华为云沙特阿拉伯金融行业网络安全遵从性指南

文档版本 1.0

发布日期 2022-07-12

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

随着科技的发展，越来越多的金融机构在逐渐寻求业务转型并希望借助先进的技术以实现服务的持续可用性和敏感数据的有效保护。为了规范金融行业对于信息科技的运用，沙特阿拉伯金融管理局（SAMA）针对沙特阿拉伯金融机构如何进行网络安全管理、信息技术风险管理等方面提出了相关的监管要求。

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。本文将针对沙特阿拉伯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 适用的沙特阿拉伯的金融监管要求简介

沙特阿拉伯金融管理局 (SAMA)： 为沙特阿拉伯王国的中央银行，其职能包括发行货币、监督商业银行、管理外汇储备、促进价格和汇率的稳定，以及确保金融体系的发展和稳健。

SAMA 在2017年5月颁发了《 网络安全框架 》，以使受 SAMA 监管的金融机构能够有效识别和应对与网络安全相关的风险，为金融机构维护信息资产和在线服务的安全提供了指导。

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。
- 外包

  指利用其他服务供应商履行通常全部或部分由金融机构自行履行的职能。
- 客户

  指与华为云达成商业关系的注册用户。
- 供应商

根据外包安排向金融机构提供服务的实体，包括其分支机构。

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系统建设、运营经验，对云服务各项服务的集成、运营、维护进行主动管理，并持续改进。同时，华为云一如既往地确保其基础设施和云服务通过业界认可的独立第三方安全权威组织的测评以及安全认证机构的审核。截至目前为止，华为云已获得众多国际和行业安全合规资质认证，全力保障云服务客户所部署业务的安全与合规。

华为云服务和平台已获得以下认证：

认证	描述
ISO 27001:2013	ISO 27001是一种被广泛使用的国际标准，它规定了信息安全管理体系的要求。基于定期风险评估，该标准提供了一套评估组织信息和客户信息管理体系的方法。
网络安全等级保护	网络安全等级保护是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。
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。
新加坡MTCS Level 3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Level 3等级认证。
ISO 20000-1:2011	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提供商可提供有效的IT服务来满足客户和业务的需求。
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。

ISO 27018:2014	ISO 27018是首个专注于云中个人数据保护的国际行为准则。ISO 27018的通过，表明华为云已拥有完备的个人数据保护管理系统，在数据安全管理方面处于全球领先地位。
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。
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。
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。
TRUCS	可信云服务（TRUCS）是中国公共云领域最权威的认证之一。该认证表明，华为云符合中国最详细的云服务数据和服务保证认证标准。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务提供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	该认证是《网络安全法》生效后中国首个云服务用户数据安全评估机制。华为云第一批通过了这一认证。
工信部云计算服务能力评估	ITSS云计算服务能力评估基于国家标准，如《信息技术云计算云服务运营通用要求》。这是中国第一个云服务/云计算领域的分级评估机制。华为私有云和公有云双双获得云计算服务能力“一级”合规证书，这使华为成为为数不多的“双冠供应商”之一。
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。
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。
国际通用准则CC EAL3+	CC (Common Criteria)认证是一种被高度认可的信息技术产品和系统安全的国际评估标准。华为云FusionSphere已经通过了CC EAL 3+认证，表明华为云软件平台在全球得到高度认可。

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。

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理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与租户的安全责任详情，可参考华为云已发布的**《华为云安全白皮书》**。

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。

5 华为云如何符合《SAMA 网络安全框架》的要求

《SAMA 网络安全框架》为金融机构启动、实施、维护、监控和改进网络安全管理提供了通用原则和目标，该框架涵盖了网络安全领导和治理、网络安全风险管理和合规性、网络安全运营和技术及第三方网络安全四大领域。

沙特阿拉伯金融机构在遵循《SAMA网络安全框架》的要求时，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《SAMA网络安全框架》中与云服务供应商相关的控制要求，并详细阐述了华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

5.1 网络安全领导和治理

《SAMA 网络安全框架》3.1 “安全管理”要求金融机构建立适当的网络安全管理机制，涵盖网络安全政策与程序、意识与培训、角色与责任等网络安全治理领域。相关控制要求及华为云的实践方式如下：

5.1.1 网络安全政策

记录金融机构在网络安全方面的承诺和目标，并将其传达给相关利益相关者。

编号	具体控制要求	华为云的内部实践	客户的职责

1	网络安全政策应该被定义、批准和传达。	华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批，员工可根据授权查看已发布的信息安全政策和程序。同时，华为云针对公司政策、文化等方面每年定期开展员工培训。	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法。
2	网络安全政策应根据预先确定的和结构化的审查程序定期审查。	华为云至少每年审查一次网络安全管理策略和流程，并根据需要予以更新，以反映业务目标或风险环境的变更情况。政策及流程的变更需要获得高级管理层的审批。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议。	客户应根据计划的频率或外部监管的变化定期对网络安全政策和程序进行审查和更新，并保留修订记录。
3	网络安全政策应该是		
b	由详细的安全标准（例如，密码标准、防火墙标准）和程序支持。	华为云参照各类国际、行业标准，法律法规监管要求以及业内的最佳实践，包括但不限于PCI DSS、NIST CSF、CSA CCM等，并结合业务所在地的安全合规要求，建立了一套完善的网络安全政策与程序。	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。
c	基于最佳实践和（国家间）标准。	华为云参照各类国际、行业标准，法律法规监管要求以及业内的最佳实践，包括但不限于PCI DSS、NIST CSF、CSA CCM等，并结合业务所在地的安全合规要求，建立了一套完善的网络安全政策与程序。	客户建立的网络安全政策与程序可参考最佳实践和国际安全标准。
d	与相关的利益相关者进行沟通。	华为云确保网络安全保障体系在各体系、各区域、全流程的实施，积极推动与政府、客户、合作伙伴、员工等各利益相关方的沟通，以确保利益相关方能及时有效地接收到的华为云网络安全有关信息。	客户应与客户的利益相关方进行积极沟通。
4	网络安全政策应包括		
a	网络安全的定义。	华为云制定了网络安全与隐私保护的管理要求，其中明确了网络安全在华为云中的定义及重要程度，将构筑并全面实施端到端的网络安全体系作为重要战略，遵从业务所在地适用的法律法规，全面满足客户的网络安全需求。	客户指定的网络安全政策中应包含网络安全的定义。

c	董事会的意图声明，支持网络安全目标。	华为公司领导层签发关于构筑网络安全保障体系的声明，对华为网络安全战略进行了明确，承诺将公司对网络和义务安全性保障的责任作为公司的重要属性，建立和完善可持续、可信赖的安全保障体系，同时该战略得到公司最高管理层的批准。	客户方的董事会应以明确的方式支持网络安全目标。
d	对网络安全通用职责和具体职责的定义。	在华为公司层面，全球网络安全与用户隐私保护团队GSPC作为最高网络安全管理机构，决策和批准公司总体网络安全战略。GSPO及其办公室负责制定和执行华为端到端网络安全保障体系。华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。同时，华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。沙特网络安全与隐私保护官遵循公司最高层面的网络安全战略，并在沙特执行落地。	客户应定义和批准网络安全角色及通用职责，确保各职责间没有利益冲突。
e	对支持网络安全标准和程序的参考。	华为云在遵从所有适用的国家和地区的安全法规政策、国际网络安全和云安全标准，参考行业最佳实践的基础上，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。	网络安全政策与程序可参考业内技术安全标准。

f	网络安全要求，确保 1.信息的分类方式要表明其对金融机构的重要性。 2. 根据网络安全要求，按照风险偏好对信息进行保护。 3.为所有信息资产指定所有者。 4.对信息资产进行网络安全风险评估。 5. 让相关的利益相关者了解网络安全和他们的预期行为（网络安全意识计划）。 6.遵守法规和合同义务。 7.报告网络安全漏洞和可疑的网络安全弱点。 8. 网络安全反映在业务连续性管理中。	华为云遵从所有适用的国家和地区的安全法规政策、国际网络安全和云安全标准，参考行业最佳实践的基础上构建了完善的网络安全管理体系，制定了华为云重点关注的领域及该领域的网络安全要求，其中包括： 1/2/3. 华为云制定了资产管理程序，明确了信息资产的分级定级办法、针对各类资产应遵循的授权规则以及根据不同级别参考组织风险偏好进行不同的保护措施。利用资产管理系统对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。 1. 华为云建立了信息安全风险管理规范，明确风险管理应遵循的关键流程、风险管理范围、风险管理相关责任部门及风险管理中应遵循的标准，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。华为云各业务团队根据要求定期执行信息安全风险评估。 2. 华为云为确保员工的信息安全意识能够符合公司要求建立了一系列的网络安全培训及学习机制，要求员工持续学习网络安全知识，了解相关的政策和制度，了解哪些该做哪些不该做，承诺按要求执行。 3. 华为云在其网络安全策略中明确合规流程，定期识别和记录合规要求。同时，华为云设立了专岗同外部各方保持积极的联系，以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律、法规要求的符合性。 4. 华为云建立了安全漏洞管理流程，规范了华为云系统安全漏洞的预警、评估、修复处理的闭环流程，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估	客户应在其网络安全要求中明确资产管理、网络安全评估、网络安全意识培训、合规性、漏洞管理以及业务连续性的安全要求。

		并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。 5. 华为云已经通过ISO22301业务连续性管理体系标准的认证。华为云每年执行一次业务影响分析和风险评估，识别关键活动及依赖、评估风险等级，并对识别出的可造成云服务资源中断的威胁制定应对策略，形成业务连续性计划。	

5.1.2 网络安全意识

建立网络安全风险意识文化，让金融机构的工作人员、第三方和客户做出基于风险的有效决策，以保护金融机构的信息。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应确定、批准和开展网络安全意识方案，以促进网络安全意识，并创造积极的网络安全文化。	华为云遵循制定的信息安全意识培训计划，在员工在职期间持续对员工的安全意识教育进行培训，培养员工安全意识，以提升全员的网络安全意识，规避网络安全违规风险，创造积极的网络安全文化，保证业务的正常运营。	客户应遵循制定的网络安全意识培训计划，对员工进行安全意识教育培训。
3	网络安全意识计划应针对网络安全行为，通过多种渠道，针对不同的目标群体量身定制计划。	华为云建立了培训机制，以提高员工的信息安全意识，根据不同的角色、岗位为员工设计合适的培训方案。制定了专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。	客户应制定完善的安全意识和技能培训管理机制，通过多种渠道并根据培训对象的职能和角色来制定培训内容。
4	网络安全意识计划的活动应定期和全年进行。	华为云建立了自己的培训机制，根据不同的角色、岗位为员工设计合适的培训方案。其中一般员工的培训频率为至少每年一次，核心岗位员工培训频率更高。新员工在入职后均须参加公司组织的网络安全考试，员工仅能在考试通过后才可以正式转正。针对在职员工，华为公司将网络安全纳入员工行为准则，通过公司统一开展的年度例行学习、考试和绩效考核措施，每半年对内部员工开展一次绩效考核，传递公司对全员在网络安全领域的要求，提高员工网络安全意识。	客户应根据定期开展网络安全意识培训活动。

5	网络安全意识计划至少应包括： a. 对所提供的网络安全措施的解释。 b. 有关网络安全的角色和责任。 c. 有关新出现的网络安全事件和网络威胁的信息（例如，鱼叉式钓鱼、捕鲸）。	华为云为确保员工的信息安全意识能够符合公司要求建立了一系列的网络安全培训及学习机制，要求员工持续学习网络安全知识，了解相关的政策和制度，了解哪些该做哪些不该做，承诺按要求执行；面向全员开展形式多样的网络安全宣传活动，包括网络安全社区运营、网络安全典型案例宣传、网络安全活动周、网络安全动画宣传片等，以提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营。	客户制定的网络安全意识计划应涵盖员工应承担的网络安全责任、最新的网络威胁及如何防范这些威胁。
6	应该对网络安全意识计划进行评估，以便 a. 衡量意识活动的有效性。 b. 制定建议以改善网络安全意识计划。	华为云每年会对建立的人员意识培训计划进行评估审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的评估审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全意识计划的实施情况进行审查。

5.1.3 网络安全培训

确保金融机构的工作人员具备保护金融机构信息资产和履行其网络安全职责所需的技能和知识。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应根据金融机构相关职能领域类别的工作人员的工作描述，向其提供专家或安全相关的技能培训，包括 a. 组织内的关键角色。 b. 网络安全职能部门的工作人员。 c. 参与开发和（技术上）维护信息资产的工作人员。 d. 参与风险评估的工作人员。	华为云建立了自己的培训机制，根据不同的角色、岗位为员工设计合适的培训方案。其中一般员工的培训频率为至少每年一次，核心岗位员工培训频率更高。华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。新员工转正前必须通过有关网络安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试，管理者需参加网络安全必须的培训和研讨。	客户应向直接从事与网络安全相关的人员提供必要的和定制的培训和专业技能组合。

5.2 网络安全风险管理与合规

《SAMA 网络安全框架》3.2 “网络安全风险管理与合规”要求金融机构以系统性方法管理网络安全风险，从网络安全风险评估到网络安全审查与审计多维度的识别和管理网络安全风险，并按照组织政策、程序及相关法律法规保护组织的信息资产。控制要求及华为云的实践方式如下：

5.2.1 网络安全风险管理

确保网络安全风险得到妥善管理，以保护金融机构信息资产的保密性、完整性和可用性，并确保网络安全风险管理流程与金融机构的企业风险管理流程相一致。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应定义、批准和实施网络安全风险管理流程。	华为云建立了信息安全风险管理规范，明确风险管理应遵循的关键流程、风险管理范围、风险管理相关责任部门及风险管理中应遵循的标准，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。	客户应建立符合其组织战略的网络安全风险管理的方法和程序。
2	网络安全风险管理过程应着重于保障信息资产的保密性、完整性和可用性。	华为云制定了信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断，同时根据要求定期执行信息安全风险评估。风险评估涵盖信息安全的各方面，基于业务流程和资产的保密性、完整性和可用性，识别华为云的威胁和漏洞并进行风险评级，对评估进行正式记录并制定风险处置计划。	客户应根据资产的机密性、完整性和可用性，实施其已建立的网络安全风险管理流程。

4	网络安全风险管理过程应该被记录下来，并涉及到。 a. 风险识别 b. 风险分析 c. 风险应对 d. 风险监测和审查	1. 风险管理人员识别各业务场景中所涉及的固有风险，基于华为云面临的威胁和脆弱性进行风险评估；基于固有风险清单，结合已有的风险管控措施，输出残余风险清单，并将风险及时录入风险管理平台，包括风险描述、所属领域、风险等级、风险来源等； 2. 基于业务流程和资产管理情况，华为云相关安全专家根据已识别到的风险的概率和影响对分配风险分析并评级； 3. 对评估进行正式记录并制定风险处置计划。风险评估报告完成后由高级管理层进行审批； 4. 为确保风险管控的有效性并实现持续改进，需定期对风险度量指标进行持续监控，根据度量值管控失效的风险，并纳入风险管理进行持续处置。	客户应遵循网络安全风险管理的流程，对风险识别、分析、应对及监测和审查进行记录。
5	网络安全风险管理过程应涉及金融机构的信息资产。风险管理过程应涉及金融机构的信息资产，包括（但不限于）。 a. 业务流程。 b. 业务应用。 c. 基础设施组件。	华为云的基础设施组件各业务团队，根据要求定期执行信息安全风险评估，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划，并对风险处置计划的实施进行监控。 此外，华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。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。	客户应确保业务流程和业务应用在网络安全风险管理中得到妥善管理。
6	应启动网络安全风险管理过程。 a. 在项目的早期阶段。 b. 在关键变化之前。 c. 在考虑外包的时候。 d. 在推出新产品和技术时。	在项目初期对其进行信息安全风险评估并在整个项目交付过程中定期评审信息安全影响。同时，华为云制定了变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，以确保对组织的运行和安全没有负面影响。	客户应确保在项目的早期阶段，关键变化之前，考虑外包及推出新产品和技术时开展网络安全风险评估，以保证组织信息安全的持续运行。

7	现有的信息资产应根据其分类或风险状况，定期进行网络安全风险评估。	华为云制定的信息安全风险管理规范中明确其网络安全评估范围包括信息资产的安全风险，根据资产的分类及自身可能存在的缺陷或漏洞，定期进行网络安全风险评估识别可能被威胁所利用而导致资产受到损害的风险。	客户应依据资产分类或风险状况，定期进行网络安全风险评估。

5.2.1.1 网络安全风险识别

发现、识别和描述金融机构网络安全风险。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应进行网络安全风险识别。	华为云风险管理人员遵循制定的网络安全风险管理规范，定期执行信息安全风险评估，依据信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。	客户应识别可能存在的网络安全风险。
2	确定的网络安全风险应该被记录下来（在一个中央登记册中）。	华为云定期执行网络安全风险评估，并基于固有风险清单，结合已有的风险管控措施，输出残余风险清单，并将风险及时录入风险管理平台，包括风险描述、所属领域、风险等级、风险来源等。	客户应遵循网络安全风险评估的流程，对组织的资产进行内外部风险的识别，并将已识别的风险记录在中央登记册中。
3	网络安全风险识别应涉及相关的信息资产、威胁、脆弱性和关键的现有网络安全控制。	华为云风险管理人员识别各业务场景中所涉及的网络安全风险，基于华为云相关信息资产面临的威胁和脆弱性进行风险评估。基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。	客户应对信息资产、威胁、脆弱性和关键的现有网络安全控制进行网络安全风险识别。

5.2.1.2 网络安全风险分析

分析和确定已识别的网络安全风险的性质和级别。

编号	具体控制要求	华为云的内部实践	客户的职责

1	应进行网络安全风险分析。	华为云风险管理人员遵循制定的网络安全风险管理规范，基于业务流程和资产管理情况，华为云相关安全专家基于业务流程和资产管理情况，并根据已识别到的漏洞与威胁的发生概率和影响对风险进行分析和评级，对评估进行正式记录并制定风险处置计划。	客户应进行网络安全风险分析。
2	网络安全风险分析应解决潜在业务影响的程度和网络安全威胁事件实现的可能性。	华为云风险管理人员遵循制定的网络安全风险管理规范，基于业务流程和资产管理情况，华为云相关安全专家基于业务流程和资产管理情况，并根据已识别到的漏洞与威胁的发生概率和影响对风险进行分析和评级，对评估进行正式记录并制定风险处置计划。	客户应对网络安全风险分析解决潜在的业务影响的程度和网络安全威胁事件实现的可能性。

5.2.1.3 网络安全风险对策

确保网络安全风险得到处理(即接受、避免、转移或减轻)。

编号	具体控制要求	华为云的内部实践	客户的职责
2	网络安全风险应对措施应确保风险处理方案的清单被记录下来（即接受、避免、转移或通过应用网络安全控制措施减轻风险）。	华为云风险管理人员遵循制定的网络安全风险管理规范，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划，包括整改措施、计划、关键里程碑和风险降级标准，利用风险整改、风险保持、风险避免和风险转移等措施降低和消除风险至可接受范围。	客户应记录网络安全风险的应对措施。

3	接受网络安全风险应包括 a. 考虑对网络安全风险水平的预先定义的限制。 b. 业务负责人的批准和签收，确保 1. 接受的网络安全风险在风险承受能力范围内，并报告给网络安全委员会。 2. 接受的网络安全风险与SAMA的规定不相矛盾。	华为云遵循已制定的网络安全风险管理规范，当风险决策后接受风险，则维持风险现状，不采取进一步控制措施。当业务部门审视，业务选择接受风险，则需要提交到风险管理员进行正式决策过程，审视和决策的结论须同步至风险管理平台。华为云在接受网络安全风险时不会与SAMA的规定相矛盾。	客户应确保能接受网络安全风险在风险承受范围内，并获得业务负责人的批准，且不能与SAMA的规定相矛盾。
4	避免网络安全风险应该是企业主决定取消或推迟某个引入不可接受的网络安全风险的特定活动或项目。	华为云遵循已制定的网络安全风险管理规范，当风险过高或风险整改措施成本过高、业务收益可能超过风险影响时，采取消除风险的方法。	客户应明确避免网络安全风险的方法，如取消或推迟导致网络安全风险的特定活动或项目。
5	转移或共享网络安全风险应。 a. 涉及与相关（内部或外部）提供者分享网络安全风险。 b. 被接受的（内部或外部）提供者所接受。 c. 最终导致网络安全风险的实际转移或共享。	华为云遵循已制定的网络安全风险管理规范，与外部组织共担风险。风险共享不能完全消除风险，只能在一定程度上降低风险带来的经济损失。	客户应明确转移或共享网络安全风险的方法，如与内外部共担风险。

6	应用网络安全控制措施来减轻网络安全风险应包括 a. 确定适当的网络安全控制。 b. 评估网络安全控制的优势和劣势。 1. 评估实施网络安全控制的成本。 2. 评估实施网络安全控制的可行性。 3.审查网络安全控制的相关合规要求。 c. 选择网络安全控制措施。 d. 识别、记录并获得企业主对任何剩余风险的签署。	华为云遵循已制定的网络安全风险管理规范，通过增加新的控制措施或调整现有控制措施的方式使风险降低至可接受范围，具体可采用安全控制策略、流程、技术控制措施、以及采取补偿措施，如安全监控、安全稽核审计和应急预案等。风险接口人在收到风险告知邮件后须输出针对风险的处置方案，由风险与流程专家组对处置方案的优缺点、可行性及合规性等方面进行评审。风险延期或风险接受需要经过华为云相关主管人的决策。	客户应明确减轻网络安全风险的方法，实施网络安全控制，该确实应获得企业主对剩余风险的签署。
7	网络安全风险处理行动应记录在风险处理计划中。	华为云遵循已制定的网络安全风险管理规范，风险接口人输出针对风险的处置方案，包括整改措施、计划、关键里程碑和风险降级标准，利用风险整改、风险保持、风险避免和风险转移等措施降低和消除风险至可接受范围。	客户应将网络安全风险处理的活动记录在风险处理计划中。

5.2.1.4 网络风险监测和审查

确保根据处理计划进行网络安全风险处理。确保修订或新实施的网络安全控制有效。

编号	具体控制要求	华为云的内部实践	客户的职责

1	应监测网络安全处理，包括。 a. 根据处理计划跟踪进展。 b. 选定和商定的网络安全控制正在实施。	华为云各业务团队根据要求定期执行信息安全风险评估，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。为确保风险管控的有效性并实现持续改进，需定期对风险度量指标进行持续监控，根据度量值管控失效的风险，并纳入风险管理进行持续处置。此外，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审。	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。
2	应审查修订新实施的网络安全控制的设计和有效性。	网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审。华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应审查修订新实施的网络安全控制的设计和有效性。

5.2.2 遵守法规

遵守影响金融机构网络安全的法规。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应建立一个程序，确保整个金融机构遵守影响网络安全的相关监管要求。确保合规的过程应 a. 定期或在新的监管要求生效时进行。 b. 涉及金融机构关键领域的代表。 c. 导致网络安全政策、标准和程序的更新，以适应任何必要的变化（如果适用）。	华为云在其网络安全策略中明确合规流程，定期识别和记录合规要求。同时，华为云设立了专岗同外部各方保持积极的联系，以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律、法规要求的符合性。	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。

5.2.3 网络安全审查

确定网络安全控制的设计和实施是否安全，并监测这些控制的有效性。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应定期对关键信息资产进行网络安全审查。	华为云建立了一个正式的、定期的审计计划包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议，同时保留审计记录免受未经授权的访问。	客户应每年至少对关键信息资产进行一次审计，保留和保护审计记录，将审计结果和建议向管理层报告，以确定网络安全控制的合规性和有效性。
2	面向客户和互联网的服务应接受年度审查和渗透测试。	华为云制定了内审管理流程，规范内部审计原则、审计管理流程和审计频率。华为云每年由专门的审计团队执行一次内部审计工作，以检查公司内部控制体系的运行情况，评估策略、规程及配套措施和指标的符合性和有效性。此外，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。	客户应对其面向客户和互联网的服务定期开展年度审查和渗透测试。
3	应记录所进行的网络安全审查的细节，包括审查的结果、发现的问题和建议的行动。	华为云制定了内审管理流程，其中明确要求审计团队须对网络安全审查的过程进行记录，包括但不限于审查计划、审查人员、审查依据、纠正措施、跟踪审核和审核报告等。	客户应确保记录所有进行网络安全审查的细节，包括审查结果、问题和建议。
4	网络安全审查的结果应报告给企业主。	华为云会向最高管理层报告调查的结果和建议。管理层进行审阅并对整改情况进行跟进，保证发现的问题得到解决并最终闭环。	客户应将审查结果和建议提交至企业主。

5	网络安全审查应接受后续审查，以检查。 a. 所有发现的问题都已得到解决。 b. 关键风险已得到有效处理。 c. 所有商定的行动都在持续管理。	网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，评估已识别的网络安全风险，并对风险处置跟进过程进行定期评审。华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应遵循网络安全审查并接受后续审查，以确保所有的问题都已得到解决和关键风险已得到有效处理。

5.2.4 网络安全审计

以合理的把握确定网络安全控制的设计和实施是否安全，以及这些控制的有效性是否受到监控。

编号	具体控制要求	华为云的内部实践	客户的职责
1	网络安全审计应独立进行，并符合公认的审计标准和SAMA网络安全框架。	华为云会定期聘请独立的外部第三方提供外部审计鉴证服务，这些评估员通过执行定期安全评估和合规性审计或检查（例如SOC、ISO标准、PCIDSS审计）来评估信息和资源的安全性、完整性、机密性和可用性，从而对风险管理内容/流程进行独立评估。 华为云会安排专人积极配合客户发起的审计要求。	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SAMA网络安全框架。
2	网络安全审计应根据金融机构的审计手册和审计计划进行。	华为云建立了一个正式的、定期的审计计划包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。 华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	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。

5.3 网络安全业务和技术

《SAMA 网络安全框架》3.3 “网络安全业务和技术”中要求金融机构制定网络安全运营和安全管理的策略及流程，包括资产管理、身份与访问管理、应用安全、密码管理、备份与恢复、网络安全事件管理等方面。相关控制要求及华为云的实践方式如下：

5.3.1 人力资源

确保金融机构工作人员的网络安全责任包含在工作人员协议中，并在其雇佣周期之前和期间对工作人员进行筛选。

编号	具体控制要求	华为云的内部实践	客户的职责
1	人力资源流程应定义、批准和实施网络安全要求。	华为云建立了人员信息安全管理规定，明确了华为云各类员工分层分级的信息安全管理要求，对内外部员工关于招聘、培训、稽核和奖罚等方面的管理进行了规范，明确了员工应遵循的华为云网络安全职责。	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。
2	应监测、衡量和定期评估人力资源程序的有效性。	华为云每年会对建立的人员信息安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	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。
3	人力资源流程应包括		
a	网络安全责任和员工协议中的不披露条款（就业期间和就业后）。	员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的网络安全责任，以确保在入职前对应遵循的保密条款进行确认。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。	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。
b	工作人员应在开始时和就业期间接受网络安全意识。	华为云为确保员工的信息安全意识能够符合公司要求建立了一系列的信息安全培训及学习机制。新员工在入职后均须参加公司组织的信息安全考试，员工仅能在考试通过后才可以正式转正。针对在职员工，在员工在职期间持续进行，华为云每年定期组织信息安全意识培训、信息安全知识宣传。	客户应对定期对在职员工进行网络安全意识培训。

c	何时适用纪律处分。	华为建立了严密的安全责任体系，贯彻违规问责机制。华为云以行为和结果为主要依据对员工进行问责。根据华为云员工安全违规的性质，以及造成的后果确定问责处理等级，分级处理。对触犯法律法规，移送司法机关处理。直接管理者和间接管理者存在管理不力或知情不作为的，须承担管理责任。违规事件处理根据违规个人态度与调查配合情况予以加重或减轻处理。华为云的违规政策供所有员工进行查看学习，并定期组织培训提升员工对违规行为、违规后果、惩罚措施的了解。	客户应对不符合组织网络安全要求的人员实施纪律处分。
d	筛选和背景调查。	人员任用前，华为云通过既定的新进员工背景调查机制对满足特定条件的拟聘员工进行背景审查，同时，在适用法律允许的情况下，华为云会根据可接触的资产的机密性，在聘用员工或外部人员前对其进行背景调查。	客户应在雇佣前对所有职位的候选人进行背景调查进行筛选和审查。
e	离职后的网络安全活动，如： 1. 撤销访问权。 2. 归还分配的信息资产（例如，访问徽章、令牌、移动设备、所有电子和物理信息）。	1. 员工及其他第三方在状态发生变化后，如离职或职位变更后，按照调动、离职安全审查清单，对内部调离、离职人员进行离岗安全审查，包括离岗权限账号的清理或修改。 2. 与合作伙伴合同/业务关系终止时，按照合作协议删除自带设备中在合作项目中产生的信息，并移交华为云提供的资产。华为云建立了人员离职/合作终止时的资产交接电子流，按照电子流程执行资产交接。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。	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。

5.3.2 物理安全

防止未经授权的物理访问金融机构的信息资产，并确保其受到保护。

编号	具体控制要求	华为云的内部实践

1	应确定、批准和实施物理安全程序。	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。华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。
2	应监测、衡量和定期评估物理安全程序的有效性。	华为云定期会对建立的物理安全和环境保护相关的策略和流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
3	物理安全程序应包括（但不限于）。	
a	物理进入控制（包括访客安全）。	华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。
b	监测和监视（例如，闭路电视、自动取款机GPS跟踪、敏感度传感器）。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。
c	数据中心和数据室的保护。	华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流程。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。

d	环境保护。	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，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。 ● 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 – Uninterrupted Power 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：华为云数据中心建筑防火等级均按一级设计施工，使用了 A 级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，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。

e	在生命周期内保护信息资产（包括运输和安全处置，避免未经授权的访问和（非）有意的数据泄漏。	华为云作为金融机构的云服务提供商，华为云已制定并实施介质的管理规定，其中明确： ● 要求包含华为公司保密信息的存储介质必须进行标记。保密数据应依据数据密级进行标记或者贴上标签，须说明其保密级别. 对于运输过程中的介质或授权存放介质的设施外部必须贴标签，对用于运输机介质的上锁容器，其外部也必须贴有标签。 ● 要求存储介质必须保存在受控访问区，或者放置在公司内部上锁的柜子里，存储介质从受控区域出入的时候必须对出库到入库的具体信息对账和闭环跟踪。 ● 对存储组织信息的介质按照其对组织的重要程度实施适当水平的保护，以及防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。 ● 各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对介质清退报废进行分类操作，通过多种方式实现数据清除、磁盘消磁，并对销毁操作进行记录。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。

5.3.3 资产管理

支持金融机构对所有可用信息资产的物理/逻辑位置和相关细节拥有准确和最新的清单和集中了解，以支持其流程，如财务、采购、IT和网络安全流程。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应确定、批准和实施资产管理程序。	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享。	客户应建立正式的资产管理程序，对其资产进行分类，并定义资产所有者。
2	应当对资产管理过程的有效性进行监测、衡量和定期评估。	华为云每年会对建立的资产管理过程进行的定期审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对资产管理过程的有效性进行监测和定期评估。
3	资产管理过程应包括		

a. b.	一个统一的登记册。信息资产的所有权和保管权。	华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。华为云并使用IPAM对IP资源进行统一的管理。同时，华为云平台部署了HSP主机安全平台套件，对平台资产进行网络安全防护。此外，华为云平台部署了HSP主机安全平台套件，对平台资产进行网络安全防护。	客户应建立资产登记册，并为资产分配所有权和保管权。 华为云的企业主机安全（Host Security Service, 简称HSS）为客户提供统一的管理界面，供客户查询并管理云服务，是服务器的贴身安全管家，为客户提供资产管理功能，包括提供账号、端口、进程、Web目录和软件等安全资产信息的管理和分析。
c	根据资产管理情况，参考相关的其他流程。	华为云在进行资产管理过程中遵循华为云制定的其他相关的安全制度。参考总体安全策略，根据资产对业务的重要性和影响程度，对资产进行分级分类，参考网络安全风险管理规范，对不同级别的资产开展风险评估，及早识别资产自身可能存在的缺陷或漏洞被威胁利用而导致资产损害的风险，并依照介质管理规范、数据管理规范、安全事件管理规范中的角色与职责，对资产全生命周期进行保护。	客户应在制定资产管理制度中，参考相关的其他流程。

d	信息资产的分类、标记和处理。	华为云通过资产管理系统（Cloud Asset Management，CAM）实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。同时，华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标记安全等级。	客户应依照法律要求、资产价值、资产对组织的重要性和敏感性标注相应资产的分类。
e	发现新的信息资产。	华为云通过CAM资产管理系统实时监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。此外，华为云利用自动化工具采集物理机、虚拟机、容器、网络设备等组件基础配置信息，如规格、OS相关配置，该工具与配置管理数据库工具（CMDB）对接，将配置信息上报到CMDB，从而确保数据的准确性。	客户应及时发现新的信息资产，维护最新的资产清单。

5.3.4 网络安全架构

支持金融机构实现战略、一致、经济、端到端的网络安全架构。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应定义、批准和实施网络安全架构。	华为云遵循华为公司建立的网络安全管理规定，其中明确了网络隔离、网络接入安全、网络安全防御等相关控制要求，确保组织免受网络恶意入侵造成网络安全风险。	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。

2	应监测对网络安全架构的遵守情况。	华为云每年会对建立的网络管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全架构的遵守情况进行监测。
3	网络安全架构应包括		
a	基于业务要求的网络安全能力和控制的战略纲要。	华为云遵循网络安全管理规定，实施正式的环境隔离机制，华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，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。同时华为云构建了多层防护措施，如使用接入控制和边界防护技术以实现对外来攻击的统筹防护，严格执行相应的管控措施，确保华为云安全。此外，华为云根据业务功能和网络安全风险将其平台划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，提供网络面对外部入侵时的自我保护和容错恢复能力。	客户基于业务需求建立网络安全能力和控制的管理要求。
b	批准确定的网络安全架构。	华为云会维护最新的网络拓扑结构图。华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。	客户应批准确定的网络安全架构，记录网络实际状态的网络拓扑结构。
c	拥有合格的网络安全架构师的要求。	华为的安全技术团队包括全球各地业界优秀的信息安全、产品安全、应用安全、系统安全、网络安全、云服务安全、运维运营安全、隐私保护等方面的专家专才。	客户应要求团队中拥有合格的网络安全架构师。
d	制定网络安全控制和应用网络安全要求的设计原则（即，设计中的安全原则）。	华为云在设计阶段，就从功能架构上考虑解决方案在边界防护中的能力，能够有效应对常见的边界风险。华为云基于业界网络安全的优秀实践以及自身多年积累的丰富经验，对平台进行了安全区域划分，安全区域内部的节点具有相同的安全等级。此外，华为云规范了采用DevOps开发模式的产品/服务在部署和发布阶段流程，当中规范了对环境隔离的相关要求，提高生产环境稳定性。	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。

e	定期审查网络安全架构。	华为云会维护最新的网络拓扑结构图。此外，华为云每年会对建立的网络管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应定期审查其网络安全架构。

5.3.5 身份和访问管理

确保金融机构只向经批准的用户提供授权和足够的访问权限。

编号	具体控制要求	华为云的内部实践	客户的职责
1	身份和访问管理政策，包括责任和问责，应该被定义、批准和实施。	华为云制定了公司用户账号权限管理的要求，规范华为云员工在申请、维护和注销权限时应遵循的流程。此外，针对华为云云平台账号，华为云制定了公有云账号权限管理要求及流程，明确了对账号的分类管理和访问控制策略，相关文件均通过评审流程并发布。	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。
2	应监测身份和访问政策的遵守情况。	华为云每年会对建立的身份与访问管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对身份与访问管理的网络安全要求进行审查和更新。
3	应衡量和定期评估身份和访问管理政策中的网络安全控制的有效性。	华为云每年会对建立的身份与访问管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对身份与访问管理的网络安全要求进行审查和更新。
4	身份和访问管理政策应包括		

a	访问控制的业务要求（即，需要拥有和需要知道）。	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。	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。 客户可使用华为云统一身份认证服务，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。
b	用户访问管理（例如，加入者、移动者、离开者）。		
1	应涵盖所有确定的用户类型（即，内部员工、第三方）。	华为云制定了公司用户账号权限管理的要求，其中规范了针对不同的用户类型，如内部员工，外部第三方人员的账号申请流程。	客户应确保账号管理要求中包含所有内外部的账号类型。
2	内部员工的工作状态或工作职位的变化（例如，加入者、迁移者和离开者）应该由人力资源部门发起。	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。新员工入职须经过用人部门总裁及部门HR的审批授权，管理平台（W3）会在审批后为该员工创建一个W3账号，该账号为员工在华为云内部各系统或平台中登录所用账号。 当华为云员工发生转岗时，转岗人员须提请转岗电子流自动会流转至该员工所在部门主管，部门主管在与相关系统管理员及HR确认员工当前拥有的权限已被清理并在电子流确认后在电子流中确认员工转岗。 在员工的离职电子流完全完成全部流程前须经过部门主管和HR的审核，确认员工在离职前已完成全部权限的清理，且该员工的W3账号会在员工离职后自动注销。	客户应确保人力资源部门对新入职员工、转岗员工及离职人员的账号权限变化进行管理。

3	外部员工或第三方的变更应由指定的负责方发起。	针对外包合作人员账号/权限，管理负责人为外包合作人员提交申请电子流，并通过相关主管的审批授权，授权完成后内部系统自动为该第三方人员创建一个仅拥有基本权限的内部账号，仅授予完成工作所需要的最低资源访问权限，当第三方人员离场或不再需要账号/权限时该管理负责人也需要提交注销申请。	客户应确保外部第三方人员权限的变更由管理负责人发起。
4	根据业务和合规要求（即需要拥有和需要知道，以避免未经授权的访问和（非）有意的数据泄漏），正式批准用户访问请求。	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。对云服务的访问通过统一身份认证服务（IAM – Identity and Access Management）对用户进行访问控制和权限管理。所有运维账号，设备及应用的账号均进行统一管理，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。如果账号使用人要使用账号，账号管理员可启动授权流程，通过口令或者提升账号的权限等方式进行授权；账号的申请人和审批人不能是同一个人。此外，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。	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。 客户可使用华为云统一身份认证服务，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。
5、6	应及时处理访问权限的变更。 应定期审查用户访问权限和资料。	华为云权限的变更均通过电子流进行申请和审批，可确保访问权限变更的及时性。 华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。针对外包合作人员账号/权限，管理负责人在外包合作人员离场或不再需要账号/权限时提交注销申请。主管会审视下属的账号/权限持有情况是否合理，如下属岗位/角色变动，将审视其原有岗位账号/权限是否已注销。	客户应定期审视账号权限范围，确保用户权限申请、变更或回收时，均可以按照身份和访问控制策略进行及时的管理。

7	应建立提交、批准和处理用户访问请求和撤销请求的审计跟踪。	华为云建立了权限定期审查机制，确保均开启了操作日志，对权限的新增/变更/删除操作进行记录，安全人员定期进行对权限变更日志审计。若发现未清除的离职账号，安全人员会要求系统管理员进行清除。	客户应建立提交、批准和处理用户访问请求和撤销请求的审计跟踪。
c	用户访问管理应得到自动化的支持。	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。对云服务的访问通过统一身份认证服务（IAM – Identity and Access Management）对用户进行访问控制和权限管理。所有运维账号，设备及应用的账号均进行统一管理，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。	客户应使用工具实现身份和访问管理的自动化和集中化。 客户可通过华为云的统一身份认证服务对使用云资源的用户账号进行管理。华为云统一身份认证服务提供适合企业级组织结构的用户账号管理服务，为客户分配不同的资源及操作权限。
d	身份和访问管理功能的集中化。	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。对云服务的访问通过统一身份认证服务（IAM – Identity and Access Management）对用户进行访问控制和权限管理。所有运维账号，设备及应用的账号均进行统一管理，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。华为云制定了内部运维账号的生命周期管理，包括帐号的开销户管理、帐号责任人/使用人管理、口令管理、开销户监控管理等，帐号一旦建立，立即纳入帐号管理员的日常维护管理工作。所有运维帐号，所有设备及应用的帐号均实现统一管理，并通过统一审计平台集中监控，并且进行自动审计，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。	客户应使用工具实现身份和访问管理的自动化和集中化。 客户可通过华为云的统一身份认证服务对使用云资源的用户账号进行管理。华为云统一身份认证服务提供适合企业级组织结构的用户账号管理服务，为客户分配不同的资源及操作权限。

e	对敏感和关键的系统和配置文件进行多因素认证。	华为云使用IAM对访问进行管理，支持多因素认证用于登录验证和操作保护，员工每次登陆均需要使用多重身份验证确定身份。员工通过互联网访问华为云办公网时须通过支持注册认证的设备及账号密码双因素认证的虚拟专属网络（VPN）方可登录认证。	客户应对敏感或关键系统的访问进行多因素身份验证策略。 客户可使用华为云统一身份认证服务，在密码认证通过后，还将收到一次性短信认证码进行二次认证。修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。
f	特权和远程访问管理，它应该解决：		
1	特权和远程访问的分配和限制使用，具体包括： a. 所有远程访问都应使用多因素认证。 b. 在风险评估的基础上，对关键系统的特权访问应使用多因素认证。	华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求，采用双因子认证对华为云运维人员进行身份认证，如USB key、Smart Card等。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。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。	客户应对远程访问及特权账号开启多因素认证。 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 Trace Service，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。

2、3	对拥有特权和远程账户的用户进行定期审查。 个人问责制。	华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求。华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，特权账号被严格纳管回收。 特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。仅在员工职责所需时，对其授予特权或应急账号。所有特权或应急账号的申请需要经过多 级的评审和批准。华为云仅会在得到客户授权后登录租户的控制台或者资源实例协助客户进行维护。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。	客户应建立特权账号的管理机制，密切监督特权账号的使用。
4	非个人特权账户的使用，包括。 a. 限制和监控。 b. 密码的保密性。 c. 经常改变密码，并在每次会话结束时改变密码。	非个人特权帐号一旦建立，立即纳入帐号管理员的日常维护管理工作。所有运维帐号，所有设备及应用的帐号均实现统一管理，并通过统一审计平台集中监控，并且进行自动审计。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。 帐号管理员可启动授权流程，通过口令或者提升帐号的权限等方式进行授权；华为云要求其账号和密码不能分配给特定的个人，账号/权限责任人会审视其负责的专用账号，当不再需要专用账号时修改口令并知会新使用人。帐号的申请人和审批人不能是同一个人。	客户应对非个人特权账户的使用进行限制和监控，确保密码的保密性。

5.3.6 应用安全

确保对所有应用实施充分的网络安全控制，并在金融机构内部定期监控其合规性和评估其有效性。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应用网络安全标准应被定义、批准和实施。	华为云已制定开发安全管理相关制度，对华为云服务在规划、设计、开发、部署、运维和用户支撑环境应遵循的安全编程规范及应用安全开发规范进行了定义。	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。

2	应监测对应用安全标准的遵守情况。	华为云定期对软件安全开发DevOps流程相关策略和流程进行审阅和更新。同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	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。
3	应该对应用网络安全控制的有效性进行测量和定期评估。	华为云定期对软件安全开发DevOps流程相关策略和流程进行审阅和更新。同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	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。
4	应用开发应遵循经批准的安全系统开发生命周期方法（SDLC）。	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。	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。
5	应用程序的安全标准应包括		
a	安全编码标准。	华为云严格遵从华为对内发布的安全编码规范。华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了静态代码扫描工具每日检查，其结果数据进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。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。	客户制定的软件开发项目管理方法或程序中应明确安全编码标准或规范。

b	实施的网络安全控制（例如，配置参数、监测和保留的事件[包括系统访问和数据]、身份和访问管理）。	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。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。	客户应确保应用程序的安全标准中包含实施网络安全的控制。
c	应用程序内的职责分离（以文件化的授权矩阵为支持）。	华为云遵循职责分离和权限制衡原则，对不相容职责进行分离，实现合理的权限分工，同时制定了SOD权责分离管理矩阵以帮助实现该管理原则。华为云研发环境采取分级管理，对开发环境进行包括物理隔离、逻辑隔离、接入访问控制、数据传输通道审批及审计等保护措施。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。	客户应确保应用程序的安全标准中包含应用程序的职责分离。
d	保护符合（商定的）分类计划的数据（包括客户数据的隐私，以及避免未经授权的访问和（非）有意的数据泄漏）。	华为云对在公共网络上提供的应用服务采用多种安全措施保护其中涉及的数据。包括使用IAM进行访问控制，对用户进行身份认证和鉴权。在信息传输过程中使用安全加密信道（如HTTPS），对存储的静态数据使用安全加密算法进行加密保护，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。对应用服务中的操作留存日志以支持审计。对接口进行身份认证及鉴权、传输保护和边界防护，确保API应用安全。	客户应确保对应用中的数据进行保护。

e	漏洞和补丁管理。	华为云建立了安全漏洞管理流程，规范了华为云系统安全漏洞的预警、评估、修复处理的闭环流程，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。华为云针对会影响客户服务的漏洞，华为云会由沙特一线业务支持团队负责与客户进行点对点漏洞披露，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。	客户应建立有效的漏洞管理机制，对所有技术资产进行漏洞识别和风险评估。
f	备份和恢复程序。	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。此外，华为云还规范了业务恢复策略的制定，确保业务能在恢复时间目标内恢复到可接受水平。	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。
g	定期网络安全合规性审查。	华为云建立了一个正式的、定期的审计计划包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以检查公司网络安全控制体系的运行情况，评估策略、规程及配套措施和指标的符合性和有效性。	客户应定期开展网络安全合规性审查，以确定网络安全控制的合规性和有效性。

5.3.7 变更管理

确保金融机构内信息资产的所有变更遵循严格的变更控制过程。

编号	具体控制要求	华为云的内部实践	客户的职责

1	应确定、批准和实施变更管理程序。	华为云制定了变更管理的管理规定和变更流程，定义了涵盖变更实施前、实施中及实施后应遵循的网络安全要求，以防止未授权变更。例如，变更前，各项变更均需通过多个环节的审核；变更实施中，会通过日志记录、操作监控及双人操作等方式确保变更安全实施，并确保变更过程可追溯；变更后，对变更实施专人验证，确保变更达到预期效果，不会造成网络安全风险。	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。
2	应监测对变更管理过程的遵守情况。	华为云每年会对建立的变更管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	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。
3	应衡量和定期评估变更管理过程中的网络安全控制的有效性。	华为云每年会对建立的变更管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	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。
4	变更管理流程应包括		
a	控制信息资产变更的网络安全要求，如评估所请求的变更的影响、变更的分类和对变更的审查。	华为云制定了变更管理的管理规定和变更流程，对不同变更类型应遵循的不同的变更管理流程，包括申请、评审及实施相变更进行了定义，各项变更均需通过多个环节的审核，并依据变更的紧急程度等因素对变更进行分类。	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。
b	安全测试，其中应（如适用）包括：		
1	渗透测试。	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。	客户应定期开展渗透测试。

2	如果应用程序是内部开发的，则进行代码审查。	华为云引入了静态代码扫描工具每日检查，其结果数据进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。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。	客户应对内部开发的应用程序开展代码审查。
3、4	对外部开发的应用程序进行代码审查，如果可以获得源代码的话。 在不能提供源代码的情况下，提供代码审查报告（或同等的报告，如独立保证声明）。	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。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。在使用中，须将第三方软件作为服务或解决方案的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或解决方案中使用独立的第三方软件是否引入新的安全问题。	客户应确保外部开发的应用程序的代码安全性。
c、d、e	业务负责人对变更的批准。 在提交给变更咨询委员会（CAB）之前，由网络安全职能部门批准。 由CAB批准。	所有的变更申请生成后，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，都需通过类生产坏境测试、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。	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。
f	对相关的网络安全控制进行实施后审查。	华为云建立了正式的内部测试及验收措施，以确保仅适当且经过授权的变更被发布至生产环境。在变更上线前须在变更管理系统中提交内部验收测试报告并说明测试验收方式，确保各类型变更需求在上线前完成测试以审查实施的网络安全控制是否有效。变更实施后，有专人进行验证，确保变更达到预期的目的。	客户对变更实施的网络安全控制进行审查。

g	开发、测试和实施对（技术）环境和参与的个人都是隔离的。	华为云建立了正式的环境隔离机制，对开发环境、测试环境、生态环境及生产环境实现严格的逻辑隔离，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。禁止未经授权打通测试环境和生产环境的网络链接，避免因测试环境被入侵而导致生产环境安全风险。	客户应该保证其开发、测试和生产环境相互隔离，并严格管控不同环境的使用。
h	紧急变更和修复的程序。	华为云也制定了规范的紧急变更管理流程。若紧急变更影响到用户，会按规定的时限提前通过公告、邮件、电话、会议等方式与用户沟通；若紧急变更不满足提前规定的通知时限，变更将升级至华为云高层领导，并在变更实施后及时对用户公告。紧急变更均留有记录，在变更执行前保留旧的程序版本及数据，在变更过程中通过双人操作等机制保证变更顺利进行，尽量减少对生产环境的影响。	客户应制定和实施紧急变更和修复的流程。
i	后退和回滚程序	变更申请必须提交变更方案，其中须提供回退方案和回退的方式，对现网产生影响第一时间按照变更方案启动问题，如果变更失败会执行变更回退。	客户应制定和实施变更后退和回滚程序。

5.3.8 基础设施安全

支持在金融机构内部正式记录基础设施内的所有网络安全控制，并对其合规性进行监控和定期评估其有效性。

编号	具体控制要求	华为云的内部实践	客户的职责

1	基础设施安全标准应得到界定、批准和实施。	华为云遵循华为公司建立的IT安全标准，其中明确了为防止对基础设施未经授权的变更或恶意入侵而实施的安全控制要求，包含有害代码防护、恶意软件防护、病毒防护、介质管理以及补丁管理的相关要求。华为云部署防病毒软件、防火墙、IPS、IDS等一系列的网络安全防护设备，同时实施有效的安全措施保障信息处理设施的安全性。此外，华为云将基础设施安全视为构筑多维全栈的云安全防护体系的核心组成部分。通过华为云构筑安全的基础设施底座，租户可以更放心地上云并利用安全的华为云服务更聚焦在业务发展上。	客户应定义和实施基础设施安全标准。
2	应监测对基础设施安全标准的遵守情况。	华为云定期对基础设施保护相关的策略和流程进行审阅和更新。同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	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。
3	应衡量和定期评估基础设施网络安全控制的有效性。	华为云定期对基础设施保护相关的策略和流程进行审阅和更新。同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	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。
4	基础设施安全标准应涵盖主数据中心、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。	华为云形成了完善的基础设施安全标准，涵盖物理环境、网络、云平台、应用程序接口、数据等主要方面的安全设计和实践。此外，华为云遵循华为公司建立的IT安全标准，其中明确了为防止对基础设施未经授权的变更或恶意入侵而实施的安全控制要求，包含有害代码防护、恶意软件防护、病毒防护、介质管理以及补丁管理的相关要求。关于办公终端、办公设备、电子邮件和文件等均遵循华为公司整体的安全标准。此外，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，两地互为灾备中心，其安全措施保持相同。	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。

5	基础设施安全标准应涵盖基础设施的所有实例（例如，操作系统、服务器、虚拟机、防火墙、网络设备、IDS、IPS、无线网络、网关服务器、代理服务器、电子邮件网关、外部连接、数据库、文件共享、工作站、笔记本电脑、平板电脑、移动设备、PBX）。	华为云形成了完善的基础设施安全标准，涵盖物理环境、网络、云平台、应用程序接口、数据等主要方面的安全设计和实践。此外，华为云遵循华为公司建立的IT安全标准，其中明确了为防止对基础设施未经授权的变更或恶意入侵而实施的安全控制要求，包含有害代码防护、恶意软件防护、病毒防护、介质管理以及补丁管理的相关要求。关于办公终端、办公设备、电子邮件和文件等均遵循华为公司整体的安全标准。	客户应确保基础设施安全标准涵盖基础设施的所有实例。
6	基础设施安全标准应包括		
a	实施的网络安全控制（例如，配置参数、监测和保留的事件[包括系统访问和数据]、数据泄漏预防[DLP]、身份和访问管理、远程维护）。	华为云针对其安全防护体系中的物理环境、网络、平台、应用程序接口（API – Application Programming Interface）和数据等主要方面实施了一系列的网络安全控制，以确保基础设施的安全设计和实践。此外，华为云对支撑业务运营的服务器操作系统、数据库管理系统及网络设备建立了统一的基线配置标准，以实现对服务基线配置的统一管理，明确华为云生产环境中各系统/组件的安全配置要求，并确保安全配置的有效执行和持续改进。	客户应遵守基础设施安全标准的的网络安全要求,实施有效的网络安全控制。
b	基础设施组件内的职责分离（以文件化的授权矩阵支持）。	华为云遵循职责分离和权限制衡原则，对不相容职责进行分离，实现合理的权限分工，同时制定了SOD权责分离管理矩阵以帮助实现该管理原则。华为云研发环境采取分级管理，对开发环境进行包括物理隔离、逻辑隔离、接入访问控制、数据传输通道审批及审计等保护措施。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。	客户应确保基础设施的安全标准中包含基础设施组件的职责分离。

c	保护符合（商定的）分类计划的数据（包括客户数据的隐私，以及避免未经授权的访问和（非）有意的数据泄漏）。	华为云从最初的网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分 区自我保护和容错恢复能力。华为云目前将生产及非生产环境划分为多个安全区域，包括：DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS –Object - Based Storage）、运维管理区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能， 确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制，并实现内部网络同外部网络的相互隔离及异常流量清洗。 此外，华为云不会访问客户的云环境，除非在故障维护时，华为云会在得到运维人员需通过工单系统或书面获得客户授权后，使用指定工具才允许接入租户的控制台或者资源实例以协助客户进行维护，严禁进行超出客户授权范围的任何操作及禁止类的高危操作，或在客户的网络上部署和运行未经客户授权的软件。此外，运维平台上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人，防止和避免未经授权的访问和数据泄露。	客户应实施保护符合分类计划的数据以避免未经授权的访问和数据泄漏。

d	使用经批准的软件和安全协议。	华为云制定并实施桌面终端服务软件标准及开源软件清单，仅可以使用其中定义的标准操作系统和软件应用程序。此外，华为云通过配置防火墙策略限制对高危端口及高危协议的使用。同时华为云内部制定了产品通信矩阵，其中对可使用的通信端口进行了维护，端口必须限定确定的合理的范围，且未在矩阵中的端口必须关闭，并通过端口扫描工具验证。	客户应确保使用经批准的软件和安全协议。
e	网络分段。	华为云基于业务功能及风险等级将生产及非生产环境划分为多个安全区域，DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS –Object - Based Storage）、运维管理区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能， 确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。	客户需对其网络进行安全区域划分和隔离，针对不同安全域之间的访问进行严格的管控。

f	恶意代码/软件和病毒保护（以及应用应用程序白名单和APT保护）。	在物理主机层面，通过部署防病毒软件，以实现对恶意软件的攻击防御。华为云桌面终端标准镜像内默认提供防病毒软件，员工默认无法对防病毒软件进行禁用操作。 此外，华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。	客户应实施恶意代码/软件和病毒的保护。 客户可使用华为云的企业主机安全（Host Security Service, 简称HSS），通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，并提供一键隔离查杀能力。同时，客户可部署华为云Web应用防火墙（Web Application Firewall，WAF）对网站业务流量进行多维度检测和防护。Web应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁，通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，全面避免网站被黑客恶意 攻击和入侵，保护Web服务安全稳定。

g	漏洞和补丁管理。	华为云建立了安全漏洞管理流程，规范了华为云系统安全漏洞的预警、评估、修复处理的闭环流程，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。	客户应建立有效的漏洞管理机制，对所有技术资产进行漏洞识别和风险评估。

h	DDOS保护（如适用）；这应包括 1. 使用刷新服务。 2. 对同意的带宽进行规范。 3. 由安全运营中心（SOC）、服务提供商（SP）和清除服务提供者进行全天候监控。 4. 对DDOS刷新的测试（至少每年两次）。 5. 应在主数据中心和灾难恢复站点实施DDOS服务。	1. 华为云在网络边界部署DoS/DDoS防范清洗层、下代防火墙、入侵防御系统层以及网站应用防火墙层。通过限制虚拟端口的连接跟踪数来抵御来自云平台外部或平台内部其他虚拟机的大流量攻击，此类攻击会产生大量连接跟踪表项，如果不做限制，会耗尽连接跟踪表资源，导致不能接受新的连接请求，最终导致业务及管理流量中断。 2. 在每个云数据中心边界部署华为专业的 Anti-DDoS设备来完成对异常和超大流量攻击的检测及清洗。Anti-DDoS可提供2Gbps的DDoS攻击防护，最高可达5Gbps。2Gbps是流量峰值，即Anti-DDoS防护流量达到的最大值。 3. 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。 4. 华为云建立了漏洞定期扫描机制，每月对DDoS流量清洗服务执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描。此外，华为云会定期对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。 5. 华为云每个云数据中心边界部署专业的 Anti-DDoS设备，此外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，两地互为灾备中心，其安全措施保持相同，因此华为云在主数据中心和灾难恢复站点均部署DDoS服务。	客户应实施DDoS保护措施，其中应明确使用流量清洗服务，对防护流量进行规范，并进行全天候监控，执行针对DDoS服务的测试以及在主数据中心和灾难恢复站点实施DDoS服务。 华为云为客户提供了Anti-DDoS流量清洗服务，客户可将Anti-DDoS流量清洗设备部署在其数据中心网络出口区域。Anti-DDoS设备通过对互联网访问弹性云服务器、弹性负载均衡和裸金属服务器的业务流量进行实时监测，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。

i	备份和恢复程序。	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。此外，华为云还规范了业务恢复策略的制定，确保业务能在恢复时间目标内恢复到可接受水平。	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。
j	定期网络安全合规性审查。	华为云建立了一个正式的、定期的审计计划包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以检查公司网络安全控制体系的运行情况，评估策略、规程及配套措施和指标的符合性和有效性。	客户应定期开展网络安全合规性审查，以确定网络安全控制的合规性和有效性。

5.3.9 密码学

确保敏感信息的获取和完整性受到保护，并能确认通信或交易的发起者。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应定义、批准和实施一项加密安全标准。	华为云制定并实施密码算法应用规范，规定了密码算法的选择规则及应用规则，同时给出了常见应用实例指导。华为云自身使用行业广泛使用的AES强效加密法对平台内的数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。	客户应建立密码管理政策，确保正确有效地使用密码学来保护信息资产，确保适当和有效地使用密码技术以保护信息的保密性、真实性和完整性。
2	应监测对加密安全标准的遵守情况。	华为云每年会对建立的密码算法应用及密钥管理安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对加密安全标准的遵守情况进行审查和更新。

3	应衡量和定期评估加密安全控制的有效性。	华为云每年会对建立的密码算法应用及密钥管理安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对加密安全标准的遵守情况的有效性进行审查和更新。
4	加密安全标准应包括		
a	已批准的密码解决方案和相关限制（如技术上、法律上）的概述。	华为云实施由华为云网络安全能力中心维护的密码算法应用规范，其中包含常见密码算法及方案的标准化信息列表，此列表已参考业界广泛采用标准和最佳实践，指导产品正确选择和使用密码算法。	客户在使用加密措施保护数据时，应考虑采用业内认可的加密算法和密钥管理机制。

b	在什么情况下应该应用经批准的加密解决方案。	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，对人员的权限与职责分配、加密级别、加密方法进行了规定。华为云自身使用行业广泛使用的AES强效加密法对平台内的数据进行加密，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，华为云提供的基础设施存储、数据库本身具有数据备份的机制，备份的数据副本和数据采用同样的数据安全措施。例如云硬盘提供安全的加密算法（AES-256）和功能、对象存储服务可提供服务端加密功能及防盗链功能、RDS数据库提供存储加密机制等。通过与数据加密服务集成，备份数据可以方便、快速地实现加密存储，有效保证备份数据的安全性。	客户应定义密码的使用策略，依据数据和信息的分类级别，考虑对传输中和静态数据的加密算法的类型、强度和质量。 客户可通过华为云的数据加密服务DEW实现对数据的加密，华为云将复杂的数据加解密、密钥管理逻辑进行封装，使得客户的数据加密操作变得简单易行。 目前，华为云云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 对于传输中的数据，当客户通过互联网提供Web网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给Web网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。

c	加密密钥的管理，包括生命周期管理、归档和恢复。	华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。	客户应建立密钥管理机制，用于处理加密密钥的生成、保护、归档、恢复和销毁，使数据的机密性和完整性不会受到损害。 华为云为客户提供了数据加密服务（DEW）,其密钥管理功能可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，HSM 拥有FIPS140-2（2级和3级）的主流国际安全认证，助力用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取客户根密钥。DEW还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。

5.3.10 自带设备(BYOD)

在使用个人设备时，确保会员组织的业务及敏感资料由工作人员妥善处理，并在传送及储存时得到保护。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应定义、批准和实施BYOD网络安全标准。	华为云制定了移动设备管理规定，以实施对移动计算设备的统一管理。对移动设备使用的原则、职责、权限要求、设备管理安全要求、网络接入要求及违规处罚等均做出规定。	客户应制定移动设备安全和BYOD管理策略。
2	应监测对BYOD网络安全标准的遵守情况。	华为云每年会对建立的移动办公终端相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对移动设备和BYOD的安全要求进行审查和更新。
3	应衡量并定期评估BYOD网络安全控制的有效性。	华为云每年会对建立的移动办公终端相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对移动设备和BYOD的安全要求进行审查和更新。
4	BYOD标准应包括		
a	用户的责任（包括意识培训）。	在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。	客户应定期对使用移动设备的员工进行安全意识培训，对移动设备的安全使用和责任进行宣贯。
b	当金融机构对员工的个人设备实施网络安全控制时，有关限制和后果的信息；例如，在使用修改过的设备（越狱）、终止雇用或个人设备丢失或被盗的情况下。	员工离职或转岗等，必须对办公计算机硬盘进行格式化处理，若涉及机密、绝密信息，应确保删除的数据无法恢复，同时主动及时的卸载BYOD上公司应用清楚公司数据。若设备丢失或被盗，员工须向业务主管和信息安全部门报告，并远程擦除公司数据，并取消设备绑定。	客户应对员工设备实施网络安全控制，如在设备丢失、被盗或与组织终止/分离后，安全清除存储在移动设备和 BYOD 上的组织数据和信息。

c	商业信息与个人信息的隔离（例如，容器化）。	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，对人员的权限与职责分配、加密级别、加密方法进行了规定。同时，针对不同级别的数据，限制含有涉密数据的电子流或邮件发布到移动BYOD端的应用中，BYOD上的组织数据和信息不涉及华为的核心信息资产。	客户应确保对存储在设备中的数据和信息资产进行加密和分离措施。
d	对企业移动应用程序或经批准的"公共 "移动应用程序的监管。	华为云制定了办公应用程序安全管理规定，明确了企业办公应用系统仅用于华为业务或相关管理层授权使用的目的，有权对办公应用系统的使用情况进行监控，保障办公应用系统的安全。	客户应对其组织内的移动应用程序进行监管。
e	使用移动设备管理（MDM）；对设备和业务容器实施访问控制，并对个人设备实施加密机制（以确保安全传输和存储）。	华为云使用MDM移动设备管理系统以实施对移动计算设备的统一管理，记录和维护所有终端用户和移动设备的清单，对移动设备进行分类、监控和管理。同时，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，对人员的权限与职责分配、加密级别、加密方法进行了规定。此外，针对不同级别的数据，限制含有涉密数据的电子流或邮件发布到移动BYOD端的应用中，BYOD上的组织数据和信息不涉及华为的核心信息资产。	客户应使用移动设备管理工具，并对存储在设备中的数据和信息资产进行加密措施。

5.3.11 信息资产的安全处置

确保金融机构的业务、客户和其他敏感信息在处置时免受泄露或未经授权披露。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应确定、批准和实施安全处置标准和程序。	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享，确保资产按照其对组织的重要程度受到适当水平的保护。华为云通过CAM资产管理系统实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。	客户应依据不同级别的资产分类定义和制定信息和技术资产管理的网络安全要求，确保资产按照其对组织的重要程度受到适当水平的保护。

2	应监测安全处置标准和程序的遵守情况。	华为云每年会对建立的资产处置流程与要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对资产处置以及程序的遵守情况进行审查和优化。
3	应衡量和定期评估安全处置网络安全控制的有效性。	华为云每年会对建立的资产处置流程与要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对资产处置要求以及流程的有效性进行审查和优化。
4	信息资产在不再需要时，应根据法律和法规要求进行处置（即满足数据隐私法规，以避免未经授权的访问和避免（非）有意的数据泄漏）。	华为云制定并实施介质管理规定，各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对介质清退报废进行分类操作，通过多种方式实现数据清除、磁盘消磁，并对销毁操作进行记录。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。	客户应定义并实施资产处置流程来处理信息资产的处置，以防止未经授权的披露或修改。
5	敏感信息的销毁应采用使信息无法检索的技术（例如，安全擦除、安全擦拭、焚烧、双重交叉切割、粉碎）。	华为云存储介质标准中明确规定了，含有残余华为公司保密信息或者个人数据的介质在处理前或者改用于与华为公司业务无关的用途前，存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。对于物理存储介质销毁的情况，须在华为员工的全程监督的情景下实施，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，使其上的数据无法恢复。	客户应明确介质储存的规定，以确保敏感信息被处置成无法读取或销毁的形式。

6	金融机构应确保用于安全处置、运输和储存的第三方服务提供商遵守安全处置标准和程序，并定期衡量和评估其有效性。	华为云作为金融机构的云服务提供商，华为云已制定并实施介质的管理规定，其中明确： ● 要求包含华为公司保密信息的存储介质必须进行标记。保密数据应依据数据密级进行标记或者贴上标签，须说明其保密级别. 对于运输过程中的介质或授权存放介质的设施外部必须贴标签，对用于运输机介质的上锁容器，其外部也必须贴有标签。 ● 要求存储介质必须保存在受控访问区，或者放置在公司内部上锁的柜子里，存储介质从受控区域出入的时候必须对出库到入库的具体信息对账和闭环跟踪。 ● 对存储组织信息的介质按照其对组织的重要程度实施适当水平的保护，以及防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。	客户应定期审查和评估第三方服务提供商是否遵守安全处置标准。

5.3.12 网络安全事件管理

确保及时识别和响应有关信息资产的异常或可疑事件。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应定义、批准和实施安全事件管理流程。	华为云内部制定了安全事件管理机制，规范了华为云安全事件响应操作，在出现安全事件时遵循华为云事件响应流程（识别、评估、决策和执行应急响应处理），明确华为云安全事件定级及通报机制。同时华为云规范了安全事件的升降原则，在溯源分析事件时若新风险被识别，则新增安全事件的定级需要衡量统一事件累计的结果，重新对其进行定级响应。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。	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。
2	应衡量和定期评估安全事件管理过程中的网络安全控制的有效性。	华为云每年会对建立的安全事件管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对安全事件管理的安全要求进行审查和更新。

3	为了支持这个过程，应该定义、批准和实施安全事件监控标准。 a. 该标准应根据信息资产的分类或风险状况，为所有信息资产解决应被监控的强制性事件。	华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理。异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录，华为云安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件，并针对收集上来的安全事件进行统一的跟踪管理，确保安全事件得以被及时处理及修复。此外，华为云会定期对事件的相关指标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。	客户应衡量与监控网络安全事件指标。
4	安全事件管理流程应包括以下要求。		
a	建立一个负责安全监控的指定团队（即安全操作中心（SOC））。	鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对。	客户应建立一个负责安全监控的制定团队（即安全操作中心（SOC））。
b	熟练和（持续）训练的工作人员。	华为的安全技术团队包括全球各地业界优秀的信息安全、产品安全、应用安全、系统安全、网络安全、云服务安全、运维运营安全、隐私保护等方面的专家专才。同时，华为云建立了自己的培训机制，根据不同的角色、岗位为员工设计合适的培训方案。其中一般员工的培训频率为至少每年一次，核心岗位员工培训频率更高。	客户应聘请熟练和（持续）训练的工作人员。
c	一个便于SOC活动和工作空间的限制区。	华为云安全运维中心通过门禁管理系统、视频监控系统、独立区域、防火防断电等物理措施确保运维安全。安全运维中心与开放办公区隔离，同时办公区分为多个不同等级的安全区域进行管理，根据员工的职责需要赋予访问权限。	客户应设置一个专门用于SOC活动和工作空间的办公区域。
d	持续监测安全事件活动所需的资源（24x7）。	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。	客户应24×7持续监测安全事件活动所需的资源。

e	检测和处理恶意代码和软件。	在物理主机层面，通过部署防病毒软件，以实现对恶意软件的攻击防御。华为云桌面终端标准镜像内默认提供防病毒软件，员工默认无法对防病毒软件进行禁用操作。 此外，华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。	客户应检测和处理恶意代码和软件。 客户可使用华为云的企业主机安全（Host Security Service, 简称HSS），通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，并提供一键隔离查杀能力。此外，客户可通过部署云防火墙（Cloud Firewall, CFW）实现云上互联网边界和VPC边界的防护，包括：实现入侵检测与防御，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，同时支持按需弹性扩容，是用户业务上云的网络安全防护基础服务。同时，客户可部署华为云Web应用防火墙（Web Application Firewall，WAF）对网站业务流量进行多维度检测和防护。Web应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁，通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用

			漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，全面避免网站被黑客恶意攻击和入侵，保护Web服务安全稳定。
f	检测和处理安全或可疑的事件和异常情况。	华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理。异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录，华为云安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件，并针对收集上来的安全事件进行统一的跟踪管理，确保安全事件得以被及时处理及修复。	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。 华为云提供的云日志服务（LTS – Log Tank Service）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务（CES – Cloud Eye Service），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。客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该IP地址的请求。

g	部署安全网络数据包分析解决方案。	华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。	客户应部署安全网络数据包分析解决方案。
h	适当保护日志。	在日志保存过程中采取安全措施防止日志被篡改，以确保支撑网络安全事件回溯和合规。为确保日志数据安全，安全日志会进行统一备份或归档，并依照数据安全管理的要求，限制安全日志使用的申请及权限，仅允许授权人员因必要原因进行安全日志的查询，确保受控使用。华为云遵从法律法规要求，具备集中、完整的日志审计系统，具备强大的数据保存及查询能力，确保所有日志内容保存时间超过 6 个月。	客户应确保保护网络安全事件日志免遭更改、披露、破坏及未经授权的访问和未经授权的发布。
i	定期监测应用程序和基础设施网络安全标准的合规性 。	华为云建立了一个正式的、定期的审计计划包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以检查公司网络安全控制体系的运行情况，评估策略、规程及配套措施和指标的符合性和有效性。	客户应定期开展网络安全合规性审查，以确定网络安全控制的合规性和有效性。

j	对安全日志进行自动和集中分析，并对事件或模式进行关联（即安全信息和事件管理（SIEM））。	华为云建立了集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以确保支撑网络安全事件回溯。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM–Security Information and Event Management）系统如ArcSight、Splunk对接。 对于集中存储安全日志的日志分析平台，系统管理员会定期例行对采集状态、存储状态进行检查，保证安全日志的可用性。华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理，异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录。	客户应对安全日志进行自动和集中分析，并对事件或模式进行关联，对网络安全事件进行及时报告。 华为云提供的云日志服务（Log Tank Service，简称LTS）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务（CES – Cloud Eye Service），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。客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该IP地址的请求
k	网络安全事件的报告。	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。	客户应明确网络安全事件报告的流程。

l	对安全操作中心的有效性进行独立的定期测试（例如，红队）。	为配合客户满足合规要求，华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性，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。此外，华为云引进业界优秀实践，开发网络安全实战演练平台，开展红蓝对抗，提供场景化的实战演练环境供员工练习和交流，提升员工的安全技能。	客户应对安全操作中心定期开展独立的渗透测试和安全评估。

5.3.13 网络安全应急事件管理

确保及时识别和处理网络安全事件，以减少对金融机构的(潜在)业务影响。

编号	具体控制要求	华为云的内部实践	客户的职责
1	应定义、批准、实施网络安全事件管理流程，并与企业事件管理流程保持一致。	华为云内部制定了安全事件管理机制，规范了华为云安全事件响应操作，明确华为云安全事件定级及通报机制。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。	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。
2	应衡量和定期评估网络安全事件管理过程中的网络安全控制的有效性。	华为云每年会对建立的安全事件相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对安全事件管理的安全要求进行审查和更新。
3	该标准应解决响应的强制性和可疑安全事件。	华为云建立了事件处理流程，在出现安全事件时遵循华为云事件响应流程（识别、评估、决策和执行应急响应处理）。同时华为云规范了安全事件的升降原则，在溯源分析事件时若新风险被识别，则新增安全事件的定级需要衡量统一事件累计的结果，重新对其进行定级响应。此外，华为云内部制定了完善的事件管理流程，根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。	客户应确保网络安全应急事件标准能够解决响应的强制性和可疑的安全事件。

4	安全事件管理流程应包括以下要求。		
a	建立一个负责安全事件管理的指定团队。	华为云建立了安全事件响应团队，负责监控和分析告警，评估是否属于信息安全事件，并针对收集上来的安全事件进行统一的跟踪管理，确保安全事件得以被及时处理及修复。	客户应建立一个负责安全监控的制定团队。
b	熟练和（持续）培训的工作人员。	华为的安全技术团队包括全球各地业界优秀的信息安全、产品安全、应用安全、系统安全、网络安全、云服务安全、运维运营安全、隐私保护等方面的专家专才。此外，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。	客户应聘请熟练和（持续）训练的工作人员。
c	法证人员有足够能力处理重大事件(例如，内部人员或与外部法证小组签约)。	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，以确保能够及时处理重大事件。此外，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。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。	客户应确保其法证人员有能力处理重大事件。
d	一个限制区，以方便计算机应急响应小组（CERT）的工作空间。	华为云制定了作战室运作规范，明确各业务团队均须维护一个与办公区域隔离的办公地点，用于紧急响应和处理安全事件，此外华为云作战室运作规范还对作战室的启动、作战指挥、通报、关闭等关键活动流程进行了明确，为华为云现网重大事件响应恢复提供指导。	客户应设置一个专用于计算机应急响应小组工作的限制区域。
e	网络安全事件的分类。	华为云内部制定了完善的事件管理流程，根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。	客户应根据事件的影响程度和范围的不同对网络安全事件进行分类。

f	及时处理网络安全事件，记录和监测进展。	在出现安全事件时华为云依照事件响应流程（识别、评估、决策和执行应急响应处理），根据不同类型及级别的安全事件实施响应机制，在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。此外，华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息安全事件的进展、 处置措施与落实。	客户应及时处理网络安全事件，并记录和监测进展。
g	保护相关证据和记录。	华为云制定了安全事件应急处置流程及响应流程，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。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。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。	客户应确保保护安全事件相关的证据和记录。
h	事故发生后的活动，如取证、事件的根本原因分析。	华为云制定了安全事件应急处置流程及响应流程，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。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。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息安全事件的进展、 处置措施与落实，对事件处置后的影响进行分析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯，并形成事件报告总结经验教训，在报告中告知事件的描述、起因、影响、华为云已采取的措施等内容。同时，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。	客户应在事故发生后开展取证、分析原因等活动，利用在分析和解决信息安全事件中得到了知识来减少未来事件发生的可能性和影响。

i	向CISO和委员会报告改进建议。	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。	当发生网络安全事件时，客户应按照本规定的要求向CISO和委员会汇报事件改进建议。
j	建立一个网络安全事件库。	华为云建立了统一的安全事件管理系统，实现对安全事件的统一收集，并针对收集上来的安全事件进行统一跟踪管理，确保事件得以被及时处理及修复时建立平台侧安全事件定期审阅机制。此外，该系统可用于记录和跟踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯。	客户应建立一个网络安全事件库。

5.3.14 威胁管理

充分了解金融机构的威胁态势。

编号	具体控制要求	华为云的内部实践	客户的职责

1	应确定、批准和实施威胁情报管理程序。	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、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。	客户应定义威胁情报管理程序。
2	应衡量和定期评估威胁情报管理程序的有效性。	华为云每年会对建立的威胁情报管理相关的策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对威胁情报的安全管理流程进行审查和更新。
3	威胁情报管理过程应包括		

a	使用内部来源，如访问控制、应用程序和基础设施日志、IDS、IPS、安全工具、安全信息和事件监控（SIEM）、支持功能（如法律、审计、IT服务台、取证、欺诈管理、风险管理、合规）	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。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。此外，华为云支持与第三方安全信息和事件管理（SIEM–Security Information and Event Management）系统如ArcSight、Splunk 对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。	客户应使用专用工具（如安全情报工具）对检测到的威胁情报事件进行持续收集和监控分析。 态势感知（SA - Situation Awareness）是华为云为客户提供的安全管理与态势分析平台。能够检测出包括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、命令与控制等多种云上安全风险。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，为客户呈现出全局安全攻击态势，帮助客户识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联DDoS高防、企业主机安全服务、Web应用防火墙和数据库安全服务等，集中呈现安全防护状态。

b	使用可靠和相关的外部资源，如SAMA、政府机构、安全论坛、（安全）供应商、安全组织和专家通知服务。	华为云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信息。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，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。	客户应使用可靠和相关的外部资源收集威胁情报。
c、d、e	c. 确定的方法，定期分析威胁信息。 d. 确定或收集到的威胁的相关细节，如工作方式、行为者、动机和威胁的类型。 e. 所得情报的相关性和后续行动的可操作性（例如，SOC、风险管理）。	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、Web 攻击、Web 未授权 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。此外，针对日常多样化的攻击告警事件，华为云有专业的安全事件管理系统对安全事件 进行端到端的跟踪闭环，整个处置过程可回溯。	客户应使用必要的技术对威胁信息和相关细节进行收集和分析。同时，应明确所得情报的相关性和后续行动的可操作性。
f	与相关的利益相关者（如SAMA，BCIS成员）分享相关情报。	为配合客户满足与利益相关者分享威胁情报的要求，华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。	客户应与客户的利益相关方(如SAMA、BCIS成员等)进行积极沟通。

5.3.15 漏洞管理

确保及时发现并有效缓解应用程序和基础设施漏洞，以减少对金融机构的可能性和业务影响。

编号	具体控制要求	华为云的内部实践	客户的职责

1	应确定、批准和实施漏洞管理程序。	华为云建立了安全漏洞管理流程，规范了华为云系统安全漏洞的预警、评估、修复处理的闭环流程，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。	客户应建立有效的漏洞管理机制，对所有技术资产进行漏洞识别和风险评估。
2	应衡量和定期评估漏洞管理过程的有效性。	华为云每年会对建立的漏洞管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对漏洞管理过程的有效性进行审查和更新。
3	漏洞管理过程应包括		

a	所有信息资产。	华为云建立了漏洞定期扫描机制，每月对报告范围内的产品执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描。	客户应对所有信息资产开展漏洞扫描。 客户可通过华为云提供漏洞扫描服务（VSS - Vulnerability Scan Service）。实现对Web应用、操作系统、配置基线的扫描，以及对资产内容合规检测和弱密码检测，以识别网站或服务器暴露在网络中的安全风险。华为云会第一时间针对紧急爆发的通用漏洞CVE进行分析并更新规则，提供快速、专业的CVE漏洞扫描。同时，客户可使用华为云的企业主机安全（Host Security Service, 简称HSS）,检测Windows/Linux操作系统与SSH、OpenSSL、Apache、Mysql等 软件存在的漏洞，并给出修复建议。此外，华为云可为客户提供容器安全服务（CGS – Container Guard Service）能够扫描镜像中的漏洞与配置信 息，发现镜像中的漏洞并给出修复建议，帮助企业解决传统安全软件无法感知容器环境的问题。

b	执行漏洞扫描的频率（基于风险）。	华为云建立了漏洞定期扫描机制，每月对报告范围内的产品执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描。华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。	客户根据漏洞扫描流程，以组织定义的频率对其信息系统进行漏洞扫描。
c、d、e	c. 漏洞的分类。 d. 确定的缓解时间表（按分类）。 e. 分类信息资产的优先次序。	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，基于业界最佳实践CVSS（Common Vulnerability Scoring System）对漏洞进行严重级别的评估，并结合漏洞在华为云中被利用的风险评估结果决定处理优先等级，制定并落实漏洞修复方案或规避措施，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。	客户应分析漏洞对关键信息资产的影响，并为根据其重要性确定风险等级和修复优先级。

f	补丁管理和部署方法。	华为云建立安全补丁管理的流程，保证安全补丁在IT安全标准规定的期限内完成安装。同时，华为云制定了漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，不断优化云平台及云产品默认安全配置、及时在规定的期限内应用修补措施或补丁、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等。	客户应建立有效的补丁和漏洞管理机制，对所有技术资产进行漏洞识别和风险评估，对关键补丁进行测试，制定补丁更新周期以及补丁修复的工作流程。 华为云镜像服务（IMS）简单方便的镜像自助管理功能。客户可通过服务控制台或API对自己的镜像进行管理。华为云负责公共镜像的定期更新与维护向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息以便用户在部署测试、故障排除等运维活动时参考。

5.4 第三方网络安全

《SAMA 网络安全框架》3. 4“第三方网络安全”中要求客户应确保第三方实施与组织内部相同级别的网络安全保护，为客户实施业务外包提供了指引。对客户的控制要求覆盖服务供应商能力、合同和协议、客户数据机密性等领域。相关控制要求及华为云的实践方式如下：

5.4.1 合同和供应商管理

确保金融机构批准的网络安全要求在签署合同前得到适当处理，并在合同生命周期内对网络安全要求的符合性进行监控和评估。

编号	具体控制要求	华为云的内部实践	客户的职责
1	网络安全要求应在合同和供应商管理过程中进行定义、批准、实施和沟通。	华为云提供了线上的《华为云用户协议》以及华为云《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。

2	应监测合同和供应商管理程序的遵守情况。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	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。
3	应衡量和定期评估合同和供应商管理过程中的网络安全控制的有效性。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	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。
4	这些合同和供应商管理流程应涵盖。 a. 是否积极要求网络安全职能的参与（例如，在尽职调查的情况下）。 b. 在所有情况下都应适用的网络安全基线要求。 c. 定期进行网络安全审查和审计的权利。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	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。
5	合同管理流程应涵盖以下要求。		
a，b，c，d	a. 作为采购过程的一部分，执行网络安全风险评估。 b. 确定具体的网络安全要求，作为投标过程的一部分。 c. 评估潜在供应商对所定义的网络安全要求的答复。 d. 对商定的网络安全要求进行测试（基于风险）。	华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据金融机构的需求进行定制化。 华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	客户应在与供应商签订的合同中明确将执行网络安全风险评估作为采购过程的一部分、将网络安全要求作为投标过程的一部分、评估供应商对网络安全要求的应答以及基于风险对商定的网络安全要求进行测试。

e	在发生网络安全事件时，确定沟通或升级程序。	华为云可能会随时自行修改或中止服务或修改或移除服务的功能。如果客户订阅的服务发生重大变更或中止，华为云会通过在网站发布通知或其他方式通知客户。此外，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。	客户应在与供应商签订的合同中明确发生网络安全事件时的沟通或升级程序。
f	确保界定退出、终止或续约的网络安全要求（如果适用，包括托管协议）。	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。 在客户确认删除数据后，华为云会对指定的数据及其所有副本进行全面的清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。 在服务协议终止时，华为云提供的云数据迁移服务（CDM），支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。	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。
g	界定相互间的保密协议。	华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，并严格遵守《SAMA》所述的网络安全原则。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。	客户应在与供应商签订的合同中明确互相间的保密协议。

6	供应商管理流程（即服务水平管理）应涵盖以下要求。 a. 定期报告、审查和评估合同约定的网络安全要求（在服务水平协议中）。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	客户应定期审查和评估与供应商签订的合同中约定的网络安全要求。

5.4.2 外包

确保在外包合同签订前、签订期间和退出时，适当满足金融机构的网络安全要求。

编号	具体控制要求	华为云的内部实践	客户的职责
1	外包政策和流程中的网络安全要求应在金融机构内定义、批准、实施和沟通。	华为云提供了线上的《华为云用户协议》以及华为云《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。	客户应定义、批准和实施外包政策和流程的网络安全要求。
2	关于外包政策和流程的网络安全要求应该被衡量和定期评估。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	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。
3	外包程序应包括 a. 在实质性外包之前，获得SAMA的批准。 b. 网络安全部门的参与。 c. 遵守SAMA关于外包的通知。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	客户在实质外包之前应获取SAMA的批准，且其外包政策的制定应由内部网络安全部门参与。

5.4.3 云计算

为确保金融机构内的所有职能部门和工作人员了解混合云和公共云服务的商定方向和立场、申请混合云和公共云服务所需的流程、混合云和公共云服务的风险偏好以及具体的混合和公共云服务的网络安全要求。

编号	具体控制要求	华为云的内部实践	客户的职责

1	混合云和公共云服务的云计算政策中的网络安全控制应在金融机构内定义、批准、实施和沟通。	华为云提供了线上的《华为云用户协议》以及华为云《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。 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、CSA STAR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。	客户应建立使用云计算服务相关的网络安全要求，确保在云上的组织的信息和技术资产的安全。
2	应监控云计算政策的遵守情况。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。 华为云作为云服务提供商，每年会对建立的信息安全管理体系进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对使用云计算有关的网络安全要求进行审查和更新。
3	应定期测量和评估与混合云和公共云服务的云计算政策和流程有关的网络安全控制。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。 华为云作为云服务提供商，每年会对建立的信息安全管理体系进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对使用云计算有关的网络安全要求进行审查和更新。
4	混合云和公共云服务的云计算政策应满足以下要求：		

a	采用云服务的过程，包括： 1. 应对云服务提供商及其云服务进行网络安全风险评估和尽职调查； 2. 金融机构在使用云服务或与云提供商签订合同前应获得SAMA批准； 3. 使用云服务前应签订合同，包括网络安全要求；	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。 华为云作为云服务提供商，遵守客户提出的网络安全要求，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。	客户应在采用云服务之前对该云提供商进行风险评估。客户在实质外包之前应获取SAMA的批准，且与云服务供应商签订的合同中应包含网络安全的要求。
b	数据位置，包括： 1. 原则上只应使用位于沙特阿拉伯境内的云服务，或在沙特阿拉伯境外使用云服务时，金融机构应获得 SAMA 的明确批准；	华为云数据中心部署在沙特阿拉伯王国境内。	客户应确保数据中心位于沙特阿拉伯王国境内，或在境外使用云服务时，应获得SAMA的批准。
c	数据使用限制，包括： 1. 云服务提供商不得将金融机构的数据用于次要目的；	华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，并严格遵守《SAMA》所述的网络安全原则。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。 华为云以为客户提供云服务为核心，基于《隐私政策声明》中披露的目的收集和处理个人数据，并且华为云针对涉及个人数据的产品及服务会定期进行隐私影响评估，以防产品及服务涉及的个人数据收集、处理超出实际目的所需范围。 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。	客户应在与云服务提供商签订的合同或协议中明确云服务不得将金融机构的数据用于其他目的。

d	安全，包括： 1. 云服务提供商应实施和监控风险评估中确定的网络安全控制措施，以保护金融机构数据的机密性、完整性和可用性；	华为云作为云服务提供商，遵守客户提出的网络安全要求，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。此外，华为云建立了信息安全风险管理规范，明确风险管理应遵循的关键流程、风险管理范围、风险管理相关责任部门及风险管理中应遵循的标准，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。	客户应明确云服务提供商应遵守的网络安全要求。
e	数据隔离，包括： 1. 金融机构的数据与云服务提供商持有的其他数据在逻辑上隔离，包括云服务提供商应能够识别金融机构的数据，并应始终能够将其与其他数据区分开来。	华为云从最初的网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。华为云对云端数据的隔离是通过虚拟私有云（VPC–Virtual Private Cloud）实施的，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构建私有网络环境，通过子网规划、路由策略配置等进行网络区域划分，将存储放置在内部子网，并通过配置网络 ACL 和安全组规则对进出子网以及和虚拟机的网络流量进行严格的管控。	客户应确保组织的数据与云服务提供商持有的其他数据在逻辑上隔离。

f	业务连续性，包括： 1. 根据金融机构的业务连续性政策满足业务连续性要求；	如果金融机构在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。 华为云制定了业务连续性管理规定，以规范业务连续性相关管理框架、目的和范围、管理目标、角色和职责等内容。华为云已经通过ISO22301业务连续性管理体系标准的认证，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。此外，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。	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。
g	审计、审查和监测，包括： 1. 金融机构有权在云服务提供商处进行网络安全审查； 2. 金融机构有权对云服务提供商进行网络安全审计； 3. 金融机构有权在云服务提供商处进行网络安全检查；	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	金融机构应对云服务提供商开展网络安全审查、审计与检查。

h	退出，包括： 1. 金融机构有终止权； 2. 云服务提供商必须返还金融机构的终止数据； 3. 云服务提供商必须在终止时不可逆转地删除金融机构的数据。	在服务协议终止时，客户可通过华为云提供的云数据迁移服务（CDM），将内容数据从华为云中迁移出去，如迁移至本地数据中心。 在客户确认删除数据后，华为云会对指定的数据及其所有副本进行全面的清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。	客户应在与云服务提供商签订的合同或协议中明确在服务结束时使用安全措施删除组织的数据。 在服务协议终止时，客户可通过华为云提供的云数据迁移服务（CDM），将内容数据从华为云中迁移出去，如迁移至本地数据中心。

6 结语

本文描述了华为云如何为客户提供符合沙特阿拉伯金融行业监管要求的云服务，并表明沙特阿拉伯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于沙特阿拉伯金融行业监管要求方面的合规性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合沙特阿拉伯金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本文仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对相关沙特阿拉伯金融行业监管要求的遵从性。

7 历史版本

日期	版本	描述
2022年7月	1.0	首次发布