华为云尼日利亚金融行业监管遵从性指南

文档版本 1.0

发布日期 2022-08-09

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 背景和发布目的

随着技术的发展，对云计算的使用已经成为尼日利亚金融机构的常态。云计算为金融机构的发展带来巨大的好处，但它也为金融机构创造了一个复杂的环境。为规范金融行业对于信息科技的运用，尼日利亚中央银行（Central Bank of Nigeria，简称CBN）发布了一系列监管要求，针对尼日利亚金融机构的网络安全、信息技术风险管理等方面提供了相关指南。

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。本文将针对尼日利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 适用的尼日利亚金融监管要求简介

尼日利亚中央银行（CBN）是尼日利亚金融服务监管机构，负责监督和管理银行和非金融机构的网络安全防御，颁布了相关指南来规范这一领域。

- **《尼日利亚金融服务行业信息技术标准蓝图》(Nigeria Financial Services Industry IT Standards Blueprint，简称“蓝图”)**

CBN于2019年7月发布了蓝图，该文件鼓励金融机构通过信息技术以及使□和实施信息技术(IT)标准的框架、指南来实现金融机构发展，维持信息技术竞争力。总体□标是使尼□利亚□融机构达到可接受的最低流程成熟度□平，这将有助于推动可持续增□、建□弹性并改善客□体验。

- **《存款货币银行和支付服务提供商基于风险的网络安全框架指南》(Risk-based Cybersecurity Framework and Guidelines For Deposit Money Banks and Payment Service Providers，简称“DMB和PSP指南”)**

为应对存款货币银行（简称“DMB”）、支付服务提供商（简称“PSP”）的网络安全威胁的数量和复杂程序的增加，CBN颁布了《DMB和PSP指南》，该指南于2019年1月1日生效，概述了DMB和PSP网络安全的最低要求，旨在为DMB和PSP实施网络安全计划提供指导，以便他们保持弹性并主动寻求保护其关键信息资产。

- **《其他金融机构基于风险的网络安全框架指南（草案）》(Draft Risk-based Cybersecurity Framework and Guidelines For Other Financial Institutions(OFIs)，简称“OFI指南草案”)**

CBN于2021年8月13日发布了尼日利亚《 OFI指南草案 》。该指南概述了OFI在制定和实施旨在减轻网络风险的战略、政策、程序和相关活动时必须遵守的最低要求。

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。

- **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。

- **客户**

与华为云达成商业关系的注册用户。

- **关键系统**

指任何IT基础设施（ 服务器、应用程序、数据库、网络、自动取款机、POS机等 ），其存储、处理或传输的信息因不可用（ 如故障、意外停机等 ）、损坏、未经授权的访问和/或拦截将导致重大财务损失，并对客户的业务运营和服务产生负面影响。

- **网络事件**

指任何可能因以下原因而导致重大经济损失的事件：

1. IT系统的意外中断，如核心银行应用，财政系统，贸易融资系统，核心网络设备，网上银行系统，电子渠道（ 如ATM，POS，USSD，移动银行等 ）和连接的支付系统，如SWIFT，RTGS，NEFT等。
2. 网络安全事件，如分布式拒绝服务（ DDOS ）、勒索软件/加密软件、数据泄露、数据破坏、网页破坏等。
3. 未经授权访问、披露、篡改或盗窃银行和客户的信息（ 个人可识别信息和财务数据 ）。重大财务损失是指超过未受损失影响的股东资金的0.01%损失。

2 华为云认证情况

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

全球性标准类认证

认证	产品介绍
ISO 20000:2011	ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的IT服务来满足客户和业务的需求。
ISO 27001:2013	ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO 27017:2015	ISO 27017是针对云计算信息安全的国际认证。ISO 27017的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 22301:2012	ISO 22301是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
SOC审计	SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况 出具的独立审计报告。
PCI DSS认证	支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discovers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IS O27701表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS 10012是BSI发布的个人信息数据管理体系标准，BS10012认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
PCI 3DS	PCI 3DS标准旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS认证的通过表明华为云在3D协议执行环境的过程、流程、人员管理等方面符合安全标准。

地区性标准类认证

认证	产品介绍
网络安全等级保护（中国）	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
可信云金牌运维专项评估（中国）	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
云服务用户数据保护能力认证（中国）	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。
工信部云计算服务能力评估（中国）	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。
可信云评估（中国）	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。

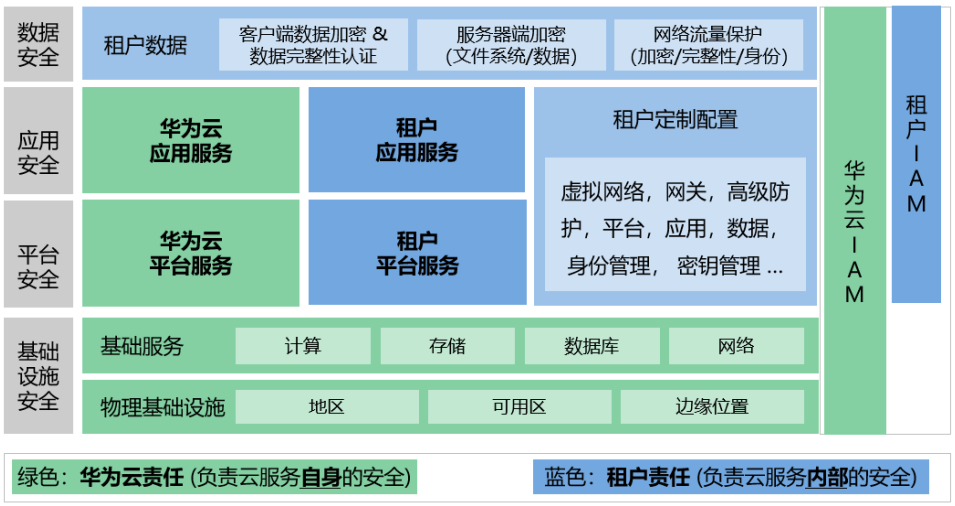
认证	产品介绍
网信办网络安全审查（中国）	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。
MTCS Level 3认证（新加坡）	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3等级认证。
OSPAR认证（新加坡）	OSPAR是新加坡银行业工会（ABS ）对外包服务提供商出具的审计报 告。华为云通过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

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

3 华为云安全责任共担

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

图 3-1 华为云安全责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和租户身份管（ 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《尼日利亚金融服务行业信息技术标准蓝图》要求

CBN于2019年7月发布了《尼日利亚金融服务行业信息技术标准蓝图》（简称“蓝图”），该蓝图旨在帮助尼日利亚金融服务机构发展八个关键技术能力领域，包含IT战略性调整、IT治理、框架&信息管理、解决方案交付、服务管理&运营、信息&技术安全、劳动力&资源管理、IT创新。这些能力领域的技能将支持将金融机构的IT职能转变为高质量IT。

金融机构在遵循《尼日利亚金融服务行业信息技术标准蓝图》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结蓝图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，会如何帮助客户客户满足这些控制控制要求的。

原文编号	控制域	具体控制要求	华为云的应答
4.1	IT服务提供商/供应商参与的注意事项	蓝图的这一部分提供了金融机构在与服务提供商合作时确保尽职尽责的指导方针： 1.政策和程序：制定供应商/服务提供商参与政策。大多数金融机构已经制定了指导与承包商、供应商和服务提供商互动的政策，这可能已经通过金融机构的业务政策，或通过ITIL、ISO20000、COBIT和/或ISO27001等IT标准的实施而存在。CIO应遵守现有的这些政策，并确保它们与金融机构的IT战略保持一致。果存在偏差或现有政策未能解决IT供应商的所有问题，建议对现有政策进行补充。	金融机构在与服务提供商合作时，应制定并执行服务提供商参与政策，CIO应确保参与政策与IT战略保持一致。 华为云遵循ISO27001、ISO20000、ISO22301等国际标准建立信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。

原文编号	控制域	具体控制要求	华为云的应答
		2.风险评估：进行风险评估以了解将任务或活动外包给供应商/服务提供商的影响。鼓励金融机构对供应商执行的业务活动进行风险评估，并确定内部执行该活动或由服务提供商执行该活动的影响。这种评估所产生的收益、风险和成本影响对于决定是在内部执行活动、让供应商在内部执行还是外包到服务提供商所在位置执行活动至关重要。	金融机构应进行风险评估，了解将任务或者活动外包给服务提供商的影响。 华为云作为云服务提供商，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风险评估活动。 华为云继承了华为公司的风险管理能力，建立了风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中有效控制风险，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。

原文编号	控制域	具体控制要求	华为云的应答
		3.供应商选择：在选择供应商/服务提供商时进行尽职调查 在正式聘用服务提供商之前进行尽职调查非常重要。推荐的尽职调查内容包括：检查服务提供商的背景和声誉、政策、运营和内部控制、财务绩效和业务连续性/应急计划（如适用）。建议金融机构独立验证和核实任何来自发证机构的证书，以确认供应商提供的证书的真实性。	金融机构在选择服务提供商时，应对其进行尽职调查，涵盖背景与声誉、政策、运营和内部控制、财务绩效、业务连续性/应急计划、服务资质等方面。 作为云服务提供商，华为云在背景与声誉、政策、运营和内部控制、财务绩效等方面的情况如下： （1）背景与声誉：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。 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。 （2）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、适用的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。 （3）运营：华为云遵循ISO27001、ISO20000、ISO22301等国际标准建立信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在

原文编号	控制域	具体控制要求	华为云的应答
			日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。 （4）内部控制：华为云继承了华为公司的风险管理能力，建立了风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中有效控制风险，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。 （5）财务绩效：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。全球权威咨询机构Gartner发布的《MarketShare:ITServices,worldwide2021》报告显示，华为云全球IaaS市场排名第五，亚太地区排名前四。 （6）业务连续性/应急计划：为向客户提供持续、稳定的云服务，华为云遵循ISO22301业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。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。 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。 （7）服务资质：华为云有多种认证以保证其服务的安全和兼容操作，这包括ISO27001、ISO27017、ISO27018、CSASTAR、PCIDSS等认证。更多认证信息请参见本文档2.华为

原文编号	控制域	具体控制要求	华为云的应答
			云的认证情况。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。
		云服务提供商需满足以下标准： 在公共云中作为个人身份信息（PII）处理者的PII保护实务准则–ISO27018； 信息安全管理系统-要求-ISO27001。	华为云获得了多个隐私合规相关国际标准的认证，以保障华为云的隐私安全，包括ISO 27701、ISO 29151、ISO 27018、BS 10012、SOC隐私原则的审计报告等，其中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，表明华为云已拥有完备的个人数据保护管理系统。 华为云参照ISO27001构建了完善的信息安全管理体系，并通过了认证。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。全方位保护客户系统和数据的保密性、完整性和可用性。

原文编号	控制域	具体控制要求	华为云的应答
		4.承包：执行彻底和严格的承包程序。 与供应商/服务提供者的合同必须与金融机构的法务部门共同起草，并由其审查。所有合同至少应包含： i.提供的服务范围 ii.服务性能要求 iii.职责划分和约定 iv.联络点、沟通和报告频率和内容 v.金融机构员工培训 vi.合同审查和争议解决流程 vii.价格结构和付款条件 viii.遵守适用的法律、法规、监管指南和标准 ix.知识产权和版权 x.审计权：合同应包含金融机构或其代表审计服务提供商的权利和/或访问审计报告的权利 xii.责任限制 xii.分包服务的能力 xiii.各方的终止权 xiv.终止时及终止后的义务	金融机构与供应商/服务提供者的合同必须由金融机构的法务部门共同起草，并由其审查。 为配合客户满足监管要求，华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化，客户及其监管机构对华为云的审计和监督权益，华为云会根据实际情况在与客户签订的协议中进行约定。

6 华为云如何遵从及协助客户满足《存款货币银行和支付服务提供商基于风险的网络安全框架指南》和《其他金融机构基于风险的网络安全框架指南（草案）》要求

6.1 网络安全风险管理体系与网络弹性评估

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南3.7	网络安全风险管理体系	3.7.DMB/PSP应确保风险评估、漏洞评估和威胁分析的行动一致，以检测和评估DMB/PSP信息资产的风险，并确定风险管理中安全控制的适当性。 3.8.IT风险应负责评估、测量和监控/报告与关键IT基础设施相关的风险，而信息/网络安全团队应负责风险缓解/处理。	金融机构应制定网络安全风险评估机制，定期进行风险评估、漏洞评估和威胁分析，检测和评估信息资产风险，并确定安全控制的适当性。 华为云作为云服务提供商，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风险评估活动。 华为云继承了华为公司的风险管理能力，建立了风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中有效控制风险，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。
OFI指南草案3.7、3.8	网络安全风险管理系统	3.7.OFI应定期进行风险评估、漏洞评估和威胁分析，以检测和评估OFI信息资产的风险，并确定风险管理中安全控制的适当性。 3.8.IT团队应负责评估、测量和监控/报告与关键IT基础设施相关的风险，信息安全/网络安全团队应负责风险缓解/处理。	

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南3.9	网络安全风险管理体系	3.9.1.确定当前的网络安全配置文件（“当前状态”） 3.9.1.1. DMB和PSP应通过评估所有可识别的网络安全漏洞、成功利用的威胁和可能性、潜在影响（声誉、财务、监管等）以及相关风险，定期确定其“当前”网络安全状况，以估计从潜在网络事件造成的损失/损害中恢复所需的资产数量和工作量。 3.9.1.2. 评估应包括但不限于网络安全治理的充分性；政策、程序和标准；业务运营中的固有风险；对信息资产新威胁的可见性；快速响应网络事件并从网络事件中恢复的能力；供应商风险，以及现有控制措施减轻已识别风险的有效性。	金融机构应评估所有可识别的网络安全漏洞、威胁和成功利用的可能性、潜在影响（声誉、财务、监管等）以及相关风险，应包括但不限于网络安全治理、固有风险，快速响应、控制措施有效性等，并且评估发现的所有差距都应记录在案并传达给高级管理层和董事会。 华为云作为云服务提供商： （1）为配合客户满足监管要求，华为云提供**企业主机安全（Host Security Service，简称HSS）**，帮助客户管理网络安全状态。HSS是服务器的贴身安全管家，提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助金融机构更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。 （2）华为云事件响应与恢复能力：华为产品安全事件响应团队已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，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，降低对用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，使基础设施、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用户业务的风险。
OFI指南草案4.1	网络弹性评估	4.1确定当前的网络安全配置文件（“当前状态”） 4.1.1.OFI应通过评估所有可识别的网络安全漏洞，、成功利用的威胁和可能性、潜在影响（声誉、财务、监管等）以及相关的风险，定期确定其“当前”网络安全状况；以估计从潜在网络事件造成的损失/损害中恢复所需的资源和工作量。 4.1.2.评估应包括但不限于网络安全治理的充分性；政策、程序和标准；业务运营中的固有风险；对信息资产新威胁的可见性；快速响应网络事件并从网络事件中恢复的能力；供应商风险，以及现有控制措施减轻已识别风险的有效性	

6.2 网络安全运营弹性

6.2.1 了解您的环境

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南4.1	了解您的环境	4.1.了解您的环境 DMB/PSP应努力熟悉其业务环境和关键资产。DMB/PSP应设计机制来维护授权软件、硬件（工作站、服务器、网络设备等）、其他网络设备以及内部和外部网络连接的最新清单。其网络上的所有未经授权的软件和硬件设备也应得到适当的识别、记录、删除和报告。 此外，DMB/PSP还应识别提供信息技术和网络安全功能/服务的员工和承包商。关于如何提高DMB/PSP的IT基础设施意识的详细信息包含在该指南的附录III中。	金融机构应了解并熟悉业务环境和关键资产，并且维护最新清单，包含所有未经授权的软件和硬件得到适当的识别、记录、删除和报告。 华为云作为云服务提供商，为配合客户满足监管要求，客户可通过**企业主机安全（HSS）**的资产管理功能，管理云上软件资产，包含云主机账号、端口、进程、Web目录和软件等安全资产信息的管理和分析。
OFI指南草案5.1	了解您的环境	5.1了解您的环境 OFI应努力了解其商业环境和关键资产。它应设计机制来维护授权软件、硬件（工作站、服务器、网络设备等）、其他网络设备以及内部和外部网络连接的最新清单，并应适当识别、记录、删除和报告其网络上所有未经授权的软件和硬件设备。	

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix III 3	了解您的环境	3.关于供应商/承包商/第三方，DMB/PSP应： 3.1 根据有效的服务水平协议(SLA)，维护由供应商/承包商/第三方提供的服务清单。 3.2确保每个SLA至少包含：所提供服务的详细信息、保密协议(NDA)、各方的角色和责任、服务期限、供应商服务水平管理、服务质量指标/评估标准和审计权条款。 3.3审核他们的供应商/承包商/第三方，以确保/强制遵守SLA，及时识别风险方；如有可能，访问他们的办公室/IT处理设施 3.4评估供应商/承包商/第三方分配给他们的供应商员工的资格、技能和/或经验。	金融机构应维护由供应商/承包商/第三方提供的服务清单，并确保SLA内容完整、详细；并评估供应商相关支持员工资格、技能或经验。 华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化，客户及其监管机构对华为云的审计和监督权益，华为云会根据实际情况在与客户签订的协议中进行约定。 华为云建立了人力资源管理框架，是建立在法律基础之上。保证员工背景和资历适合华为云业务的需要。员工行为符合所有法律、政策、流程以及华为商业行为准则的要求。员工有履行其职责必备的知识、技能和经验。 华为云作为云服务提供商，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要求和尽职调查。
OFI指南草案AppendixII3	了解您的环境	3. 3. 供应商/承包商/第三方，一个OFI应 3.1 维护由供应商/承包商/第三方提供的具有有效收件人级别协议（SLA）的最新收件人清单。 3.2 确保每个SLA至少包括：提供的收件人详情、保密协议（NDA）、各方的角色和责任、期限、供应商收件人级别经理、服务质量指标/评价标准以及审计权条款。 3.3 审核其供应商/承包商/第三方，以确保/执行对服务水平协议的遵守；并及时确定有风险的一方；如果可能，访问其办公室/IT处理设施。 3.4 评估其供应商/承包商/第三方分配给他们的供应商工作人员的资格、技能和/或经验。	

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix III 4	了解您的环境	4.关于外部连接，DMB/PSP应： 4.1识别并记录与第三方（提供增值服务(VAS)的批发客户、供应商和交换机）的所有连接；每个连接的目标应记录在案并定期审查。 4.2适当地评估、记录和降低与已识别的外部连接相关的所有风险。 4.3在适用的情况下，访问第三方的数据中心和网络基础设施；访问他们批准的网络安全政策，并确保其解决所有网络安全问题。 4.4确保第三方访问仅限于网络的授权段；仅允许来自第三方的特定IP地址，并将连接限制在一段时间内（如适用）。 4.5始终记录、监控和审查其网络的所有第三方连接。	金融机构应识别、记录与第三方的所有连接，对第三方的访问进行授权管理，确保第三方访问仅限于网络授权段，并定期审查。 华为云提供**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。 华为云作为云服务提供商，通过**虚拟私有云（Virtual Private Cloud，简称VPC）**对云端数据实施隔离，VPC 采用网络隔离技术，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：一方面，结合VPN或云专线，将VPC与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用VPC的ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。 在网络边界防护方面，华为云建立了 稳固、完善的边界和多层立体的安全 防护系统，部署了Anti-DDoS、IDS/ IPS、WAF等防护机制。Anti-DDoS快速发现和防护DDoS攻击，实时对流量型攻击和应用层攻击进行全面防护；WAF实时检测和防御Web攻击，对高危攻击进行告警并立刻自动阻断；IDS/IPS实时检测和阻断来自互联网的 网络攻击、监控主机异常行为等。
OFI指南草案AppendixII4	了解您的环境	4.关于外部连接，OFI应： 4.1识别并记录与第三方（提供增值服务(VAS)的批发客户、供应商和交换机）的所有连接，每个连接的目标应记录在案并定期审查。 4.2适当地评估、记录和降低与已识别的外部连接相关的所有风险。 4.3在适用的情况下，访问第三方的数据中心和网络基础设施；访问他们批准的网络安全政策，并确保其解决所有网络安全问题。 4.4确保第三方访问仅限于网络的授权段；仅允许来自第三方的特定IP地址，并将连接限制在一段时间内（如适用）。 4.5始终记录、监控并审查其网络的所有第三方连接。	

6.2.2 增强网络安全弹性

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix IV 1	增强网络安全弹性	1.关于访问控制，DMB/PSP应建立访问控制政策，以确保： a.存在机制、标准和程序来规范管理用户、系统和服务帐户对所有系统、网络和应用程序的访问配置、标识和授权。 b.所有工作站/笔记本电脑、最终用户、服务帐户、网络设备（内部和外部）以及管理员都拥有访问银行资源的身份和凭证。 c.任何时候对其信息资产（包括客户信息）、资源和连接的服务/设施的访问仅限于基于最小权限原则，并以访问控制矩阵为指导，仅限于对用户、服务、流程或设备（包括无线网络）进行授权。 d.授予用户、服务和系统帐户的授权仅限于其提供的功能/服务；必要时实施登录时间和天数限制。 e.根据资产处理、存储和传输的信息的重要性和敏感性来控制对资产的物理访问。 f.所有用户、管理员和系统身份和凭证的存储库都受到保护。	金融机构应建立访问控制政策，设定与职责匹配的用户权限，采用安全的身份认证和数据加密技术，并通过日志对用户访问进行记录。 华为云作为云服务提供商，为配合客户满足监管要求： （1）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。每一位华为云客户在华为云都拥有唯一可辨识的用户ID，此外，华为云还提供多种用户身份验证机制，包括账号密码、多因素认证等。 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。 （2）针对于客户个人数据，华为云广泛采用加密技术对客户个人数据进行加密存储和传输，确保个人数据存储和传输中的安全； 如果客户的业务数据中涉及敏感个人数据，云服务将默认加密存储该等数据（可选），在非信任网络之间的传输的数据都是被加密的。 同时，华为云提供**数据库安全服务（Database Security Service，简称DBSS）**，可使用此服务对个人数据存储的数据库进行安全防护，包括数据库安全审计和数据库安全防护两大功能模块，提供数据库审计、数据泄露保护、数据库防火墙三大功能，全面保障云上数据库安全和资产安全。

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案 AppendixIII1	增强网络安全弹性	1.关于访问控制，OFI应建立访问控制政策，以确保： a.存在机制、标准和程序来规范管理用户、系统和服务帐户对所有系统、网络和应用程序的访问配置、标识和授权。 b.所有工作站/笔记本电脑、最终用户、服务帐户、网络设备（内部和外部）以及管理员都拥有访问银行资源的身份和凭证。 c.任何时候对其信息资产（包括客户信息）、资源和连接的服务/设施的访问仅限于基于最小权限原则，并以访问控制矩阵为指导，仅权限限于对用户、服务、流程或设备（包括无线网络）进行授权。 d.授予用户、服务和系统帐户的授权仅限于其提供的功能/服务；必要时实施登录时间和天数限制。 e.根据资产处理、存储和传输的信息的重要性和敏感性来控制对资产的物理访问。 f.所有用户、管理员以及系统身份和凭证的存储库都受到保护。	

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix IV 2	增强网络安全弹性	2.安全系统配置管理： 为了通过系统配置增强弹性，DMB/PSP应： a.获取和部署具有内置弹性配置的系统/应用程序。 b.开发最低安全基线配置，例如反恶意软件；数据丢失预防解决方案；工作站/笔记本电脑、服务器、应用程序/软件（包括供应商建议、附录V中的参考资料和CBN指南中所管理的网络设备）的系统安全设置。 c.设计机制以在系统、应用程序和网络设备上合理应用和维护其网络安全政策和安全基线配置。 d.为所有IT流程和活动建立标准操作程序(SOP)。 e.审核系统和网络设备上的安全配置项，确保符合预配置的安全设置。 f.设计一种机制来监控、检测、记录和报告所有未经授权的系统配置更改；在可能的情况下，该机制应无缝地重新应用安全配置。	金融机构应制定最低安全基线配置，并且监控、监测、记录和报告所有未经授权的系统配置更改。 金融机构可通过**企业主机安全服务（HSS）**，进行基线检查、监测恶意程序等。HSS是服务器的贴身安全管家，提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为或通过《华为云安全基线配置指南》对云服务的安全基线进行检查和配置。 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。

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案AppendixIII2	增强网络安全弹性	2.安全系统配置管理：为了通过系统配置增强弹性，OFI应该： a.获取和部署具有内置弹性配置的系统/应用程序。 b.开发最低安全基线配置，例如反恶意软件；数据丢失预防解决方案；工作站/笔记本电脑、服务器、应用程序/软件（包括受供应商建议、附录IV中的信息参考和CBN指南管理的网络设备）的系统安全设置。 c.设计机制以在系统、应用程序和网络设备上合理应用和维护其网络安全策略和安全基线配置。 d.为所有IT流程和活动建立标准操作程序(SOP)。 e.审核系统和网络设备上的安全配置项，以确保符合预先配置的安全设置。 f.设计一种机制来监控、检测、记录和报告所有未经授权的系统配置更改；在可能的情况下，该机制应无缝地重新应用安全配置。	

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix IV 4	增强网络安全弹性	4.数据丢失防护： 保护和控制企业网络内外客户个人身份信息(PII)和银行敏感和关键信息的可访问性和使用是网络安全弹性的主要目标。因此， a.DMB/PSP应制定数据丢失/泄漏预防策略，以发现、监控和保护端点、存储、网络和其他数字商店（无论是在线还是离线）的敏感、机密的业务和客户数据/信息。 b.该战略应提供但不限于以下机制： i.对结构化和非结构化数据/信息进行分类； ii.发现敏感/机密数据/信息的存储位置； iii.监控敏感/机密数据/信息的使用情况； iv.无论端点是否打开/关闭公司网络，都可以持续保护数据； v.解决通过USB、电子邮件、手机和网络引起的显着数据丢失问题； vi.当怀疑或检测到潜在的数据泄露时立即采取行动：例如阻止员工尝试将敏感信息保存到外部存储或网络共享驱动器；和 vii.建立管理以降低机构中的数据丢失风险。 c.资产的关键和敏感信息应在整个搬迁、转移和处置过程中得到正式管理。所有确定要处理的资产都应根据其批准的政策进行消磁和/或完全销毁。 d.DMB/PSP应验证供应商管理的设施（例如托管数据中心和云服务提供商）是否存在类似的控制。	金融机构应制定数据防丢失策略，包括对数据分类策略，数据识别与监测策略，数据迁移策略，资产销毁策略，并验证供应商是否有类似的策略。 在华为云的责任共担模型中，无论使用哪一项华为云服务，租户始终是其数据的所有者和控制者。租户负责各项具体的数据安全配置，对其保密性、完整性、可用性以及数据访问的身份验证和鉴权进行有效保障。 华为云提供**数据安全中心（Data Security Center，简称DSC）**，DSC是新一代的云原生数据安全平台，提供数据分类分级，数据安全风险识别，数据水印溯源，数据脱敏等基础数据安全能力。客户可通过DSC整合数据安全生命周期各阶段状态，构建云服务全景图，保护数据采集、存储/传输、使用、交换/销毁的安全。 同时，华为云提供提供**数据库安全服务（DBSS）**，DBSS是一款智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能。客户可通过DBSS检测潜在风险，保障云上数据库的安全。 华为云作为云服务提供商，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、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，为用户提供最切实有效的数据保护能力，保证租户对其数据的隐私权、所有权和控制权不受侵犯。 华为云使用多种隐私保护平台工具，帮助华为云更快速、系统、高效地处理与隐私保护相关的各项工作。

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案4.1	增强网络安全弹性	4.数据丢失防护： 保护和控制企业网络内外敏感和关键信息的可访问性和使用是网络安全弹性的主要目标。因此， a.OFIs应制定数据丢失/泄漏预防策略，以发现、监控和保护端点、存储、网络和其他数字商店（无论是在线还是离线）的敏感、机密的业务和客户数据/信息。 b.该战略应提供但不限于以下机制： i.对结构化和非结构化数据/信息进行分类； ii.发现敏感/机密数据/信息的存储位置； iii.监控敏感/机密数据/信息的使用情况； iv.无论端点是否打开/关闭公司网络，都可以持续保护数据； v.解决通过USB、电子邮件、手机和网络引起的显着数据丢失问题； vi.当怀疑或检测到潜在的数据泄露时立即采取行动：通过弹出警告消息、加密或阻止该行动来教育员工；和 vii.建立管理以降低机构中的数据丢失风险 c.资产的关键和敏感信息应在整个搬迁、转移和处置过程中得到正式管理。所有确定要处置的资产都应根据其批准的政策进行消磁和/或完全销毁。 d.OFI应验证供应商管理的设施（例如托管数据中心和云服务提供商）是否存在类似的控制。	**数据发现和管理：**数据发现工具可以帮助华为云识别系统、数据库或者文件里的个人数据，以了解业务是否包含个人数据以及个人数据的类型和流转情况等相关的信息，同时也可以帮助华为云采取恰当的隐私保护措施。数据管理服务可以帮助华为云完成数据资产注册和管理，对个人数据清单的记录、全生命周期管理提供工具化的能力。 **隐私风险分析：**将隐私保护风险分析全过程工具化，可帮助各个业务团队通过标准化的流程和工具识别隐私保护风险并制定和实施相应的风险处置措施。 **加密数据防泄漏：**华为云广泛采用加密技术对客户个人数据进行加密存储和传输，确保个人数据存储和传输中的安全。 **数据删除：**华为云制定了介质管理流程，确保存储在介质中的数据的安全。 当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。 实现方式如下：当客户确认删除操作后，华为云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。 **内部管理：**为了保证华为云平台以及网络的安全、稳定运行，华为云内部采取了一系列管理措施，包括：漏洞分析和处理，日志监控和事件响应、云产品默认安全配置优化、安全补丁部署、防病毒软件部署以及定期备份系统和设备配置文件并测试其有效性。

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix IV 5	增强网络安全弹性	5.系统生命周期管理：在管理系统生命周期时，DMB/PSP应： a.建立持续监督应用程序、组件和系统的生命周期（识别、获取/开发、维护/更新和处置）的政策和程序。 b.确保在系统/应用程序生命周期的所有阶段都考虑并纳入网络安全控制。获取/开发系统/应用程序的业务需求也应识别和记录安全需求。这包括但不限于访问控制、访问权限管理、身份验证、事件记录、审计跟踪、用户会话管理、职责分离和最小权限等。 c.在部署之前验证系统/应用程序是否满足所有其他要求（功能、性能、可靠性等）和任何适用的CBN法规。 d.确保所有内部应用程序的开发符合安全编码实践，例如威胁建模、输入验证、最小权限、深度防御和故障安全，同时缓解OWASP漏洞。这些应用程序还应由合格的软件测试人员和业务/应用程序所有者组成的团队进行彻底测试。 e.将生产/实时环境与开发和测试环境分开。 f.通过实施数据屏蔽解决方案来屏蔽/制造银行和客户的敏感信息，以用于开发、系统和用户验收测试，从而在开发和测试环境中清理敏感数据。 g.建立维护现场和远程组织资产的程序，以防止未经授权的访问。 h.采用加密控制，例如公钥基础设施、散列和加密，以保护机密和敏感信息免受未经授权的访问。 I.遵守信用卡计划的现行规则及相关利益相关者规则	金融机构应建立持续监督应用程序、组件和系统的生命周期的政策和程序，并确保在所有阶段纳入网络安全控制；部署之前应验证是否满足功能、性能、可靠性或其他的法规要求，并确保所有的内部应用程序的开发符合安全编码实践；生产、开发、测试环境应分开，访问需控制，开发与测试环境中不能有敏感数据；数据应加密。 作为云服务提供商： （1）华为云构筑多维全栈的安全防护体系和高可用、高可信的云服务。同时，云服务特有的持续集成，持续交付，持续部署需要全新思维、方法论、流程和工具链。通过结合华为在安全上的长期积累和华为云的现状，华为云不仅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。 （2）华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。威胁分析使用的引导分析威胁库、消减库、安全设计方案库来源于包括传统领域产品和新的云领域所有产品的安全积累和业界优秀实践。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。 （3）华为云严格遵从华为对内发布的安全编码规范，要求服务研发和测试人员在上岗前均需通

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案 AppendixIII5	增强网络安全弹性	5、系统生命周期管理： 在管理系统的生命周期时，OFI应： a.建立持续监督应用程序、组件和系统的生命周期（识别、获取/开发、维护/更新和处置）的政策和程序。 b.确保在系统/应用程序生命周期的所有阶段都考虑并纳入网络安全控制。获取/开发系统/应用程序的业务需求也应识别和记录安全需求。这包括但不限于访问控制、访问权限管理、身份验证、事件记录、审计跟踪、用户会话管理、职责分离和最小权限等。 c.在部署之前验证系统/应用程序是否满足所有其他要求（功能、性能、可靠性等）和任何适用的CBN法规。 d.确保所有内部应用程序的开发符合安全编码实践，例如威胁建模、输入验证、最小权限、故障拒绝、深度防御和故障安全，同时缓解OWASP漏洞。这些应用程序还应由一组独立的软件测试人员和业务/应用程序所有者进行彻底测试。 e.将生产/实时环境与开发/测试环境分开。 f.建立维护现场和远程组织资产的程序，以防止未经授权的访问。 g.采用加密控制，例如公钥基础设施、散列和加密，以保护机密和敏感信息免受未经授权的访问。	过了对应规范的学习和考试。其次，华为云引入了静态代码扫描工具进行每日检查，其结果数据将导入云服务持续集成和持续部署（CI/CD-Continuous Integration，Continuous Deployment）工具链，通过质量门限进行控制，以评估云服务产品的质量。最后，所有云服务在发布在前均需完成静态代码扫描的告警清零，确保服务上线时不存在编码相关的安全问题。 （4）为了确保华为云服务的安全性，所有云服务在发布前首先将由服务测试团队执行多轮安全测试，包括但不限于 Alpha阶段的认证、鉴权、会话安全等微服务级功能和接口安全测试，Beta阶段的对API和协议的fuzzing测试以及Gamma阶段的数据库安全等专项安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。同时，华为云将利用其对客户安全需求的深入理解与业界安全标准，设计安全检查项、开发配套的安全测试工具。 （5）华为云广泛采用加密技术对客户个人数据进行加密存储和传输，确保个人数据存储和传输中的安全。华为云建议租户对要上云的重要数据进行加密存储，防止泄露。数据需要删除时，通过直接删除相关数据加密密钥，防止数据在被彻底删除前被恢复为明文后造成泄露。华为云提供**数据加密服务（Data Encryption Workshop，简称DEW）**，DEW是一个综合的云上数据加密服务，帮助客户实现数据加密存储。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。

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix IV 6	增强网络安全弹性	6.漏洞管理：IT漏洞管理是风险管理的一个组成部分。为此，DMB/PSP应迅速识别其IT基础设施（数据库、应用程序、网络等）、帐户配置文件（系统管理员和特权用户）、供应商等中的弱点。 a.信息资产：为及时识别运营和IT资产的所有系统漏洞和网络安全风险，DMB/PSP应： i.实施经执行管理层批准的漏洞管理政策； ii.建立自动化机制来检测其资产中的所有漏洞，这包括但不限于工作站、网络设备、服务器（生产、测试和开发）等。漏洞和威胁应记录在案；潜在的业务影响和可能性应被识别。 iii.至少每季度或在银行的信息处理基础设施发生重大变化（例如安装新系统、设备、应用程序等）或已知漏洞时进行漏洞评估。 iv.通过聘请该领域的专业人员每年进行渗透测试(PT)，以进一步识别其资产中的漏洞。但是，PT应经常在面向互联网的系统/应用程序上进行。 v.持续识别与用于商业服务的IT平台/协议相关的固有风险和漏洞，例如USSD和SMS移动银行协议。 vi.根据问题的严重性、可能性和影响，及时对漏洞评估过程中发现的问题进行分类和解决；还应进行后续验证以评估此类漏洞的关闭情况；还应解决已识别漏洞的根本原因，例如安全策略缺陷、系统配置错误、不一致的标准操作程序(SOP)、不遵守变更管理流程以及表面	金融机构应制定并实施漏洞管理政策，建立自动化的机制持续监测、分析与评估、记录漏洞，根据漏洞的等级以及风险等级进行分类和解决，直到漏洞关闭。 金融机构应每年聘请网络安全专业人员进行渗透测试；应制定安全补丁管理流程。 华为云提供**漏洞扫描服务（Vulnerability Scan Service，简称VSS）**，VSS是一款多维度的安全检测服务，具有Web漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测五大核心功能。客户可通过VSS可自动识别网站或服务器暴露在网络中的安全威胁，从而保护数据的完整性。 同时，华为云提供**态势感知（Situation Awareness，简称SA）**帮助客户进行漏洞管理，通过实时获取业界热点安全漏洞讯息，同步主机漏洞扫描和网站漏洞扫描结果，全面掌握云上资产漏洞风险状况，并提供相应漏洞修复建议。结合大数据分析、高准确度的威胁情报库，“实时监控”云上威胁，分析威胁攻击情况，及时提供告警通知，并可针对典型威胁事件预置响应策略。 华为云作为云服务提供商： 华为产品安全事件响应团队（PSIRT -product Security Incident Response Team）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完善的漏洞感知、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

原文编号	控制域	具体控制要求	华为云的应答
		风险评估，以阻止未来发生。 vii.建立一个专门的团队来监控其供应商/OEM发布的安全补丁/更新。安全更新是强制性的，应根据DMB和PSP的补丁管理政策快速部署。对已知漏洞或零日漏洞也应按照其紧急补丁管理流程迅速进行补丁。 viii.建立有效的机制和流程来识别资产补丁的合规状态——在用户的笔记本电脑和台式机、服务器（包括DMZ上的服务器）、虚拟机等上的操作系统和应用软件——并修复补丁缺陷。	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。 华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，此系统会自动接收来自PSIRT、在线扫描工具等众多漏洞收集渠道提交的漏洞，并自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复SLA要求。对于重大安全漏洞，安全运维团队可通过自研工具，对现网进行扫描，实现分钟级的受影响服务和模块的范围界定；同时安全运维团队会根据现网情况，采取必要的漏洞缓解措施，例如限制端口访问、实施WAF漏洞规则等方式对受影响的服务进行防护或隔离，以降低漏洞被利用的风险。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。同时，华为云还持续更新操作系统及容器镜像，通过镜像和容器的滚动升级完成系统漏洞修复，不会对租户业务造成影响。

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案AppendixIII6	增强网络安全弹性	6、漏洞管理： OFI应迅速识别其IT基础设施（资产）、帐户配置文件（系统管理员和特权用户）和供应商中的潜在弱点。 a.信息资产： 为及时识别运营和IT资产的所有系统漏洞和网络安全风险，OFI应： i.实施经董事会批准的漏洞管理策略。 ii.建立自动化机制来检测其资产中的所有漏洞。这个包括但不限于工作站、网络设备、服务器（生产、测试和开发）等。应记录漏洞和威胁：还应识别潜在的业务影响和可能性。 iii.至少每季度或在银行的信息处理基础设施发生重大变化（例如安装新系统、设备、应用程序等）或已知漏洞时进行漏洞评估。 iv.通过聘请该领域的专业人员进行渗透测试(PT)，进一步识别其资产中的漏洞。PT应经常在面向互联网的系统/应用程序上进行。 V.持续识别与用于业务服务的IT平台/协议相关的固有风险和漏洞，例如USSD和SMS移动银行协议 vi.根据问题的严重性、可能性和影响，及时对漏洞评估过程中发现的问题进行分类和解决；还应进行后续验证以评估此类漏洞的关闭情况；还应解决已识别漏洞的来源，例如安全策略缺陷、系统配置错误、不一致的标准操作程序(SOP)、不遵守变更管理流程和表面风险评估，以阻止未来发生。 vii.拥有一个专门的团队，不断监控其供应商/OEM发布的安全补丁/更新。安全更新是强制性的，应根据DMB和	

原文编号	控制域	具体控制要求	华为云的应答
		PSP的补丁管理政策快速部署。针对已知或零日漏洞也应根据其紧急补丁管理流程快速进行补丁。 viii.建立有效的机制和流程来识别资产补丁的合规状态-用户笔记本电脑和台式机、服务器（包括DMZ上的服务器）、虚拟机等上的操作系统和应用软件-并修复补丁不足之处。	
DMB和PSP指南Appendix IV 6	增强网络安全弹性	b.系统管理员和特权帐户：为限制威胁在内部暴露，DMB/PSP应： i.识别在每个系统、应用程序、数据库和设备上具有超级权限的所有员工和系统/服务帐户；并对这些账户实施职责分离和最小特权原则。 ii.在适用的情况下，还要对这些帐户强制执行密码、帐户管理政策和实践。使用共享默认/匿名特权帐户是高度禁止的。 iii.确保没有一个管理员可以不受限制地访问其关键系统。关键系统、应用程序和网络的登录凭据应由至少2名不同的员工创建并单独记录。 iv.在资产接入网络前，需要更改默认系统帐户的登录，这适用于测试和开发服务器。 v.建立策略、机制和智能程序来记录、监控、审计这些帐户的执行操作。所有日志/审计跟踪应根据每个机构的账户管理政策保存和定期审查。	金融机构应识别每个系统、应用程序、数据库和设备上具有超级权限的所有员工和系统/服务帐户；并对这些账户实施职责分离和最小特权原则，并审计账户的操作。 华为云作为云服务提供商： （1）为保证平台安全，华为云对主机操作系统进行最小化裁剪并对服务做安全加固。同时，对接入主机操作系统的华为云管理员执行严格的权限访问控制(PAM – Privilege Access Management)，对其所执行的各项运维运营操作实行全面的日志审计。华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。 （2）提供**统一身份认证（Identity and Access Management，简称IAM）**，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用IAM可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。 （3）提供**云审计服务（CTS）**，可对各种云资源操作记录的收集、存储和查询功能，

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案 Appendix III 6	增强网络安全弹性	b.系统管理员和特权帐户：为限制威胁在内部暴露，OFI应该： i.识别在每个系统、应用程序、数据库和设备上具有超级权限的所有员工和系统/服务帐户，并对这些账户实施职责分离和最小特权原则。 ii.在适用的情况下，还要对这些帐户强制执行密码、帐户管理政策和实践。高度禁止多个用户使用共享默认/匿名特权帐户。 iii.确保没有一个管理员可以不受限制地访问其关键系统。关键系统、应用程序和网络的登录凭据应由至少2名不同的员工创建并单独记录。 iv.在资产连接到网络之前，更改资产默认系统帐户的登录凭据，这也适用于测试和开发服务器。 v.建立策略、机制和智能程序来记录、监控和审计这些帐户执行的操作。所有日志/审计跟踪都应根据每个机构的账户管理政策进行保存和定期审查。	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。
DMB和PSP指南 Appendix IV 6	增强网络安全弹性	c.供应商： DMB/PSP应确保： i.没有供应商可以不受限制地访问其系统、数据库、网络和应用程序（尤其是核心应用程序）。 ii.如果供应商需要访问其信息资产，则应仅在需要访问期间寻求管理层的批准，此类访问应由授权管理员进行管理。 iii.任何已登录其信息资产的供应商均不得无人看管。他们的行为应被记录并随时密切监控。如果可能，在所有供应商员工获得访问权限之前对其进行背景调查。	金融机构应建立供应商访问其系统、数据库、网络和应用程序的程序，访问需批准与授权，访问时进行监控。 华为云作为云服务提供商，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。

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案 AppendixIII6	增强网络安全弹性	c.供应商：OFI应确保： i.没有供应商可以不受限制地访问其系统、数据库、网络和应用程序（尤其是核心应用程序）。 ii.如果供应商需要访问其信息资产，则应寻求管理层的批准，并且此类访问应由授权的管理员进行管理。 iii.任何已登录其信息资产的供应商均不得无人看管。他们的行为应被记录并随时密切监控。如果可能，在所有供应商员工获得访问权限之前对其进行背景调查。	

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix IV 8	增强网络安全弹性	7.持续安全监控： 应持续了解信息安全漏洞和威胁，以支持DMB/PSP风险管理决策。为改进监督，应： a.确定需要监控的内容：收集有关支持业务活动的所有系统、数据库和网络的信息；分析有关过去发生的网络事件的报告；评估来自近期内部和第三方审计/网络风险评估的建议；网络安全自我评估报告。 c.为这些变量确定适当的绩效指标；这包括但不限于技能、系统可用性、要监控的系统的事件记录能力等。 d.确定如何存储和保护从各种来源收集的日志数据。 e.定义持续的安全监控政策/策略；它应包括但不限于已识别的系统和流程、关键因变量及其性能指标、角色和职责、保留日志数据的持续时间、将触发这些系统发送警报的事件、监控间隔/频率以及如何控制、处理、记录和报告已确定的网络事件/违规行为。 f.确定已识别系统的用户、系统和网络的操作基线和预期数据流。这包括但不限于登录时间、网络流量阈值、处理器利用率等。 h.建立非侵入式实时监控机制，及时收集、关联和检测关键系统、数据库和网络上的异常用户、管理员、系统和进程/服务活动，同时验证保护措施的有效性. i.确保该机制提供增值服务(VAS)，例如将真实事件与非影响事件（误报）分离，定位和控制事件、向适当的工作人员发送警报以进行调查、补救、报告、保留历史	金融机构应制定并审查灾难恢复和业务连续性计划文件，采用自动检测工具及早发现网络事件。 华为云提供如下四种产品，帮助金融机构持续安全监控： （1）**企业主机安全（HSS）**提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。 （2）华为云提供**云防火墙（Cloud Firewall，简称CFW）**，CFW是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，支持按需弹性扩容，是为用户业务上云提供网络安全防护的基础服务。其具体安全功能包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等功能特性。入侵检测与防御IPS功能，针对开放公网访问的资产，能够自动识别威胁暴露面，并支持一键开启防护，集成华为全网威胁漏洞库，实现智能精准防护。 （3）**态势感知（SA）**是华为云安全管理与态势分析平台。能够检测出超过20大类的云上安全威胁，包括DDoS攻击、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全态势。 （4）**威胁检测服务（Managed Threat Detection，简称MTD）**，通过接入目标区域中用户在华为云操作所产生的的IAM日志、DNS日志、CTS日志、OBS日志、VPC日志，持续检测日志中访问者的IP或域名是否存在潜在的恶意活动和未经授权行为，发现异常将及时告警。此服务集成了AI智能引擎、威胁

原文编号	控制域	具体控制要求	华为云的应答
		数据以进行取证和管理运营风险。 J.监控资产所在物理环境(服务器机房、网络设备、数据中心、灾备站点、非站点存储位置)，及时发现潜在威胁。 k.建立有效、高效的入侵检测机制，对所有系统(包括DMZ区域)的恶意代码和非法移动代码进行检测和修复。对于基于签名的解决方案，更新频率至少为每天一次。 l.有意或拥有云服务提供商的DMB和PSP应以云安全联盟(CSA)的持续安全监控建议为指导。	情报、规则基线三种能力实现威胁检测，智能检测来自多个云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中隐含的异常访问行为，主动发现潜在威胁，对可能存在威胁的访问行为生成告警信息，输出告警结果。用户可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护用户的帐户安全、保障服务稳定运行。 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。通知的信息至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，华为云会根据具体情况向客户提供事件报告。 华为云已制定并实施完善的物理和环境安全防护策略、规程和措施。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以确保华为云数据中心的物理和环境安全。

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案 AppendixIII7	增强网络安全弹性	7.应持续关注信息安全漏洞和威胁，以支持OFI风险管理决策。为改进监督，应： a.确定需要监控的内容：收集有关支持业务活动的所有系统、数据库和网络的信息；分析有关过去发生的网络事件的报告；评估来自近期内部和第三方审计/网络风险评估的建议；网络安全自我评估报告。 c.为这些变量确定适当的绩效指标；这包括但不限于技能、系统可用性、要监控的系统的事件记录能力等。 d,确定如何存储和保护从各种来源收集的日志数据。 e.根据其关键性和对其操作的敏感性，对已识别的需要监控的系统和过程进行分类。 f,制定应由董事会批准的持续安全监控政策/策略；它应包括但不限于已识别的系统和流程、关键因变量及其性能指标、角色和职责、保留日志数据的持续时间、将触发这些系统发送警报的事件、监控间隔/频率以及如何控制、处理、记录和报告已确定的网络事件/违规行为。 g,确定已识别系统的用户、系统和网络的操作基线和预期数据流。这包括但不限于登录时间、网络流量阈值、处理器利用率等。 i.建立非侵入式实时监控机制，及时收集、关联和检测系统、数据库、网络上的异常用户、管理员、系统和进程/服务活动，同时验证保护措施的有效性。 j.确保该机制提供增值服务(VAS)，例如将真实事件与非影响事件（误报）分离、定位和控制事件、向适当的工作人员发送警报以进行调	华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划，并定期对其进行测试。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。 华为云还制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。 华为于2012年加入CSA，并于2017年1月升级为执行企业成员。并且，华为云通过了云安全联盟 CSA STAR金牌认证（CSA–Cloud Security Allianc，STAR–Security， Trust & Assurance Registry），该认证在ISO/IEC 27001 的基础上，增加了云安全控制矩阵（CCM–Cloud Control Matrix）和其他安全要求，涵盖了风险治理、数据安全、应用安全、基础设施安全、开发和设计等16个控制领域。取得CSA STAR金牌认证标志着华为云的运营安全管理和技术能

原文编号	控制域	具体控制要求	华为云的应答
		查、补救、报告、保留历史数据以供取证，和管理运营风险。 k.监控资产所在物理环境(服务器机房、网络设备、数据中心、灾备站点、非站点存储位置)，及时发现潜在威胁。 l.建立有效、高效的入侵检测机制，对所有系统(包括DMZ区域)的恶意代码和非法移动代码进行检测和修复。对于基于签名的解决方案，更新频率更新频率至少为每天一次。 m.有意或拥有云服务提供商的DMB和PSP应以云安全联盟(CSA)的持续安全监控建议为指导。	力获得了国际权威的认可，其安全合规性已处于世界领先水平。

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix IV 1	增强网络安全弹性	8.事件响应(IR): 这是一种有组织的方法来解决和管理安全漏洞或攻击（也称为“事件”）的后果，目的是减少损坏、恢复时间和事件成本。为了有效和高效的事件响应，DMB/PSP应： a.与企业（利益相关者）一起审查其灾难恢复和业务连续性计划文件(DR/BCP)，以确保它们足以有效地支持网络安全弹性。 b.创建DR/BCP测试日历以确定灾难恢复和业务连续性计划的有效性和效率。 c.测试DR/BCP。吸取的经验教训应作为改进纳入DR/BCP文件。 d.与利益相关者一起制定IR政策。投资者关系政策应规定： i.制定网络事件响应计划；经董事会批准； ii.高级管理层和业务流程所有者对所有类别的网络事件的可接受中断窗口(AIW)的定义；IR流程每个阶段的绩效指标； iii.建立一个专注于检测和响应网络事件的专门团队； iv.对IR团队进行充分和持续的培训，了解如何应对、报告网络事件以及进行趋势分析以阻止未来发生； v.根据批准的网络事件响应计划和测试时间表进行网络安全演习，以确定其可行性、有效性和效率； vi.采用自动检测工具，例如网络和系统（端点）扫描仪；来自日志管理解决方案、防火墙、入侵检测/入侵防御系统(ID/IPS)等的警报，以有效地及早发现网络事件；	金融机构应制定并审查灾难恢复和业务连续性计划文件，采用自动检测工具及早发现网络事件。 华为云作为云服务提供商： 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。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。通知的信息至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，华为云会根据具体情况向客户提供事件报告。 华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划，并定期对其进行测试。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。 华为云还制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。 华为云提供**云防火墙（CFW）**，CFW是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，支持按需弹性扩容，是为用户业务上云提供网络安全防护的基础服务。其具体安全功能包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等功能特性。

原文编号	控制域	具体控制要求	华为云的应答
		vii.以合法的方式收集、分析和报告网络事件时的适当监管链；和 viii.如何与包括CBN和公众在内的利益相关者交流和共享危机信息。	

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案AppendixIII8	增强网络安全弹性	8.事件响应(IR)： 这是一种有组织的方法来解决和管理安全漏洞或攻击（也称为“事件”）的后果，目的是减少损害、恢复时间和事件成本。 为了有效和高效的事件响应，OFI应： a.与企业（利益相关者）一起审查其灾难恢复和业务连续性计划文件(DR/BCP)，以确保它们足以有效地支持网络安全弹性。 b.创建DR/BCP测试日历以确定灾难恢复和业务连续性计划的有效性和效率。 c.测试DR/BCP。吸取的经验教训应作为改进纳入DR/BCP文件。 d.与利益相关者一起制定IR政策。投资者关系政策应规定： i.制定网络事件响应计划；经董事会批准； ii.高级管理层和业务流程所有者对所有类别的网络事件的可接受中断窗口(AIW)的定义；IR流程每个阶段的绩效指标； iii.建立一个专注于检测和响应网络事件的专门团队； iv.对IR团队进行充分和持续的培训，了解如何应对、报告网络事件以及进行趋势分析以阻止未来发生； v.根据批准的网络事件响应计划和测试时间表进行网络安全演习，以确定其可行性、有效性和效率； vi.采用自动检测工具，例如网络和系统（端点）扫描仪；来自日志管理解决方案、防火墙、入侵检测/入侵防御系统(ID/IPS)等的警报，以有效地及早发现网络事件；	

原文编号	控制域	具体控制要求	华为云的应答
		vii.以合法的方式收集、分析和报告网络事件时的适当监管链；和 viii.如何与包括CBN和公众在内的利益相关者交流和共享危机信息。	

6.3 网络威胁情报

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南4	网络威胁情报	基于事实拥有对所有新兴威胁、网络攻击、攻击向量、攻击/损害其信息资产的机制和指标的客观知识，这些知识应用于做出明智的决策。 为此，DMB和PSP必须： 4.3.1.建立网络威胁情报(CTI)计划，该计划应主动识别、检测和减轻潜在的网络威胁和风险。 4.3.2.制定经董事会批准的CTI政策（作为网络安全政策的一部分），以帮助主动识别新出现的网络威胁、趋势、模式、风险和可能的影响。 4.3.3.识别并记录各种CTI来源。详见附录六。 4.3.4.根据CTI计划做出明智的决定，因为它提供了有关易受网络攻击、最新威胁、攻击媒介等影响的领域的宝贵信息。决定可能包括：审查自带设备(BYOD)政策；进行应急意识培训、漏洞评估和渗透测试；审查供应商源代码、网络事件响应计划、BCP/DR计划、供应商SLA；并增加系统日志记录等。 4.3.5.在有关当局批准后，使用附录VII中的网络威胁情报报告模板，立即向尼日利亚中央银行银行监管总监报告对其信息资产的所有迫在眉睫和具有挑战性的网络威胁。	金融机构应建立威胁情报计划，主动识别、检测和减轻潜在的网络威胁和风险，并向监管部门报告。 华为云提供**威胁检测服务（Managed Threat Detection，简称MTD）**，此服务集成了AI智能引擎、威胁情报、规则基线三种能力实现威胁检测，智能检测来自多个云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中隐含的异常访问行为，主动发现潜在威胁，对可能存在威胁的访问行为生成告警信息，输出告警结果。用户可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护用户的帐户安全、保障服务稳定运行。

原文编号	控制域	具体控制要求	华为云的应答
OFI指南草案6	网络威胁情报	要求OFI拥有基于事实的客观知识，包括新出现的威胁、网络攻击、攻击向量、攻击/损害其信息资产的机制和指标，这些知识应用于做出明智的决策。为此，OFI必须： 6.1建立网络威胁情报(CTI)计划，该计划应主动识别、检测和减轻潜在的网络威胁和风险。 6.2制定经董事会批准的CTI政策（作为网络安全政策的一部分），以帮助主动识别新出现的网络威胁、趋势、模式、风险和可能的影响。 6.3识别并记录各种CTI来源。详见附录五。 6.4根据CTI计划做出明智的决定，因为它提供了有关易受网络攻击、最新威胁、攻击媒介等影响的领域的宝贵信息。决定可能包括：进行应急意识培训、漏洞评估和渗透测试；审查供应商源代码、网络事件响应计划。业务连续性/灾难恢复计划(BCP/DRP)、供应商服务水平协议(SLA)；并增加系统日志记录、查看自带设备(BYOD)政策等。 6.5使用附录I中的网络威胁情报报告模板，立即向尼日利亚中央银行其他金融机构监管部主任报告对其信息资产的所有潜在网络威胁。	

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南Appendix VI、OFI指南草案Appendix V	网络威胁情报来源	内部威胁情报 (TI) 来源 6.安全运营中心（简称“SOC”）不仅应包含复杂的工具，还应配备安全信息和事件管理(SIEM)解决方案，该解决方案汇总来自各种安全源的数据，以提供安全警报的实时分析。在适用的情况下，SOC应能够提供及时的补救服务。 7.为了直观的关联和快速了解银行的安全状况，向SIEM提供的信息还应包括来自网络设备的日志、漏洞评估系统；应用程序和数据库扫描仪；渗透测试工具；IDS/IPS；以及企业防病毒系统。 10.SOC应有详细的记录流程，以对各种类型的网络事件进行分类，并通过业务流程所有者批准的适当响应，以实现操作一致性；识别、分析和报告新出现的威胁；为司法取证收集和保存证据 11.应该有一个容量规划工具/流程来与SOC基础架构(SIEM)存储进行通信，以使SOC团队能够平衡任务工作负载和可用资源。 外部威胁情报 (TI) 来源 1.DMB/PSP/OFI应订阅外部T1提供商，例如来自IT供应商的数据馈送；ngCERT、FS-ISAC、ICS-CERT等情报共享组；其他DMB/PSP和海外金融机构；被通知网络威胁和漏洞的相关机构。 2.由于误报和/或误报警报率高，应谨慎对待开源网络威胁情报源。	金融机构威胁情报来源应包含内部和外部；应建立安全运营中心（SOC），包含工具、安全信息和事件管理解决方案。 华为云提供**威胁检测服务（MTD）**，通过接入目标区域中用户在华为云操作所产生的的IAM日志、DNS日志、CTS日志、OBS日志、VPC日志，持续检测日志中访问者的IP或域名是否存在潜在的恶意活动和未经授权行为，发现异常将及时告警。此服务集成了AI智能引擎、威胁情报、规则基线三种能力实现威胁检测，智能检测来自多个云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中隐含的异常访问行为，主动发现潜在威胁，对可能存在威胁的访问行为生成告警信息，输出告警结果。用户可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护用户的帐户安全、保障服务稳定运行。 华为云提供**云监控服务（Cloud Eye，简称CES）**，为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台，帮助用户容量挂历。CES 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。

6.4 指标、监控和报告

原文编号	控制域	具体控制要求	华为云的应答
DMB和PSP指南5.4	指标、监控和报告	5.4.应建立定义报告和沟通渠道的报告流程，以传播与安全相关的材料，例如政策、标准、程序的变化、新的或新出现的威胁和漏洞。	金融机构应定义报告和沟通渠道的报告流程，以传播与安全相关的材料。 华为云作为云服务提供商，制定了事件报告流程，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。通知的信息至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，华为云会根据具体情况向客户提供事件报告。
OFI指南草案7.4	指标、监控和报告	7.4 应建立定义报告和沟通渠道的报告流程，以传播与安全相关的材料，例如政策、标准、程序的变化、新的或正在出现的威胁和漏洞。	

7 结语

本文描述了华为云如何为客户提供遵从尼日利亚金融行业监管要求的云服务，并表明华为云遵守尼日利亚中央银行（CBN）发布的重点监管要求，有助于客户详细了解华为云对尼日利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、构建和部署遵从尼日利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尼日利亚金融行业监管要求的遵从性。

8 历史版本

日期	版本	描述
2022年8月8日	1.0	首次发布