规 ● 在云安全合规方面，面向提供云服务的地区，华为云积极与监管机构对话，理解他们的担忧和要求，贡献华为云的知识和经验，不断巩固华为在云技术、云服务和云安全方面与相关法律法规的契合度。同时，华为也将法律法规的分析结果共享给租户，避免信息缺失导致的违规风险，通过合同明确双方的安全职责。华为一方面通过跨行业、跨区域的云安全认证满足监管机构要求，另一方面通过获得重点行业、重点区域所要求的安全认证，建立并巩固华为云业务的客户信赖度，最终在法律法规制定者、管理者、租户三者间共建安全的云环境。 云安全责任 ● 华为云对租户数据提供机密性、完整性、可用

编号	具体控制要求	客户关注点	华为云的内部实践
			性、持久性、认证、授权、以及不可否认性等方面的全面数据保护功能，并对相关功能的安全性负责。但是，华为云只是租户数据托管者，租户对其数据拥有所有权和控制权。华为云绝不允许运维运营人员在未经授权的情况下访问租户数据。华为云关注内外部合规要求的变化，负责遵从华为云服务所必需的安全法律法规，开展所服务行业的安全标准评估，并且向租户分享我们的合规实践，保持应有的透明度。
第23条	(1) 银行必须在印度尼西亚境内组织基于信息技术的交易处理。 (2) 基于信息技术的交易处理可由印度尼西亚境内的服务提供商进行。	客户应确保数据中心位于印度尼西亚境内，或在境外使用云服务时，应获得金融监管机构的批准。	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。同时，华为云目前获得了国际上多项权威的安全与隐私保护认证，第三方测评公司也会定期对华为云展开保密性、安全充分性和合规性的审核并出具专家报告。更多详细信息请参见**《华为云安全白皮书》**。

5.3 报告

编号	具体控制要求	客户关注点	华为云的内部实践
第31条	(1) 银行必须报告在实施信息技术过程中可能和/或已经导致重大财务损失和/或扰乱银行平稳运作的重大事件、滥用和/或犯罪。 (2) 第(1)款所指的报告必须立即通过电子邮件或电话提交给金融服务管理局，然后在知道重大事件和/或滥用或犯罪后不晚于7个工作日提交书面报告。	客户应制定网络安全事件管理策略，建立安全事件上报和决策流程，并采取适当应对计划和沟通策略。 当发生网络安全事件时，客户应按照规定的要求向金融服务管理局等或其他相关监管机构汇报事件改进建议。	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、汇报至相应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CISO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。

6 华为云如何遵从及协助客户满足《 No.21/SEOJK.03/2017 关于商业银行在使用信息技术时实施风险管理的通知 》

印尼金融服务管理局发布的《 No.21/SEOJK.03/2017 》规定对于金融机构的信息科技风险管理提出了多个方面的要求， 包括多个IT领域的要求，如业务连续性，数据安全、信息安全、供应商要求等。

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 信息技术管理

编号	具体控制要求	客户关注点	华为云的内部实践
1.5. 项目管理	根据POJK MRTI第11条规定，银行有义务采取控制措施，创造一个完全保密和集成的系统和数据，并支持实现银行的目标，包括在系统开发中应用项目管理。	客户应建立项目管理框架，确保外包项目的交付和实践流程满足其项目目标和要求。对于每个IT项目计划，客户应考虑项目范围、活动、里程碑以及每个阶段应交付的内容。	华为云制定了完整的项目管理方法，实施基于CCM5/CMMI、ISO 9001:2000和PMI框架的实践，使合格的项目管理专业人员在全球成功实施项目。

6.2 信息技术开发和采购

编号	具体控制要求	客户关注点	华为云的内部实践
2.2. 开发和采购中的控制措施	在进行信息技术开发和采购时，银行需要采取控制措施，以创造保密性和集成整合性的系统和数据，以维护和支持实现第11条规定的银行的目标。 除了第11条规定的控制措施外，控制措施还可以包括。 a. 确保系统是根据用户需求开发的。 b. 确保一个系统与另一个系统的兼容性，以便它们能够继续正常运行（互操作性和兼容性）。 c. 拥有专门为有关银行开发的软件的源代码（专），以便在审查和调查需要时可以获取源代码。 d. 充分识别、衡量和控制与信息技术开发和采购有关的可能出现的风险。 e. 确定银行在信息技术开发和采购方面可接受的风险偏好和风险敞口暴露。 f. 制定紧急情况下的系统开发程序；以及 g. 确保开发和运营环境的分离，包括将负责开发过程的人力资源与开展银行运营活动的人力资源分开。	客户在选择服务提供商之前应进行尽职调查，特别是在治理、风险和合规管理机制方面。客户应制定一份信誉良好的服务提供商列表，并能够确定是否有任何可行的替代首选服务提供商。	为了开发过程的安全，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。华为云积极推行快速迭代的全新DevOps流程，还将华为的安全生命周期SDL无缝嵌入DevOps逐步形成高度自动化的DevSecOps全新安全生命周期管理流程，以及确保全新流程顺利而灵活执行的云安全工程能力和工具链。 为了保证开发过程中开源和第三方的软件安全，华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。 华为云追求新的DevOps流程，具有快速持续迭代能力，集成了华为安全开发生命周期(SDL)。此外，逐步形成高度自动化的新安全生命周期管理方法和流程，称为DevSecOps，与云安全工程能力和工具链一起确保DevSecOps的顺利灵活实施。华为云对开

编号	具体控制要求	客户关注点	华为云的内部实践
			发环境进行分层管理，并实施物理隔离、逻辑隔离、访问控制、数据传输通道审批和审计等保护措施。

编号	具体控制要求	客户关注点	华为云的内部实践
2.3银行需要有开发和采购政策、标准和程序	银行必须根据POJK MRTI第8条规定制定IT开发和采购政策、标准和程序。IT开发和采购程序必须始终处于IT工作部门的控制之下，并由项目管理部门进行管理。项目管理可以采取工作小组的形式，其成员至少来自IT工作单位和IT用户工作单位，其任务是确保系统的开发具有良好的结构并满足用户需求。如果在流程开发过程中的采购和变化，如用户需求的变化或支持技术的变化，必须设计、实施和正确记录变化管理程序。 开发和采购政策、标准和程序必须考虑以下内容。 a. IT开发阶段至少包括 1) 识别和分析用户需求。 2) 定义用户需求。 3) 系统设计。 4) 编程。 5) 测试。 6) 实施。 7) 实施后的审查。 8) 维护；以及 9) 处置。 b. IT采购过程包括 1) 采购标准。 2) 采购项目指南。 3) 托管协议。 4) 软件购买、许可和维护合同。 5) 维护。 6) 保修。 7) 争端解决。 8) 协议的变更。	客户应根据要求建立一个框架来管理其系统开发生命周期（SDLC）。 客户应确定、定义和记录IT系统的功能要求，覆盖系统性能、弹性和安全控制。	为了开发过程的安全，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。华为云积极推行快速迭代的全新DevOps流程，还将华为的安全生命周期SDL无缝嵌入DevOps逐步形成高度自动化的DevSecOps全新安全生命周期管理流程，以及确保全新流程顺利而灵活执行的云安全工程能力和工具链。 为了保证开发过程中开源和第三方的软件安全，华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。 华为云追求新的DevOps流程，具有快速持续迭代能力，集成了华为安全开发生命周期(SDL)。此外，逐步形成高度自动化的新安全生命周期管理方法和流程，称为DevSecOps，与云安全工程能力和工具链一起确保DevSecOps的顺利灵活实施。华为云对开发环境进行分层管理，并实施物理隔离、逻辑隔离、访问控制、数据

编号	具体控制要求	客户关注点	华为云的内部实践
	9) 安全；以及 10) 分包给其他方。 c. 银行在项目管理和变更管理方面需要制定的政策、标准和程序。		传输通道审批和审计等保护措施。

编号	具体控制要求	客户关注点	华为云的内部实践
2.4开发和采购风险管理过程	2.4.1. 与开发和采购有关的风险测量 IT开发和采购流程中的风险测量水平取决于相关因素，其中包括 a. 是否符合业务战略计划和监管要求。 b. 系统或流程范围的变化。 c. 开发、测试和运行环境的分离，包括开发人员、测试人员和用户的访问安排。 d. 通过购买未经修改的软件包、购买经过修改的软件包、内部开发或由第三方开发获得的应用系统计划。 e. 系统的范围和重要性或受影响的业务单位的数量。 f. 要开发的应用程序的处理类型的复杂性（批处理、实时、客户或服务器、平行分布）。 g. 要开发的应用系统的数量和交易价值。 h. 待开发系统的分类和数据敏感性。 i. 对数据的影响（读取、下载、上传、更新或更改）。 j. 如果系统是由第三方购买或开发，供应商的经验和能力水平。 k. 开发团队中人员的数量和能力是否足够。 l. 所选平台和应用程序与银行架构的兼容性。 m. 开发的系统与现有系统的依赖性。 n. 用户数量与最初的开发计划不匹配或开发过程中组织结构的变化。 o. 政策的改变。	客户应建立变更管理程序，根据信息资产的重要性，对变更进行识别、分类和优先级排序。 客户应根据计划的频率定期对变更管理的安全要求以及流程的有效性进行审查和更新。 客户应根据计划的频率定期对变更管理的安全要求以及流程的有效性进行审查和更新。	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。华为云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。 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。

编号	具体控制要求	客户关注点	华为云的内部实践
	p. 存在新的风险或正在开发的技术可能产生的风险或技术过时的风险。 q. 审计弱点或在自我评估中遇到的弱点；以及 r. 开发实施与目标完成时间的不匹配。 2.4.2. 开发和采购中的风险控制 在信息技术开发和采购的每个阶段，银行必须通过银行信息技术开发和采购的政策、标准和程序中规定的几种控制手段来减轻已经确定和衡量的风险。在减轻风险后，银行必须监测受控风险和剩余风险，因为任何可能影响信息技术开发和采购计划及流程的干扰，最终都可能影响银行的业务活动。 2.4.2.1. 开发中的风险控制 为了控制与信息技术开发有关的风险，银行必须能够确保所进行的系统开发符合每个开发阶段的政策、标准和程序，这要通过注意以下几点来实现： a. 系统开发计划符合用户需求和银行的业务政策方向。 b. 所开发的系统设计在启动和规划阶段就包含了用户需求，并符合涉及内部审计参与的应用控制标准。根据其目的，控制分为预防、检测或发现、纠正等控制。必须进行的控制至少包括： 1) 输入控制 这至少包括检查数据的有效性或正确性，数据范围，参数，以及输入数据的重复性。 2 ）过程控制 确保流程准确工作，并能存储或拒绝信息。可由系统自动控制的过程控制至少包括错误报		

编号	具体控制要求	客户关注点	华为云的内部实践
	告、交易日志、顺序检查和文件备份；以及 3) 输出控制 确保系统安全地管理信息，适当地分发已处理的信息，并删除已过保留期的信息。 c. 编程交付物是根据设计规范建立的，并有文件化的测试计划，以便于跟踪应用系统的变化。 d. 通过定义测试场景的范围，进行一系列的测试，评估测试结果，对系统进行改进，直到测试报告被批准。 e. 实施新系统可以与旧系统一起运行，准备安装、文件迁移、数据转换、技术指导文件和培训；以及 f. 实施系统的结果在持续的基础上运行良好，并对维护效果的结果进行定期审查。 2.4.2.2. 采购中的风险控制 为了控制采购中的风险，银行在选择供应商的产品或服务之前，必须制定供应商的选择标准，并审查供应商的能力，其中包括与财务状况、支持水平和安全控制有关的能力。 银行应审查许可协议，以确保每一方的权利和责任是明确和合理的。在管理层签署协议之前，银行的法律顾问必须确认履约保证、对源代码的访问、版权、以及软件或数据的安全，都有明确的规定。需要考虑的事项有 a. 确保采购过程符合银行的政策、标准和程序，以及与采购有关的适用规定；以及 b. 签订所有具有足够法律效力的协议。		

6.3 信息技术运营管理

编号	具体控制要求	客户关注点	华为云的内部实践
3.2. 与信息技术运营活动有关的政策、标准和程序	根据POJK MRTI第12条 银行必须确保信息技术运营的连续性和稳定性，并降低可能破坏银行运营活动的风险。 银行必须制定涵盖IT运营各个方面的政策，并根据银行IT运营的复杂性进行调整。IT运营方面包括数据中心、容量规划和监测、硬件和软件配置管理以及数据库管理。 该程序包含实施运营活动的职责、问责、授权和指导方针。 此外，管理层必须制定用于银行 IT 运营的运营建设、测试和业务环境的硬件和软件标准。	客户应建立并定期审查正式的信息安全政策和流程。 客户基于业务需求建立网络安全能力和控制的管理要求。 客户应制定和应用网络安全控制要求时考虑设计中的安全原则。	根据ISO 27001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、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。

编号	具体控制要求	客户关注点	华为云的内部实践
3.3 IT运营活动的风险管理过程	IT运营活动的风险管理必须考虑： a. 可能扰乱运营的事件或活动包括： 1) 技术投资错误，包括实施不当，供应商的失败，业务需求定义不当，与现有系统不兼容，或软件过时，以及银行使用的硬件和软件失去供应商支持。 2) 系统开发和实施问题包括项目管理不足、成本和时间超支、编程错误、未能整合或迁移现有系统，或系统未能满足用户需求。 4) 系统故障，包括网络、接口、硬件、软件或内部通信故障；以及 5) 系统安全漏洞，包括外部和内部安全漏洞、编程欺诈或计算机病毒。 b. 信息技术操作风险的水平取决于相关因素，其中包括： 4) 应用程序的获取可以通过购买未经修改的软件包，购买经过修改的软件包，和/或在内部或由第三方开发的软件包。 11) 实施人员的数量和能力是否足够。	客户应定义和实施基础设施安全标准。 客户应根据计划的频率定期对应用网络安全的控制进行审查和更新。	为配合客户满足合规要求，华为作为云技术的研发者和云服务运营者的双重角色，华为云负责其作为CSP的基础设施和IaaS、PaaS 和 SaaS 各类各项云服务自身的安全保障。华为云一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、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。此外为了保证华为云平台以及网络的安全、稳定运行，华为云采取了一系列管理措施，包括：漏洞分析和处理，日志监控和事件响应、云产品默认安全配置优化、安全补丁部署、防病毒软件部署以及定期备份系统和设备配置文件并测试其有效性。

6.4 信息技术运营管理

编号	具体控制要求	客户关注点	华为云的内部实践
4.2 与通信网络有关的政策、标准和程序	根据POJK MRTI第13条规定，银行必须提供符合保密性、完整性和可用性原则的通信网络。为履行这一义务，银行必须制定政策、标准和程序，作为提供通信网络的准则，以确保通信网络的运行连续性和安全性。通信网络政策是指将由银行组织的通信网络管理的方向和目的，例如与通信网络上的加密应用有关。 通信网络标准是银行为履行通信网络政策而设定的一些参数，例如，在银行内部使用安全插座层（SSL）。 通信网络程序是银行为履行通信网络标准而采取的一系列技术步骤，其需要建立的政策、标准和程序至少包括： a. 网络性能和容量规划。 b. 保证通讯网络的安全（网络访问控制，包括远程访问）。 c. 变更管理（设置、配置和测试）。 d. 网络管理、网络日志和网络监控。 e. 互联网、内部网、电子邮件和无线的使用（包括使用通信网络的机制）。 f. 问题处理程序。 g. 备份和恢复设施；以及 h. 如果银行使用的通信网络是由信息技术服务提供商组织的，则应签订符合银行需求的协议和服务水	客户应制定网络安全政策和程序，并获得组织负责人或代表的批准，分发给组织的内外部相关组织。 客户应建立正式的系统以及网络安全架构，确保组织的网络免受安全风险。 客户应定期对网络安全的风险处置计划的实施情况进行跟踪监测。	根据ISO 27001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、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。

编号	具体控制要求	客户关注点	华为云的内部实践
	平协议，并定期进行监测。		

编号	具体控制要求	客户关注点	华为云的内部实践
4.3 通信网络风险管理过程	4.3.1. 风险控制 a. 通信网络技术的使用为银行和客户提供了各种便利和好处，然而，注意可能出现的风险，其中包括： 1 ）数据/信息的丢失。 2 ）数据/信息完整性的丢失。 3 ）传输的数据/信息不完整。 4 ）信息的保密性丢失。 5) 通信网络因中断或灾难而无法使用；以及 6) 通信网络设备的丢失/损坏。 b. 在控制通信网络的风险方面，银行必须注意以下事项： 1 ）通信网络设计 通信网络的设计必须是有效的，但也是动态的，以预测未来的发展。在这一阶段，有几件事需要考虑： a) 确定通信网络拓扑结构。 b) 规划通信网络的容量（ 容量规划 ）。 c) 通信网络媒体的选择。 d) 硬件备份，替代路由，或替代供应商。 e) 物理安全和逻辑。 f. 将网络设备放置在不受自然干扰和未经授权人员进入的地方；以及 ii. 设置网络设备的系统参数。 f) 提供审计跟踪，至少对通信网络设备的参数设置和访问权限的变化以及这些访问权限的使用进行审计。 2) 访问控制	客户应建立正式的系统以及网络安全架构，确保组织的网络免受安全风险。 客户应定期对网络安全的风险处置计划的实施情况进行跟踪监测。	华为云参照ISO27001、ISO20000、CSA STAR等众多的国际及行业标准，构建并实施了一套完善的信息科技风险管理体系，涵盖了IT治理/管理、信息系统开发和获取、IT运营、通信网络、信息安全等各个领域，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。其中，在信息安全领域，华为云构建了完善的信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性等。 华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，包括最常见的云攻击威胁：暴力破解、端口扫描、肉鸡（ 被黑客远程控制的机器 ）、Web攻击、Web未授权访问、APT攻击等。并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。同时，华为PSIRT会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为相关漏洞

编号	具体控制要求	客户关注点	华为云的内部实践
	通信网络的访问控制非常重要，必须加以考虑，因为通信网络是进入银行信息系统的主要门户。如果管理不善，信息安全就会受到危害。在实施访问控制时，银行必须考虑几件事，即： a) 用户对通信网络的访问是基于业务需要，并注意信息安全方面。 b) 根据物理和逻辑两部分对通信网络进行分割，如开发环境和操作环境之间的分离。 c) 如果不能进行物理分离，银行必须对通信网络进行逻辑分离，并对网络通信的安全访问进行监控。 d) 连接到银行以外的通信网络的决定必须符合安全要求，并在实施前由管理层正式批准。 e) 实施能够限制未经授权或意外的网络通信的控制措施。 f) 通信网络设备的配置应组织良好。不需要的功能或服务应被禁用。 g) 使用通信网络安全设备，如防火墙、入侵检测系统（IDS）和入侵预防系统（IPS）。 h) 在适当考虑安全的情况下，使用额外的通信网络监控设备（网络管理系统）；以及 i) 定期测试通信网络的安全性，例如通过渗透测试。 4.3.2. 风险监测 对银行使用的通信网络可能出现的风险进行监测，主要包括：		信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。此外，华为云配备了专人与行业机构、风险和合规组织、地方当局和监管机构保持联系并建立联络点。

编号	具体控制要求	客户关注点	华为云的内部实践
	a. 应定期监测现有的审计线索，以尽早发现任何违规行为。 b. 根据可用性和响应时间，定期测量通信网络的性能。 c. 与装机容量相比，银行应监控业务发展计划所使用和所需的容量。 d. 银行应监测并跟踪对通信网络的入侵或攻击；以及 e. 银行必须定期审查授予用户的权限，以确保授予的权限仍然符合职责和权限。此外，有必要审查银行内可访问银行外通信网络的通信网络用户。		

6.5 信息安全

编号	具体控制要求	客户关注点	华为云的内部实践
5.2 与信息安全有关的政策、标准和程序	根据POJK MRTI第16条，银行必须确保信息安全得到有效实施，至少要注意以下几点： a. 信息安全的目的是通过考虑到对规定的遵守，确保所管理的信息得到有效和高效的保密性、完整性和可用性，并使其得到有效和高效的维护。 b. 信息安全是在信息技术使用中的技术、人力资源和流程等方面进行的。 c. 根据对银行所持信息的风险评估结果，实施信息安全；以及 d. 确保提供信息安全方面的事件处理管理的可用性。	客户应制定网络安全政策和程序，并获得组织负责人或代表的批准，分发给组织的内外部相关组织。 客户建立的网络安全政策与程序可参考业内技术安全标准。	根据ISO 27001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、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。

编号	具体控制要求	客户关注点	华为云的内部实践
5.2.3.2 人力资源管理程序	人力资源管理程序至少包括： d. 与银行雇员、顾问、临时荣誉雇员和信息技术服务供应商的雇员签订的协议必须包括符合银行信息安全政策的信息技术安全条款。例如，有必要制定一个条款，说明他们必须根据信息的分类，对其获得的信息进行保密。 e. 除了银行与信息技术服务提供商公司之间的协议外，信息技术服务提供商公司分配给银行的所有员工必须签署一份保密声明，包括为保护客户数据而进行的信息保密。 f. 必须向银行雇员、顾问、临时雇员和IT服务供应商的雇员提供关于信息安全的培训和/或社会化。这种培训和/或社会化是根据员工和IT服务商的角色和责任提供的。 g. 银行必须对人力资源部门违反信息安全政策的行为制定制裁措施；以及 h. 银行应制定程序，管理银行员工、顾问、临时员工和信息技术服务提供商的员工因职责变化或完成就业或协议而导致的资产归还和访问权的变更或终止。	客户应制定并落实员工在雇佣前、雇佣期间及雇佣后的网络安全要求。 客户应根据计划的频率定期对人员网络安全管理要求以及流程的有效性进行监测和定期评估。 客户应在劳动合同及保密条款中包含人员应遵守的网络安全的要求和责任。 客户应对定期对在职员工进行网络安全意识培训 客户应确保在员工离职后对其相关权限和资产进行审查和回收。	根据ISO 27001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、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。

编号	具体控制要求	客户关注点	华为云的内部实践
5.2.3.3 物理和环境安全程序	物理和环境安全程序至少包括： a. 关键信息处理设施（如主机、服务器、计算机和有源网络设备）应提供足够的物理和环境保障，以防止未经授权的访问、损坏和其他干扰。 b. 关键信息处理设施的物理和环境保障包括，除其他外，房间的隔板、访问控制（如使用访问控制卡、个人识别码（PIN）和生物识别技术）、房间内安全设备的完整性，如警报器、火灾探测器和灭火器、空气温度和湿度计、闭路电视摄像机，以及保持房间和设备的清洁，如远离灰尘、香烟、食物、饮料和易燃物品。 c. 必须确保空调、电力资源和火警等配套设施在支持信息处理设施运行方面的能力和可用性。 d. 属于信息技术服务供应商的资产，如服务器和交换工具，必须被明确识别并给予适当的保护，例如，实施适当的安全、双重控制或将其与银行的资产分开；以及 e. 按照既定程序，定期维护和检查信息处理设施和配套支持设施。	当客户使用云服务时，物理和环境安全的责任由云服务提供商承担。	机房选址：华为云数据中心机房选址一定程度上决定面临的自然灾害以及可能的环境威胁。华为云数据中心选址一律避开自然灾害不利或危险的地区，减少周边环境对数据中心产生的干扰，如400米内无实验室、化工厂等危险区域。同时，选址上保证了数据中心正常运营需要的配套资源，如市电、水、通信线路等。 访问控制：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了全天候（一天 24 小时、一周 7 天，即 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。门禁控制系统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。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。 安保措施：华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行 7*24 小

编号	具体控制要求	客户关注点	华为云的内部实践
			时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。 电力保障：华为云数据中心采用多级保护方案保障业务 7*24 小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源（UPS – UninterruptedPower Supply），提供短期备用电力供应。在机房供电线路上配置了稳压器和过压防护设备。在供电设备及线路上还设置冗余或并行的电力电缆线路为计算机系统供电。 温湿度控制：通过精密空调、集中加湿器自动调节，华为云数据中心机房温湿度保持在设备运行所允许的范围内，使设备元器件处于良好运行状态。机柜冷热通道有合理的布置，利用架空地板下空间作为静压箱来给机柜送风，并设置了冷通道密闭，以防止局部热点。 消防能力： 机房满足印尼《建筑与环境防火系统技术要求（26/PRT/M/2008）》，同时也遵守国家防火协会（National Fire Protection Association）的要求。采用了阻燃、耐火电

编号	具体控制要求	客户关注点	华为云的内部实践
			缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统，得以控制火情。 例行监控：华为云数据中心的电力、温湿度、消防等环境运行状态通过日常巡检制度得到例行监控，安全隐患能被及时发现并修复，确保设备稳定运行。 供水排水：华为云数据中心的供水和排水系统均有合理规划，保证了总阀门正常可用，确保关键人员知晓阀门位置，以免信息系统受到漏水事故破坏。机房建筑和楼层均有抬高场地，在外围设置了绿化地排水沟，加速排水，以降低场地积水倒灌风险。建筑满足防水一级标准，保证了雨水不能通过屋顶、墙壁向机房渗透。数据中心也配备了及时排水的设施，供水灾时使用。 防静电：华为云数据中心机房铺设了防静电地板，导线连接地板支架与接地网，机器接地以导走静电。在机房大楼顶部设置了避雷带，供电线路安装了多级避雷器，导走电流。

编号	具体控制要求	客户关注点	华为云的内部实践
5.2.3.4. 访问控制程序	访问控制程序至少包括 a. 物理和逻辑访问控制。 b. 银行必须根据风险分析应用识别和认证方法。使用的认证方法可以是 "你知道什么"（包括PIN和密码）、"你有什么"（包括手机、带芯片的磁卡和令牌）、"你是什么"（包括生物识别，如视网膜和指纹）的一种或多种组合。 c. 银行必须有经管理层批准的关于用户管理的正式书面程序，涵盖内部用户和外部用户（如供应商或IT服务提供商）的用户注册、变更和删除。 d. 授予访问权是指基于业务需求和尽可能少的访问权的原则。 e. 银行必须通过向用户提供初始密码或PIN码来建立控制程序，其中要考虑到： 1) 初始密码或个人识别码必须在第一次登录时更改。 2) 密码或PIN码要安全地给出，例如通过双层复写纸，以便只有被授权方知道。 3）初始密码或PIN码对每个用户来说都是唯一的，不容易被猜到。 4) 用户ID的所有者，特别是来自银行员工、临时员工和IT服务提供商的员工，在收到初始用户ID和密码或PIN码时，必须签署一份关于使用该用户ID和密码或PIN码的责任声明或协议；以及 5) 操作系统、应用系统、数据库管理系统以及网络和安全设备的默认密码或PIN码必须在实施前由银行更	客户应建立身份认证与访问控制管理机制，对访问系统的行为进行权限限制和监督。 客户应确保账号管理要求中包含所有内外部的账号类型。 客户应实施基于角色的访问控制及权限管理，符合按需知晓和使用的最小原则。	客户可通过华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**，对使用云资源的用户账号进行管理。IAM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（Cloud Trace Service，简称CTS）**，可提供对各种云资源操作记录的收集、存储和查询功能，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，华为云内部建立了完善的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

编号	具体控制要求	客户关注点	华为云的内部实践
	改，并替换默认用户-ID系统必。		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。 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。 此外，华为云只能通过华为云统一管理接入网关和SVN权限远程访问其内部系统。此外，接入网关支持强日志审计，确保运维人员能够在目标主机上的行为可以定位到个人。

编号	具体控制要求	客户关注点	华为云的内部实践
5.2.3.5 IT运营安全程序	IT 运营安全程序至少包括： f. 银行必须对信息技术服务供应商提供的信息技术操作服务进行定期审查。审查期限必须在银行与信息技术服务供应商的合作协议中规定。	客户应实施恶意代码/软件和病毒的保护。 客户应遵循已制定的网络安全事件管理策略，对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。 客户应定义和实施基础设施安全标准。	为了保证华为云平台以及网络的安全、稳定运行，华为云采取了一系列管理措施，包括：漏洞分析和处理，日志监控和事件响应、云产品默认安全配置优化、安全补丁部署、防病毒软件部署以及定期备份系统和设备配置文件并测试其有效性。 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。此外，华为云制定了完善的供应商管理机制，定期对供应商（包括外包人员）的表现进行考核，考核结果作为下次采购的关键参考。华为云也会与供应商（包括外包人员个人）签订安全合规和保密协议。

编号	具体控制要求	客户关注点	华为云的内部实践
5.2.3.6. 信息安全监控程序	银行必须进行监控，以发现威胁信息安全的工作，其方法根据风险或银行信息或IT资产的重要程度确定。监测可以实时进行，以便在出现被归类为可疑的活动时发出警报，例如，针对管理员密码的暴力攻击或试图在不合理的端口上访问服务器，或者根据风险水平定期进行，例如在一天结束时进行。	客户应制定网络安全事件管理策略，建立安全事件上报和决策流程，并采取适当应对计划和沟通策略。 客户应遵循已制定的网络安全事件管理策略，对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。	华为云作为CSP，负责其提供的基础设施和IaaS、PaaS 和 SaaS 各类各项云服务的重大事件管理。华为云拥有集中、完整的日志审计系统。并利用大数据安全分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的重大事件。并根据事件的实时状态进行事件升级和通报。 华为云可帮助客户构建网络安全防护体系，保障客户云服务的安全：在互联网边界客户可通过部署 Anti-DDoS流量清洗服务，来完成对异常和超大流量攻击的检测和清洗；通过**虚拟私有云（Virtual Private Cloud，简称VPC）**对关键网络分区进行划分和隔离；部署**Web应用防火墙（Web Application Firewall，简称WAF）**应对 Web 攻击以保护部署在 DMZ 区、面向外网的 Web 应用服务和系统。同时，为保证租户业务不影响管理操作，确保设备、资源和流量不会脱离有效监管，华为云将其网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、BMC

编号	具体控制要求	客户关注点	华为云的内部实践
			（Baseboard ManagementController）管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，便于实现职责分离。

6.6 灾难恢复计划

编号	具体控制要求	客户关注点	华为云的内部实践
6.2 与灾难恢复计划有关的政策、标准和程序	6.2.2. 与灾难恢复计划有关的政策 c. 灾难恢复中心 银行必须建立灾难恢复中心，并作为数据中心的备份，在数据中心因中断和/或灾难而无法运行时可以运行。根据银行选择的替代策略，灾难恢复中心可以由银行自己管理，也可以由IT服务提供商管理。在灾难恢复中心运作时，银行必须注意以下事项： 1) 灾难恢复中心应设在与数据中心位置分开的地方，同时考虑到地理因素。 a) 扰动或灾难的地理范围及其对灾难恢复中心所在城市或地区的影响；以及 b) 分析与灾难恢复中心位置相关的风险（如不位于地震、洪水或雷电多发地区），并与不同于数据中心的通信和电力基础设施以及保持系统运行所需的其他设施相连。 2）所选的灾难恢复中心地点对暴乱和动乱的可能性的脆弱性。 3）灾难恢复中心必须有能够保证灾难恢复中心运行的电力供应和电信设施。 4) 灾难恢复中心的系统必须与数据中心使用的系统兼容，如果数据中心发生变化，必须进行调整。 5) 灾难恢复中心是一个限制区域；以及	客户应确保基础设施的安全标准涵盖主数据中心、灾难恢复数据站点和办公空间中的所有可用基础设施实例。	客户可以依托华为云数据中心集群多区域（Region）和多可用区（AZ）架构，实现业务系统的容灾和备份。数据中心部署在世界各地，因此客户将在灾难发生时拥有相互的灾难数据备份中心。当一个区域发生一次故障时，系统会自动将客户应用程序和数据从受影响区域转移到数据备份中心，在满足合规策略的同时，确保受影响客户的业务连续性。华为云还部署了全球负载均衡管理中心，客户的应用在数据中心内实现N+1部署规模，同时将流量负载均衡到其他中心，即使数据中心故障也是如此。 华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范

编号	具体控制要求	客户关注点	华为云的内部实践
	6）安全返回时间，以确保在灾难恢复中心的恢复过程。		围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。 同时，华为云在提供高可用基础设施、冗余数据备份、可用区灾备等服务外，还制定了自身的业务连续性计划。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。如果华为云的灾难测试过程中需要客户的参与，华为会提前通知。 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，符合GB 50174《 电子信息系统机房设计规范 》A类标准和TIA-942《 数据中心电信基础设施标准 》T3+标准。-华为云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洞被利用对客户造成的业务影响。

6.7 信息技术供应商管理

编号	具体控制要求	客户关注点	华为云的内部实践
9.4. 内部控制和内部审计	9.4.1. 对信息技术服务供应商的监测和监督 如果银行的信息技术实施是由信息技术服务提供商进行的，银行仍然建立信息技术工作部门和领导信息技术工作部门的最高官员。 银行应当建立监督计划，以确保IT服务商按照协议完成工作或提供服务。支持该计划的资源可能会有所不同，这取决于IT服务供应商所从事的系统、流程和服务的重要性和复杂性。 银行必须在雇用IT服务供应商之前和之后进行审查，以确保银行的风险管理政策、标准和程序得到有效执行。此外，定期进行绩效审查和SLA成就，并以报告的形式进行记录。银行应该对信息技术服务提供商的审计报告进行监测。 9.4.2. 内部审计 本行定期对 IT 服务供应商进行审计，审计工作由银行的内部审计或银行指定的外部审计方进行。审计的范围符合协议中规定的服务范围。被审计的领域包括 a. IT系统。 b. 数据安全。 c. 内部控制框架；以及 d. 灾难恢复计划。 银行必须确保金融服务局或金融服务局指定的其他各方有权访问信息技术服务提供商，以获取记录和交易文件，以及由信息技术服务提供商存储或处理的银行信息，并有权获取与信息技术服务有关的信息技术	客户与其服务供应商签订的合同中应清楚列明所提供的服务内容和水平，以及服务供应商在合约下的网络安全责任和义务。 客户应对其外包政策和流程的网络安全要求仅定期的衡量和评估。 客户的网络安全审计应根据其组织内部的审计手册和审计计划进行。	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**《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》**对。 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。此外，华为云制定了完善的供应商管理机制，定期对供应商（包括外包人员）的表现进行考核，考核结果作为下次采购的关键参考。华为云也会与供应商（包括外包人员个人）签订安全合规和保密协议。 华为云会根据外部审计机构的要求，提供用于验证华为云安全和合规管控措施有效性的审计样本，如安全体系管理文件、操作记录、系统日志等。如有特殊情况导致审计样本覆盖的时间不满足要求，华为云

编号	具体控制要求	客户关注点	华为云的内部实践
	服务提供商的报告和审计结果。		将配合审计机构在审计报告中注明原因。 针对审计过程中发现的所有问题，华为云将在审计机构的协助下，根据风险评估机制，评估这些问题对金融行业客户的潜在影响。若经评估后，识别出可能对客户业务/数据的可用性、完整性和保密性造成严重影响的问题，华为云会将此类问题列为安全事件，并根据已制定的客户通知流程，及时对受影响的客户群体进行通知，通知的内容包括但不限于问题描述、问题影响、下一步补救计划等。同时，华为云会根据内部的安全事件管理流程对问题进行整改，整改完成后审计机构会进行再评估。

7 华为云如何遵从及协助客户满足《 No.4_POJK.05_2021 关于非银行金融机构在使用信息技术时实施风险管理的规定 》

印尼金融服务管理局发布的《 No.4_POJK.05_2021 》规定对非银行金融机构（ LJKNB ）实施IT技术提出的风险管理要求，涉及多个IT领域的要求，如信息安全、业务连续性、数据安全、境内交易处理、供应商管理等要求。

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。

7.1 识别、测量、控制和监控信息技术风险的充分性

编号	具体控制要求	客户关注点	华为云的内部实践
第11条	（1）LJKNB必须制定政策和程序，以执行第3条第（2）款c点所述的使用信息技术的风险的识别、测量、控制和监控过程。 （2）LJKNB必须根据第（1）款所述的政策和程序，识别、测量、控制和监控使用信息技术的风险。 （3）第（2）款所述的识别、测量、控制和监测使用信息技术的风险的过程应至少在第9条第（3）款所述信息技术相关方面进行。 （4）LJKNB在使用信息技术服务提供商的情况下，LJKNB有义务确保信息技术服务提供商按照金融服务管理局规则进行风险管理。	客户应定期对网络安全的风险处置计划的实施情况进行跟踪监测。 客户应审查修订新实施的网络安全控制的设计和有效性。	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。华为云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。 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

编号	具体控制要求	客户关注点	华为云的内部实践
			管理要求得到适当管理。

编号	具体控制要求	客户关注点	华为云的内部实践
第12条	（1）在开发信息技术时，LJKNB必须采取控制措施，以建立支持以下内容的系统： a. 实现LJKNB目标；和 b.维护机密性和数据集成。 （2）第（1）款所述的控制措施至少包括： a. 建立和应用信息技术开发和采购的方法和程序； b.在系统开发和采购中实施项目管理； c.在系统开发和安装过程中进行适当的测试，包括使用用户工作单元进行测试，以确保用户需要的准确性和一致性，以及系统与其他系统的兼容性； d.关于开发、安装和维护信息技术系统的文件； e.具有信息技术系统变更管理； f.确保LJKNB信息技术系统能够完整显示信息；和 g.在软件影响LJKNB运营的连续性且由另一方创建的情况下，确保就该软件达成书面协议。	客户应建立变更管理程序，根据信息资产的重要性，对变更进行识别、分类和优先级排序。 客户应确保外部开发的应用程序的代码安全性。 客户应建立正式的变更审批机制，由业务负责人、网络安全职能部门及变更委员会授权批准后才可以变更。	华为云制定了完整的项目管理方法，实施基于CCM5/CMMI、ISO 9001:2000和PMI框架的实践，使合格的项目管理专业人员在全球成功实施项目。 为配合客户满足合规要求，华为云也制定了变更管理程序，管理应用变更和基础设施变更。在提出变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。 华为云开发、测试和生产环境都进行了隔离，并且严格控制未脱敏的数据流入测试环境。华为云严格遵从华为对内发布的多种编程语言的安全编码规范。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。 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。华为云将派专人积极配合FI的尽职调查。客户在华为云的审计和监督权将根据情况在与客户签署的协议中承诺。

编号	具体控制要求	客户关注点	华为云的内部实践
			华为云已获得ISO27001、ISO27017、ISO 27018、SOC、CSA STAR等国际安全和隐私保护认证，并每年接受第三方审计。
第16条	（1）LJKNB必须有灾难恢复计划。 （2）LJKNB必须确保第（1）款所述的灾难恢复计划能够有效实施，以便LJKNB在发生灾难和/或LJKNB所使用的信息技术设施中断期间继续运行。 （3）LJKNB必须根据信息技术用户的定期影响分析的结果，对所有核心应用程序和关键基础设施进行第（1）款所述的灾难恢复计划试验。 （4）LJKNB必须定期审查第（1）款所述的灾难恢复计划。 （5）LJKNB应以书面形式确定第（3）款所述的试验期限和第（4）款所述的审查期限。	客户应确保基础设施的安全标准涵盖主数据中心、灾难恢复数据站点和办公空间中的所有可用基础设施实例。	华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。

7.2 信息技术使用的内部控制制度

编号	具体控制要求	客户关注点	华为云的内部实践
第20条	（1）LJKNB必须拥有LJKNB自身和/或信息技术服务提供商持有的信息技术使用内部审计指南。 （2）LJKNB必须定期审查信息技术使用方面的内部审计职能。 （3）LJKNB必须以书面形式设定本政策第（2）款所述的审查期限。	客户的网络安全审计应根据其组织内部的审计手册和审计计划进行。	华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。华为内部审计团队直接向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。严格的审计活动在推动网络安全流程和标准落地，保障结果交付上起着关键的作用。此外，华为云建立了完备的供应商选择机制和管理机制，除了对供应商的绩效进行日常监督和管理之外，也会定期对供应商进行风险评估。针对审计发现的问题，组织内会进行再评估，如果问题对金融机构的业务会造成重大影响，华为云会告知金融机构。 华为云对外提供了统一的沟通接口，负责收集并处理客户侧的投诉，以及向金融客户同步监管机构发布的通告。

7.3 非银行金融机构或信息技术服务商实施信息技术

编号	具体控制要求	客户关注点	华为云的内部实践
第21条	(1) LJKNB的信息技术的实施可以独立进行和/或使用信息技术服务提供商。 (2) 如果LJKNB信息技术的实施是由第(1)款所述的信息技术服务提供商进行的，LJKNB必须： a. 负责实施风险管理。 b. 建立组织信息技术的工作单元。 c. 监督信息技术服务提供商组织的LJKNB活动的实施。 d. 通过信息技术运营单元的成本和收益分析，选择信息技术服务供应商。 e. 监督和评估服务提供商的表现、声誉以及信息技术服务的提供是否充分。 f. 在必要时向内部审计员、外部审计员、LJKNB集团的内部审计员和/或金融服务管理局提供获取数据和信息的途径。 g. 及时向金融服务管理局提供对数据库的访问，包括对最新数据和过去数据的访问；以及 h. 确保信息技术服务提供商： 1.根据信息技术实施的需要，有学术和/或专业证书支持的具有可靠性的专家； 2.以符合独立审计结果的方式执行信息技术的管理原则。 4.宣布对金融服务管理局和/或任何其他方按照法规的规则授权进行检查，对进行检查提供的信息技术服务的活动没有异议。 5. 作为服务提供商，维护所有信息的安全，包括LJKNB	客户与其服务供应商签订的合同中应清楚列明所提供的服务内容和水平，以及服务供应商在合约下的网络安全责任和义务。 客户应定期评估合同和供应商管理程序的遵守情况，以及供应商对服务合同的履行情况。 客户应定期评估合同和供应商管理程序的网络安全控制的有效性。 客户在制定合同和供应商管理流程应要求网络安全职能的参与，考虑适用的网络安全基线要求，以及定期进行网络安全审计和审查。 客户应在与供应商签订的合同中明确退出、终止或续约的网络安全要求。 客户应在与供应商签订的合同中明确互相间的保密协议。	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。 此外，华为云制定了完善的供应商管理机制，定期对供应商（包括外包人员）的表现进行考核，考核结果作为下次采购的关键参考。华为云也会与供应商（包括外包人员个人）签订安全合规和保密协议。 华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。华为内部审计团队直接向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。严格的审计活动在推动网络安全流程和标准落地，保障结果交付上起着关键的作用。此外，华为云建立了完备的供应商选择机制和管理机制，除了对供应商的绩效进行日常监督和管理之外，也会定期对供应商进行风险评估。针对审计发现的问题，组织内会进行再评估，如果问题对金融机构的业务会造成重大影响，

编号	具体控制要求	客户关注点	华为云的内部实践
	的机密和消费者的个人数据。 6. 经LJKNB的书面同意，可以只进行部分转让活动（分包）。 7.向LJKNB报告任何可能导致重大经济损失和/或扰乱LJKNB运作的重大事件。 8. 提供经过测试的、充分的灾难恢复计划。 9. 愿意接受在协议期满前终止协议的可能性。 10.根据LJKNB与信息技术服务提供商之间的服务水平协议，履行服务水平；以及 11. 在执行其业务时有明确和可衡量的标准操作程序。 (3) LJKNB使用第(2)款所指的信息技术服务提供商，必须签订书面协议，其中至少包含信息技术服务提供商愿意遵守第(2)款h点所指的规定。		华为云会告知金融机构。 华为云对外提供了统一的沟通接口，负责收集并处理客户侧的投诉，以及向金融客户同步监管机构发布的通告。

编号	具体控制要求	客户关注点	华为云的内部实践
第22条	(1) 总资产不超过500,000,000,000.00印尼盾（5000亿盾）的LJKNB，需要利用信息技术对已处理的活动数据进行备份，并定期进行。 (2) 总资产超过500,000,000,000.00印尼盾（五千亿盾）至1,000,000,000,000.00印尼盾（一万亿盾）的LJKNB必须： a. 建立一个数据中心；以及 b. 对使用信息技术处理的活动数据进行备份，并定期进行。 (3) LJKNB必须以书面形式确定政策第(1)和(2)段所述的使用信息技术处理的活动数据的备份期限。 (4) LJKNB。 a. 总资产超过1,000,000,000,000.00印尼盾（一万亿印尼盾）的；和/或 b. 大部分业务是利用信息技术进行的，必须建立数据中心和灾难恢复中心。 (5) 管理局要求LJKNB。 a. 符合第（1）款所述的拥有数据中心的标准；以及 (b) 满足拥有灾难恢复中心的标准。	客户应确保基础设施的安全标准涵盖主数据中心、灾难恢复数据站点和办公空间中的所有可用基础设施实例。 客户应制定备份与恢复的安全管理策略，定义组织对信息、软件和系统备份的要求。	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。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

编号	具体控制要求	客户关注点	华为云的内部实践
第23条	(1) 拥有数据中心和/或灾难恢复中心的 LJKNB 必须在印度尼西亚境内的数据中心和/或灾难恢复中心放置电子系统。 (2) 第 (1) 款中提到的 LJKNB 有义务考虑地理因素，将数据中心的电子系统放置在与灾难恢复中心不同的位置。 (3) 第 (1) 段所述的 LJKNB 禁止将电子系统放置在印度尼西亚境外的数据中心和/或灾难恢复中心，除非它们已获得金融服务管理局的批准。 （5）在下列情况下，可以批准第（3）款所属的金融服务管理局的批准申请： e. 确保与信息技术服务提供商的书面协议包含法律选择条款； f. 提交印度尼西亚境外信息技术服务提供商监管局出具的无异议声明函，表示金融服务局有权对信息技术服务提供商进行检查；	客户应确保基础设施的安全标准涵盖主数据中心、灾难恢复数据站点和办公空间中的所有可用基础设施实例。 客户应确保由金融机构关键领域的代表定期识别网络安全相关的监管要求，并根据网络安全监管要求或标准的更新，对组织内的网络安全政策进行优化。	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。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

编号	具体控制要求	客户关注点	华为云的内部实践
第24条	LJKNB需要确保第23条所述的数据中心和/或灾难恢复中心能够保证LJKNB业务的连续性。	金融机构应建立自身的业务连续性机制，并制定保证其关键业务的RTO、RPO指标。	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。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。 华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。

编号	具体控制要求	客户关注点	华为云的内部实践
第25条	（1）LJKNB需要在印度尼西亚境内执行基于信息技术的交易处理。 （2）基于信息技术的交易处理可由印度尼西亚境内的服务提供商进行。 （3）第（2）款所述的服务提供商实施基于信息技术的交易处理，只要： a. 遵守预防原则； b. 符合第21条第（2）款至第（4）款所述的要求；和 c. 注意消费者保护方面。	客户应确保数据中心位于印度尼西亚境内，或在境外使用云服务时，应获得金融监管机构的批准。	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。同时，华为云目前获得了国际上多项权威的安全与隐私保护认证，第三方测评公司也会定期对华为云展开保密性、安全充分性和合规性的审核并出具专家报告。更多详细信息请参见**《华为云安全白皮书》**。
第26条	（1）LJKNB 需要在 LJKNB 信息技术发展计划中包括在数据中心、灾难恢复中心和/或基于信息技术的交易处理中使用信息技术服务提供商的计划。 （2）信息技术服务提供商实现数据中心、灾难恢复中心和/或基于信息技术的处理的计划必须作为业务计划实现报告的一部分进行报告。 （3）第（2）款所述义务仅适用于需要向金融服务管理局提交商业计划实现报告的LJKNB。	金融机构应建立自身的业务连续性机制，并制定保证其关键业务的RTO、RPO指标。 客户应确保基础设施的安全标准涵盖主数据中心、灾难恢复数据站点和办公空间中的所有可用基础设施实例。	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。 此外，华为云制定了完善的供应商管理机制，定期对供应商（包括外包人员）的表现进行考核，考核结果作为下次采购的关键参考。华为云也会与供应商（包括外包人员个人）签订安全合规和保密协议。

7.4 消费者个人数据的安全

编号	具体控制要求	客户关注点	华为云的内部实践
第30条	在实施信息技术时，LJKNB必须保证： a. 除非法律法规另有规定，消费者个人数据的获取、处理、使用、存储、更新和/或披露应在征得相关消费者同意的基础上进行；和 b. 根据数据采集时提交给消费者的目的使用或披露消费者个人数据。	客户应正确、全面地识别云端的个人数据，制定可保护个人数据的安全及隐私的策略并选择恰当的隐私保护措施，保障个人数据、隐私数据或机密数据的安全。	华为云会基于客户的同意或履行合同目的等合法目的，收集提供服务所必须的客户的个人数据，同时提供隐私通知告知客户所收集的个人数据类型、目的、处理方式、时间等内容。如在官网提供隐私政策声明以及客户同意及撤销同意的机制。对于各类线下市场营销活动中需收集个人数据时，在显著的位置提供隐私通知，并在收集个人数据时提供同意选项。华为云在其官网上提供丰富的配置选项，客户可根据偏好设置接收消息的种类和方式。针对涉及个人数据处理相关特性的云服务，华为云在其产品资料中，告知客户关于个人数据的种类、处理和存储的方式等相关信息，客户可根据产品资料的信息采取相应的隐私保护措施。

7.5 报告

编号	具体控制要求	客户关注点	华为云的内部实践
第31条	(1) LJKNB必须报告信息技术运营中可能和/或已经导致重大财务损失和/或扰乱LJKNB顺利运营的重大事件、滥用和/或犯罪。 （2）第（1）款所述报告必须在得知重大事件和/或滥用或犯罪后的5（五）个工作日内，按照附录中规定的格式提交给金融服务管理局，附录是金融服务管理局条例的组成部分。	当发生网络安全事件时，客户应按照规定的要求向金融服务管理局等或其他相关监管机构汇报事件改进建议。	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。 为配合客户满足监管要求，华为云会在规定的时限内向客户报告安全事件，报告的内容包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。 同时华为云会针对安全事件进行根因分析，制定预防规避措施。此外，华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。 华为云还建立了危机沟通计划，在发生影响客户业务持续运行的突发事件时，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 结语

本文描述了华为云如何为客户提供遵从印度尼西亚金融行业监管要求的云服务，并表明华为云遵守印度尼西亚金融服务管理局发布的重点监管要求，有助于客户详细了解华为云对印度尼西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、构建和部署遵从印度尼西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印度尼西亚金融行业监管要求的遵从性。

9 历史版本

日期	版本	描述
2022年10月	1.0	首次发布