华为云马来西亚金融行业监管遵从性指南

文档版本 2.0

发布日期 2023-02-21

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述.....1
1.1 背景与发布目的.....1
1.2 适用的马来西亚金融监管要求简介.....1
1.3 名词定义.....2
2 华为云的认证情况.....4
3 华为云安全责任共担模型.....7
4 华为云全球基础设施.....8
5 华为云如何遵从及协助客户满足 BNM《科技风险管理》的要求.....9
5.1 科技运营管理.....10
5.2 网络安全管理.....25
5.3 科技审计.....31
5.4 内部意识和培训.....32
6 华为云如何遵从及协助客户满足 BNM《外包》的要求.....33
6.1 外包流程与风险管理.....34
6.2 马来西亚境外的外包.....39
6.3 涉及云服务的外包.....40
7 华为云如何遵从及协助客户满足 BNM《客户信息管理与许可披露》的要求.....41
7.1 控制环境.....42
7.2 客户信息泄露.....49
7.3 外包服务提供商.....51
8 华为云如何遵从及协助客户满足 BNM《发展金融机构的数据管理和管理信息系统框架指引》的要求.....53
9 华为云如何遵从及协助客户满足 BNM《业务连续性管理》的要求.....55
10 华为云如何遵从及协助客户满足 BNM《云技术风险评估指南（CTRAG）- 技术风险管理（RMIT）政策文件附录》（征求意见稿）的要求.....63
10.1 云治理.....64
10.2 云设计和控制.....70
11 华为云如何遵从及协助客户满足 SC《网络风险管理指引》的要求.....93
12 华为云如何遵从及协助客户满足 SC《业务连续性指导原则》的要求.....98

13 结语 101
14 版本历史 102

1 概述

1.1 背景与发布目的

随着在提供金融服务中更普遍地使用技术，金融机构有必要加强其应对业务中断的技术恢复能力，以保持对金融系统的信心。网络威胁日益复杂，这也要求金融机构提高警惕和应对新出现的威胁的能力。至关重要的是，金融机构应确保向客户持续提供必要的金融服务的同时，充分保障客户数据的安全。为了规范金融行业对于信息科技的运用，马来西亚国家银行（BNM）和马来西亚证券委员会（SC）发布了一系列监管要求，针对马来西亚金融机构科技风险管理、科技外包管理、客户信息保护、业务连续性管理、云技术风险评估等方面提出了相关监管要求。

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

1.2 适用的马来西亚金融监管要求简介

马来西亚国家银行（BNM）

- **科技风险管理（Risk Management in Technology，简称RMiT）：** 该政策文件规定了马来西亚国家银行对金融机构科技风险管理的要求。在遵守这些要求时，金融机构应考虑其业务的规模和复杂性。此外，所有金融机构应遵守该文件规定的最低标准，防止利用互联网络和系统中的薄弱环节，损害其他金融机构和更广泛的金融体系。
- **外包（Outsourcing）：** 该政策文件规定了与外包相关安排的范围，以及马来西亚国家银行对金融机构保持适当的内部治理和外包风险框架的要求和期望，包括与保护数据机密性有关的框架。这些要求也有助于确保金融机构具备持续能力对外包活动进行有效的监督。
- **客户信息管理与许可披露（Management of Customer Information and Permitted Disclosures）：** 该政策文件规定了马来西亚国家银行对金融服务提供商在整个信息生命周期中处理客户信息的措施和控制的要求和期望，涵盖了客户信息的收集、存储、使用、传输、共享、披露和处置。
- **发展金融机构的数据管理和管理信息系统框架指引（Guidelines on Data Management and Management Information System Framework for**

Development Financial Institutions）:该政策文件规定了金融机构在发展内部数据管理能力时应遵循的合理数据管理和管理信息系统实践的高阶指导原则。金融机构应以与指引中规定的原则一致并且适合每个金融机构特定业务需求的方式来构建和实施数据和管理信息系统。

- 业务连续性管理（Business Continuity Management）：本政策文件旨在促进金融机构制定和实施与其总体风险偏好相结合的稳健的业务连续性管理框架、政策和流程，并加强健全的风险管理做法；加强金融机构应对业务中断并从中恢复的能力和准备；和在运营中断的情况下，在指定的时间范围内保持关键业务功能和基本服务的连续性。
- 云技术风险评估指南（CTRAG）- 技术风险管理（RMIT）政策文件附录（征求意见稿）（Cloud Technology Risk Assessment Guideline (CTRAG) - Appendix to Risk Management in Technology (RMIT) Policy Document (Exposure Draft)）：本征求意见稿规定了评估金融机构采用云服务时常见关键风险和控制措施考虑因素的指南。拟议的预期作为技术风险管理（RMiT）政策文件的补充指南，以加强金融机构的云风险管理能力。

马来西亚证券委员会（SC）

- 网络风险管理指引（Guidelines on Management of Cyber Risk）：该政策文件规定了马来西亚证券委员会对金融机构网络风险管理的要求。这些要求有助于金融机构提升网络风险管理能力，保障金融机构的网络安全。
- 业务连续性指导原则（Guiding Principles on Business Continuity）：该政策文件旨在指导金融机构制定最低标准，并鼓励金融机构根据其业务运营的性质、规模和复杂性采用这些标准。原则的总体预期结果是确保在中断情况下关键服务的及时持续提供以及业务义务的履行，最终目标是减轻或管理对马来西亚资本市场可能产生的更大范围的系统性风险。

注：马来西亚国家银行发布的上述监管要求适用于银行、保险等金融机构，而马来西亚证券委员会发布的上述监管要求适用于马来西亚证券交易所、资本市场服务牌照持有者、注册人士以及马来西亚证券法规定的自我监管组织，具体的适用对象请参见监管要求原文。

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。
- **服务提供商**

  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。
- **网络弹性**

  指人员，流程，IT系统，应用程序，平台或基础架构承受不良网络事件的能力。
- **央行**

  指马来西亚国家银行（Bank Negara Malaysia, BNM）。
- **业务连续性**

指金融机构在中断事件期间保持其业务和服务连续性的能力。

- **业务影响分析（BIA）**

指在发生中断时衡量对金融机构运营和服务的定量和定性影响的过程。它用于确定对制定业务连续性计划至关重要的恢复优先级和恢复策略。

- **业务连续性计划（BCP）**

指一项综合行动计划，该计划记录了在发生中断时恢复和恢复金融机构运营和服务所需的流程、程序、系统和资源。

- **危机管理计划**

指一项综合行动计划，该计划记录了在危机发生时支持危机管理团队（CMT）决策的程序和流程。它包括启动BCP和灾难恢复计划（DRP）的标准。

- **灾难恢复计划（DRP）**

指一项综合行动计划，其中记录了在发生中断时恢复和恢复金融机构的信息技术系统、应用程序和数据所需的程序和流程。

- **关键业务职能（CBF）**

指金融机构承担的业务职能，此类业务职能的失败或中断可能会——

（a）严重影响金融机构的财务或非财务状况；和

（b）中断向客户提供基本服务。

- **最大可容忍停机时间（MTD）**

指在中断危及金融机构关键业务功能之前允许恢复的时间段。

- **恢复时间目标（RTO）**

指金融机构的系统和应用程序在中断后恢复并做好运行准备以支持其关键业务功能所需的时间框架。恢复时间目标包括以下两个部分：

（a）BCP从中断到激活的持续时间；和

（b）从启动BCP到恢复业务运营的持续时间。

2 华为云的认证情况

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	描述
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供应商可提供有效的IT服务来满足客户和业务的需求。
ISO 27001:2013	ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO 27017:2015	ISO 27017是针对云计算信息安全的国际认证。ISO 27017的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 22301:2012	ISO 22301是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
SOC审计	SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
PCI DSS认证	支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discover、万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。

认证	描述
CSA STAR金牌认证	CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
国际通用准则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。ISO 27018的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
ISO 29151:2017	ISO 29151是国际个人身份信息保护实践指南。ISO 29151的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
ISO 27701:2019	ISO 27701规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过ISO27701表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS 10012是BSI发布的个人信息数据管理体系标准，BS10012认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
M&O认证	Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。
NIST网络安全框架(CSF)	NIST CSF由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
PCI 3DS认证	PCI 3DS标准，旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS的评估对象为3D协议执行环境，包括访问控制服务器、目录服务器或3DS服务器功能；以及3D执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估3D协议执行环境的过程、流程、人员管理等。

地区性标准类认证

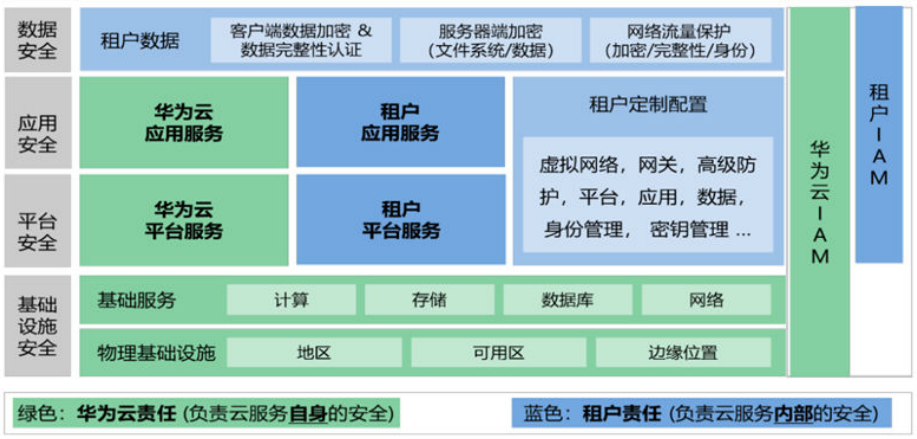
认证	描述
网络安全等级保护	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡 MTCS Level 3 认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3等级认证。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、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	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	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	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。

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模型

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

图 3-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

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

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

4 华为云全球基础设施

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

5 华为云如何遵从及协助客户满足 BNM《科技风险管理》的要求

马来西亚国家银行于2020年6月19日发布了《科技风险管理》。该规定从治理、科技风险管理、科技运营管理、网络安全管理、科技审计、内部意识和培训、技术相关应用通知等领域提出对金融机构科技风险管理相关要求。其中运营管理包括系统开发和获取、密码管理、数据中心弹性、网络弹性、第三方服务提供商管理、云服务、访问控制等方面的要求。网络安全管理包括网络安全运营、数据防泄漏、网络响应与恢复等方面的要求。

金融机构在遵循《科技风险管理》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《科技风险管理》中与云服务供应商相关的控制要求，并阐述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 科技运营管理

原文编号	具体控制要求	客户的关注	华为云的内部实践
系统开发和获取 10.5-10.8、10.10、10.12-10.14	10.5 金融机构必须为系统开发生命周期（SDLC）的关键阶段（包括系统设计、开发、测试、部署、变更管理、维护和停用）制定明确的风险管理政策和实践。这些策略和实践还必须将安全性和相关的企业架构考虑因素嵌入到SDLC中，以确保数据的机密性、完整性和可用性。 10.6 鼓励金融机构为软件开发、测试、软件部署、变更管理、代码扫描和软件版本控制部署自动化工具，以支持更安全的系统开发。 10.7 金融机构应考虑技术多样性的必要性，以确保关键系统基础设施不会过度暴露于类似的技术风险中，从而增强弹性。 10.8 金融机构在部署前必须建立一套完善的系统测试方法。测试应确保系统满足用户要求，性能可靠。如果使用敏感测试数据，金融机构必须确保适当的授权程序和适当的措施，以防止其未经授权的披露。 10.10 金融机构必须确保对关键系统源代码的任何更改都经过适当的源代码审查，以确保代码是安全的，并在引入任何系统更	客户应建立安全开发管理机制，对系统开发生命周期（包括系统设计、开发、测试、部署、变更等）制定风险管理政策和措施，不限于使用自动化工具、制定安全编码规范、代码复核、测试环境与生产环境隔离等，并应考虑通过正式的程序来管理变更。	作为云服务提供商： （1）华为云的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。为配合客户满足合规要求，华为云通过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。 华为云及相关云服务遵从安全及隐私设计原则和规范、适用的法律法规要求，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，保障产品、服务的安全。 （2）华为云严格遵从华为公司对内发布的多种编程语言的安全编码规范。使用静态代码扫描工具例行检查，其结果数据进入云服务工具链，以评估编码的质量。所有云服务在发布前，均须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。 （3）华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，使发布的云服务满足安全要求，测试在与生产环境隔离的测试环境中进行，并避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱

原文编号	具体控制要求	客户的关注	华为云的内部实践
	改之前按照公认的编码实践进行开发。 10.12 金融机构应将生产环境与关键系统的开发和测试环境进行物理隔离。金融机构依赖云环境的，应当确保云环境不在同一虚拟主机上运行。 10.13 金融机构必须建立适当的程序，独立审查和批准系统变更。金融机构还必须在重大变更未能成功实施时建立和测试应急计划，以尽量减少任何业务中断。 10.14 如果金融机构的信息技术系统由第三方服务提供商管理，金融机构应确保，包括通过合同义务，在进行任何可能影响信息技术系统的变更之前，第三方服务提供商向金融机构提供充分的通知。		敏，使用完成后需要进行数据清理。 （4）为配合客户满足合规要求，华为云制定了规范的变更管理流程，生产环境的各要素发生变更，都需要通过有序的活动进行变更管理。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，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，使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。同时华为云制定了更细粒度的变更操作规范，指导整个变更的实施、跟踪以及变更执行后的验证，使变更达到预期目的。另外，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。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。变更实施后，有专人进行验证，使变更达到预期的目的。

原文编号	具体控制要求	客户的关注	华为云的内部实践
密码管理 10.16、19.19、10.20	10.16 金融机构必须制定一项稳健而有弹性的密码政策，以促进采用强有力的密码控制措施来保护重要数据和信息。 10.19 金融机构必须确保密码控制以有效实施适当的密码协议为基础。协议应包括秘密和公开密码密钥协议，二者均应反映对适用的密钥或私人密码密钥的高度保护。此类协议的选择必须基于公认的国际标准，并进行相应的测试。与风险级别相称，必须在受保护的环境中进行密钥和私钥存储以及加密/解密计算，并由硬件安全模块（HSM）或可信执行环境（TEM）支持。 10.20金融机构应当根据风险程度，将公共密码密钥存储在证书颁发机构颁发的证书中。与客户相关的此类证书应由认可的证书颁发机构颁发。金融机构必须确保使用此类证书的身份验证和签名协议的实施受到强有力的保护，以确保与用户证书相对应的私钥的使用具有法律约束力且无可辩驳。	客户应建立密码管理政策，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，并使用专门的证书颁发机构的证书对密钥的存储和传输进行管理。 华为云为客户提供了**数据加密服务（Data Encryption Workshop，简称DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。DEW采用分层密钥管理	为配合客户满足监管要求： **（1）**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 FIPS 140-2（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。更多信息请参见**《华为云安全白皮书》**6.8.2数据加密（DEW）服务。 **（2）**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。 **（3）**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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
		机制，方便各层密钥的轮换。	

原文编号	具体控制要求	客户的关注	华为云的内部实践
数据中心弹性-数据中心基础设施 10.21-10.24	10.21 金融机构必须明确其数据中心的弹性和可用性目标，这些目标与其业务需求相一致。网络基础设施的设计必须具有弹性、安全性和可扩展性。潜在的数据中心故障或中断不得严重影响其金融服务的提供或妨碍其内部运营。 10.22金融机构必须确保生产数据中心可以同时维护。这包括确保生产数据中心具有为计算机设备服务的冗余容量组件和分配路径。 10.23除了第10.22段的要求外，还要求大型金融机构确保恢复数据中心可以同时维护。 10.24 金融机构应在专用空间内托管关键系统，以供生产数据中心使用。专用空间必须进行物理保护，以防止未经授权的访问，且位于不易受灾害影响的区域。金融机构还必须确保生产数据中心的关键部件（包括硬件部件、电力设施、热管理和数据中心基础设施）的设计和连接不存在单一故障点（SPOF）。金融机构还必须确保对这些关键组成部分进行充分的维护、全面和持续的监测，并及时发出故障警报和潜在问题的指示。	客户应建立与业务需求一致的弹性和高可用数据中心，应考虑网络基础设施的安全性和可拓展性、关键系统的独立空间和物理安全、基础设施和硬件设备的冗余、环境和资源的持续监控等，以防止因数据中心故障或中断严重影响其服务的提供或内部运营。	作为云服务提供商，配合客户满足监管要求： （1）华为云的数据中心满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3+标准。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，而且提供了合理足够的物理空间、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定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急响应等措施。更多关于内容请参见**《华为云安全白皮书》**5.1物理与环境安全。 （2）客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

原文编号	具体控制要求	客户的关注	华为云的内部实践
数据中心弹性-数据中心运营 10.26、10.27、10.30	10.26 金融机构必须确保其能力需求得到妥善规划和管理，并适当考虑业务增长计划。这包括确保足够的系统存储、中央处理器（CPU）电源、内存和网络带宽。 10.27金融机构必须建立实时监控机制，以跟踪关键流程和服务的能力利用和绩效。这些监测机制应能够向管理员提供及时和可采取行动的警报。 10.30金融机构必须保留足够数量的关键数据备份副本、操作系统软件的更新版本、生产程序、系统实用程序、所有主文件和事务文件以及用于恢复目的的事件日志。备份媒体必须存储在环境安全且受访问控制的备份站点中。	客户应建立性能监控及容量规划机制，基于业务的发展对其IT基础资源进行容量规划和管理，并对关键系统的性能进行持续监控。另外，客户应制定备份管理机制，对关键业务数据、操作系统、应用软件进行备份。 客户可以使用**对象存储服务（OBS）**的版本控制、**云硬盘备份（VBS）**、**云服务器备份（CSBS）**等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保	为配合客户满足监管要求： （1）华为云的**云监控服务（Cloud Eye Service，简称CES）**为用户提供一个针对**弹性云服务器（Elastic Cloud Server，简称ECS）**、带宽等资源的立体化监控平台。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。 （2）华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对用户云服务的系统性能造成影响。 （3）华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。

原文编号	具体控制要求	客户的关注	华为云的内部实践
		证在灾难发生时数据不丢失。	

原文编号	具体控制要求	客户的关注	华为云的内部实践
网络弹性10.33-10.36、10.38、10.39	10.33金融机构必须设计一个可靠、可扩展和安全的企业网络，能够支持其业务活动，包括未来的增长计划。 10.34金融机构必须确保其关键系统的网络服务是可靠的，并且没有单点故障（SPOF），以便保护关键系统免受潜在的网络故障和网络威胁的侵害。 10.35金融机构必须建立实时网络带宽监控流程和相应的网络服务弹性指标，以标记由于带宽拥塞和网络故障导致的带宽过度使用和系统中断。这包括用于检测趋势和异常的流量分析。 10.36金融机构必须确保设计和实施支持关键系统的网络服务，以确保数据的机密性、完整性和可用性。 10.38金融机构必须确保为调查和司法目的保留足够和相关的网络设备日志至少三年。 10.39金融机构必须实施适当的保障措施，以最大限度地降低一个实体中影响集团内其他实体的系统损害风险。实施的保障措施可能包括为金融机构与集团内其他实体建立逻辑网络分割。	客户应建立可靠、可拓展的企业网络，包括部署冗余的网络线路、建立网络性能监控、网络通道的加密、网络设备日志的保存、适当的网络隔离等措施。 客户可以使用华为云提供的**虚拟专用网络（Virtual Private Network，简称VPN）**、**云专线（Direct Connect，简称DC）**、**云连接（Cloud Connect，简称CC）**等服务，实现不同区域之间业务的互联互通和数据传输安全。 华为云的**云审计服务（Cloud Trace Service，**	作为云服务提供商： （1）华为云一方面负责各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，助力华为云安全。 （2）客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。 （3）华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。 （4）华为云VPN服务采用华为公司专业设备，基于IKE和IPsec协议在Internet网络上虚拟出私有网络，在本地数据中心和华为云VPC之间、华为云不同区域的VPC之间构建安全可靠的加密传输通道。云专线服务基于运营商多种类型的专线网络，在本地数据中心与华为云VPC之间构建专享的加密传输通道，各客户专线之间物理隔离，满足更高的安全性、稳定性要求。云连接服务能够快速在多个本地数据中心与多个云上VPC之间建立私有通信网

原文编号	具体控制要求	客户的关注	华为云的内部实践
		简称CTS）为用户提供包括网络在内的云服务资源的操作记录，供用户查询、审计和回溯使用。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的API执行的操作，以及华为云系统内部触发的操作。 客户可以使用华为云提供的**虚拟私有云（Virtual Private Cloud，简称VPC）**、**弹性负载均衡（Elastic Load Balance，简称ELB）**服务，实现不同区域之间网络隔离和负载平衡。	络，支持跨云VPC的互连，大大提升了客户业务向全球拓展的安全性和速度。 （5）CTS支持将操作记录合并，周期性地生成事件文件，实时同步转存至OBS存储桶，帮助用户实现操作记录高可用、低成本的长久保存。同时，华为云有集中、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，日志包含资源ID(如：源IP、主机ID、用户ID等)、事件类型、日期时间、受影响的数据/组件/资源的ID（如目的IP、主机ID、服务ID等）、成功或失败等信息，以助力支撑网络安全事件回溯和合规。 （6）VPC可为用户构建出私有网络环境，实现不同用户间在三层网络的完全隔离，用户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络ACL和安全组规则，对进出子网以和虚拟机的网络流量进行严格的管控，满足用户更细粒度的网络隔离需求。ELB将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

原文编号	具体控制要求	客户的关注	华为云的内部实践
第三方服务提供商管理 10.42、10.43、 10.46-10.48	10.42金融机构在提供服务之前，必须对第三方服务提供商的能力、系统基础设施和财务可行性进行适当的尽职调查。此外，应评估第三方服务提供商管理以下特定风险的能力： (a)数据泄露，如未经授权披露客户和交易对手信息; (b)服务中断，包括容量性能; (c)处理错误; (d)物理安全漏洞; (e)网络威胁; (f)过分依赖关键人员; (g)在传输、处理或存储此类信息的过程中，对与金融机构或其客户有关的机密信息处理不当; (h)集中风险。 10.43金融机构在与第三方服务提供商接洽时，必须建立服务水平协议（SLA）。SLA至少应包含以下内容： (a)监管机构和金融机构指定的任何一方审查金融机构的任何活动或实体的访问权限。 (b)要求服务提供者向金融机构充分事先通知任何重大分包的义务; (c)服务提供者就遵守有关法例的保密规定作出书面承诺; (d)在适用的情况下，安排灾难恢复和备份能力;	客户在指定服务供应商之前，应对其服务能力、系统基础设施和财务可行性进行尽职调查，并评估其风险管理能力。客户应与供应商签订具有法律效力的协议，在协议中约定关于配合审计、保密、业务连续性安排、通知、服务终止等方面的条款，以保障客户自身的权益，满足监管要求。 在服务协议终止时，客户可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移**	客户在指定服务供应商之前，应对其服务能力、系统基础设施和为配合客户满足监管要求： **（1）**华为云会安排专人积极配合客户发起的尽职调查要求。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。 **（2）**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。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。 **（2）**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。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。 **（3）**华为云为客户提供售后服务保障，华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等寻求帮助，将问题升级。除基础支持以外，系统复杂的企业客户可以选择适用的支持计划，获取由IM企业群、技术服务经理（TAM）、服务经理等组成的专属支持。为配合客户满足事件快速响应的要求，华为云内部制定了事件管理流程，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

原文编号	具体控制要求	客户的关注	华为云的内部实践
	(e)关键系统可用性;和 (f)业务连续性安排，以确保在服务提供商退出或终止时的业务连续性。 10.46金融机构必须确保存储在第三方服务提供商中的数据能够及时恢复。金融机构应确保与第三方服务提供商有明确的安排，以便于金融机构在发生网络事件时立即通知央行和其他相关监管机构并及时更新。 10.47金融机构必须确保其数据的存储至少在逻辑上与第三方服务提供商的其他客户隔离。应适当控制并定期审查向授权用户提供的访问权限。 10.48金融机构必须确保由第三方服务提供商托管的任何关键系统具有强大的恢复和持续能力，并在第三方服务提供商出现故障或表现不理想时提供便利有序退出的条款。	**服务（Server Migration Service，简称SMS）**，将内容数据从华为云中迁移出去，如迁移至本地数据中心。	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。 **（4）**华为云不用客户数据做商业变现，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，或者为遵守适用的法律法规或政府机关的约束性命令，并遵守马来西亚《个人数据保护法》所述的数据保护原则。此外，华为云各服务产品和组件从设计之初就规划并实现了合理的隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。 **（5）**华为云基础设施具备高可用性，同时华为云内部制定了完善的流程，对基础设施的运行状况进行持续监控、定期维修、定期测试，将系统故障给客户带来的影响降到最低。客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵循相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。此外，华为云针对支撑云服务的重要岗位设置了一岗多人、岗位互备的机制。

原文编号	具体控制要求	客户的关注	华为云的内部实践
云服务 10.51、10.53	10.51 要求金融机构在关键系统使用公有云之前咨询央行。金融机构应证明，与关键系统使用云服务相关的特定风险已得到充分考虑和解决。风险评估应解决以下方面： （b）云服务提供商至少在以下领域获得独立的、国际认可的认证： （i）信息安全管理框架，包括用于加密和解密用户数据的加密模块 （ii）针对云的安全控制，以保护客户和交易对手或专有信息，包括使用中、存储中和传输中的支付交易数据； 10.53 金融机构在使用云服务时，必须对客户和交易对手的信息和专有数据实施适当的保护措施，防止未经授权的披露和访问。这应包括保留与客户和交易对手信息、专有数据和托管在云上的服务相关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	客户应在关键系统使用公有云之前咨询央行，并对云服务提供商的安全资质进行评估。另外，客户还应制定的数据保护措施，防止在云服务上的数据的非法访问。 华为云为客户提供了**数据加密服务（Data Encryption Workshop，简称DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。	作为云服务提供商： （1）华为云已获得众多国际和行业安全合规资质认证，包括ISO27001、ISO27017、ISO27018、PCI-DSS、CSA STAR等。华为云遵循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。 （2）华为云不用客户数据做商业变现，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，或者为遵守适用的法律法规或政府机关的约束性命令，并遵守马来西亚《个人数据保护法》所述的数据保护原则。此外，华为云各服务产品和组件从设计之初就规划并实现了合理隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。 （3）华为云**云硬盘（EVS）**、**对象存储服务（OBS）**、**镜像服务（IMS）**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。 （4）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 FIPS 140-2（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。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

原文编号	具体控制要求	客户的关注	华为云的内部实践
			密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。更多信息请参见《华为云安全白皮书》6.8.2数据加密（DEW）服务。

原文编号	具体控制要求	客户的关注	华为云的内部实践
访问控制 10.54、10.56-10.58	10.54 金融机构必须实施适当的访问控制政策，以识别、认证和授权用户（内部和外部用户，如第三方服务提供商）。这必须解决与未经授权访问其技术系统的风险水平相称的逻辑和物理技术访问控制。 10.56金融机构必须采用可靠的认证流程，以确保使用中身份的真实性。认证机制应与功能的重要性相称，并至少采用这三个基本认证因素中的一个或多个，即用户应知（例如密码、PIN）、用户应有（例如智能卡、安全设备）和用户应是（例如生物特征，例如指纹或虹膜）。 10.57金融机构应定期审查和调整其密码做法，以增强抵御不断演变的攻击的能力。这包括有效和安全地生成密码。必须设置适当的控件来检查创建的密码的强度。 10.58依赖于多个因素的身份验证方法通常比单因素系统更难统一。有鉴于此，鼓励金融机构适当设计和实施（特别是在高风险或“单点登录”系统中）更可靠、更能遏制欺诈的多因素认证（MFA）。	客户应建立适当的访问控制政策，采用可靠的认证方式，如多因素认证。另外，客户还应定期审查和更新密码策略，保障密码的安全性。 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。 华为云的**云审计服务（Cloud Trace Service，简称CTS）**，可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和	为配合客户满足监管要求： （1）每一位华为云客户在华为云都拥有唯一可辨识的用户ID，并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支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。 IAM同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、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。 如果用户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问用户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。 （2）华为云内部建立了运维和运营账号管理机制。华为云运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。此外，还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。所有运维账号由LDAP集中管理，通过统一运维审计平台集中监控并进行自动审计,以实现从创

原文编号	具体控制要求	客户的关注	华为云的内部实践
		问题定位等常见应用场景。	建用户、授权、鉴权到权限回收的全流程管理,并根据不同业务维度和相同业务不同职责，实行RBAC权限管理，保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。
补丁管理 10.65	金融机构必须建立补丁管理框架，该框架应满足以下要求： （a）对所有技术资产进行识别和风险评估，以确定未部署补丁程序引起的潜在漏洞； （b）对关键补丁进行兼容性测试； （c）根据修补程序的严重性指定部署修补程序的周转时间；以及 （d）遵守端到端修补程序部署流程的工作流程，包括批准、监控和跟踪活动。	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（Image Management Service，简称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。	作为云服务提供商： （1）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。 （2）华为云产品安全事件响应团队（CSIRT）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。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用户业务造成影响。

5.2 网络安全管理

原文编号	具体控制要求	客户的关注	华为云的内部实践
网络安全运营 11.7-11.9	11.7 金融机构必须部署有效的工具，支持对其技术基础设施中的异常活动进行持续、主动的监测和及时发现。监测范围必须涵盖所有关键系统，包括支持性基础设施。 11.8 金融机构必须确保其网络安全业务能够持续地防止和发现其安全控制的任何潜在危害或其安全态势的削弱。对于大型金融机构，这必须包括对支持所有关键系统的外部和内部网络组件进行季度脆弱性评估。 11.9 金融机构必须每年对其内部和外部网络基础设施以及包括网络、移动和所有面向外部的应用程序在内的关键系统进行以情报为导向的渗透测试。渗透测试应反映基于新出现和演变的威胁场景的极端但似乎合理的网络攻击场景。金融机构必须聘请适当认可的渗透测试人员和服务提供商来履行这一职能。	客户应部署有效的工具以对技术基础设施进行监控，并每季度对关键系统的网络组建进行脆弱性评估，每年对网络基础和关键系统进行渗透测试。 华为云的**云审计服务（Cloud Trace Service，简称CTS）**为用户提供云服务资源的操作记录，供用户查询、审计和回溯使用。	为配合客户满足监管要求： **（1）**华为云的**云审计服务（CTS）**记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的API执行的操作，以及华为云系统内部触发的操作。CTS会对各服务发送过来的日志数据进行检视，使数据本身不含敏感信息；在传输阶段，通过身份认证、格式校验、白名单校验以及单向接收机制等手段，保障日志信息传输和保存的准确；在保存阶段，采取多重备份，并根据华为网络安全规范要求，对数据库自身安全进行安全加固，杜绝仿冒、抵赖、篡改以及信息泄露等风险；最后，CTS支持数据以加密的方式保存到OBS桶。同时，华为云有集中、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，以助力支撑网络安全事件回溯。 **（2）**华为云产品安全事件响应团队（CSIRT）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CSIRT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。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用户业务造成影响。

原文编号	具体控制要求	客户的关注	华为云的内部实践
			（3）华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。华为云已与合作伙伴联合推出了主机入侵检测、Web 应用防火墙、主机漏洞检测、网页防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力。
分布式拒绝服务（DDoS） 11.13	金融机构必须通过以下措施，确保其技术系统和基础设施，包括外包给第三方服务提供商或由第三方服务提供商托管的关键系统，受到充分保护，免受各类DDoS攻击（包括批量、协议和应用层攻击）： （a）订阅DDoS缓解服务，包括自动“清洁管道”服务，以过滤和转移网络带宽以外的任何潜在流量； （b）定期评估提供商按需扩展网络带宽的能力，包括上游提供商的能力、提供商事件响应计划的充分性及其对攻击的响应能力；以及 （c）实施缓解基于域名服务器（DNS）的层攻击的机制。	客户应建立防DDoS攻击机制，购买防DDoS攻击服务，定期评估供应商按需拓展网络带宽的能力，实施防DNS层攻击的措施。 华为云为客户提供两种防DDoS攻击服务：**Anti-DDoS流量清洗服务（简称Anti-DDoS）**和**DDoS高防（Advanced Anti-DDoS，简称AAD）**。	为配合客户满足监管要求，华为云为客户提供两种防DDoS攻击服务： （1）Anti-DDoS是一种流量清洗服务，为客户的华为云内资源（弹性云服务器、弹性负载均衡），提供网络层和应用层的DDoS攻击防护，并提供攻击拦截实时告警，有效提升用户带宽利用率，保障业务稳定可靠。AAD则可服务于华为云和非华为云的主机，用户可以通过修改DNS解析或对外服务地址为高防IP，将恶意攻击流量引流到高防IP清洗，助力重要业务不被攻击中断。 （2）华为云的防DDoS攻击服务提供精细化的抵御DDoS攻击的功能，包括但不限于Ping Flood、SYN Flood、UDP Flood、Challenge Collapsar、HTTP Flood 、DNS Flood。用户只需根据租用带宽及业务模型自助配置防护阈值，系统检测到攻击后就会实时通知用户并进行有效防御。 （3）华为云的防DDoS攻击服务还通过华为云自身的一系列技术，如安全的基础架构平台、安全组网及边界防护、虚拟机网络隔离、API 接口安全与日志审计等，增强其安全能力，保障防DDoS攻击服务服务自身的业务安全。

原文编号	具体控制要求	客户的关注	华为云的内部实践
数据防泄漏（DLP） 11.15	金融机构必须设计内部控制程序，并在所有应用程序和访问点中实施适当的技术，以实施DLP策略并触发任何违反策略的行为。部署的技术必须涵盖以下内容： （a）使用中的数据-IT资源正在处理的数据； （b）数据动态-数据正在网络上传输；和 （c）静态数据–存储在诸如服务器，备份介质和数据库之类的存储介质中的数据。	客户应建立数据防泄漏机制，并通过适当的技术手段来防止数据泄露，部署的技术应覆盖数据使用、数据传输、数据存储等数据生命周期。 华为云为客户提供了**数据加密服务（Data Encryption Workshop，简称DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。	为保障客户安全的处理云上数据，华为云对数据生命周期的各阶段进行层层防护： **（1）数据创建：**华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据。客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，使客户内容数据存储在目标位置。当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，使客户只能访问到自己的数据。 **（2）数据存储：**目前，**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，采用高强度的算法对存储的数据进行加密。服务端加密功能集成了华为云**数据加密服务（DEW）**的密钥管理功能，由DEW进行密钥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。 **（3）数据使用：**华为云从数据访问控制、安全防护、审计等方面为客户提供了相关服务，协助客户对数据的使用和流转做到更加细粒度的管控。更多信息可参见《华为云数据安全白皮书》4.5。 **（4）数据传输：**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。针对客户业务混合云部署和全球化布局的场景，可以使用华为云提供的虚拟专用网络（VPN）、云专线服务、云连接等服务，实现不同区域之间业务的互联互通和数据传输安全。

原文编号	具体控制要求	客户的关注	华为云的内部实践
			（5）数据归档：华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用**对象存储服务（OBS）**的版本控制、**云硬盘备份（VBS）**、**云服务器备份（CSBS）**等功能，将云上的文档、硬盘、服务器进行备份。通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。 **（6）数据销毁：**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，华为云会严格遵循适用的法律法规，以及与客户之间的协议约定，按照数据销毁标准清除客户的数据。

原文编号	具体控制要求	客户的关注	华为云的内部实践
安全运营中心（SOC） 11.17	11.17 金融机构必须确保其SOC（无论是内部管理还是由第三方服务提供商管理）具有足够的能力来主动监控其技术安全状况。这将使金融机构能够检测异常的用户或网络活动，标记潜在的违规行为，并根据警报的复杂程度建立由熟练资源支持的适当响应。SOC活动的结果还应告知金融机构对其网络安全状况和策略的审查。	客户应建立安全运营中心，对用户和网络活动进行监控，识别违规行为，并进行适当的响应。	作为云服务提供商： **（1）**华为云有集中、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，日志包含资源ID(如：源IP、主机ID、用户ID等)、事件类型、日期时间、受影响的数据/组件/资源的ID（如目的IP、主机ID、服务ID等）、成功或失败等信息，以助力支撑网络安全事件回溯。该日志分析系统有强大的数据保存及查询能力，使所有日志保存时间超过180天，90天内可以实时查询。华为云有专门的内审部门，定期对运维流程各项活动进行审计。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。 **（2）**华为云建立了合理、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；Anti-DDoS 快速发现和防护DDoS 攻击；WAF 实时检测和防御Web 攻击；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。针对公有云攻击的手段多样、流量巨大的特点，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。 更多关于内容请参见**《华为云安全白皮书》**8.3安全日志和事件管理。

原文编号	具体控制要求	客户的关注	华为云的内部实践
网络响应和恢复 11.22-11.25	11.22 金融机构必须建立全面的网络危机管理政策和程序，将网络攻击场景和响应纳入组织的整体危机管理计划，升级流程，业务连续性和灾难恢复计划中。这包括制定清晰的沟通计划，以在发生网络事件时让股东，监管机构，客户和员工参与进来。 11.23 金融机构必须建立并实施全面的网络事件响应计划（CIRP）。 11.24 金融机构必须确保相关的网络应急团队（CERT）成员熟悉事故响应计划和处理程序，并始终保持联系。 11.25 金融机构必须根据各种当前和新出现的威胁情景（例如，社会工程学），在董事会，高级管理层，和相关第三方服务提供商等主要利益相关者的参与下，进行年度网络演习，以测试CIRP的有效性。	客户应当建立网络危机管理政策和流程，制定并实施网络安全事件响应计划并确保网络应急团队成员对此的熟悉。另外，还应每年开展网络安全演习，测试网络安全事件响应计划的有效性。	作为云服务提供商： **（1）**华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM – Security Information and Event Management）系统如ArcSight、Splunk对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、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，会根据具体情况向客户提供事件报告。 **（2）**基于云面临环境下存在复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，从而在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。同时，根据内部信息安全管理体系和业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。

5.3 科技审计

原文编号	具体控制要求	客户的关注	华为云的内部实践
科技审计 12.5	金融机构必须建立科技审计计划，以适当覆盖关键技术服务，第三方服务提供商，重要的外部系统接口，延迟或过早终止的关键技术项目，以及对新的或重要改进的技术服务进行实施后审查。	客户应制定科技审计计划，并对关键技术服务，第三方服务提供商，重要的外部系统接口等实施审查。	作为云服务提供商，华为云会安排专人积极配合客户发起的审计要求。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。

5.4 内部意识和培训

原文编号	具体控制要求	客户的关注	华为云的内部实践
内部意识和培训 13.1-13.4	13.1 金融机构必须为所有员工发挥各自的作用提供适当的定期技术和网络安全意识教育，并衡量其教育和意识计划的有效性。这种网络安全意识教育必须至少每年由金融机构进行一次，并且必须反映当前的网络威胁形势。 13.2 金融机构必须为从事技术运营，网络安全和风险管理的员工提供充分和连续的培训，以确保他们有能力有效地履行其职责。 13.3为了满足第13.2款的要求，大型金融机构应确保从事日常IT运营（例如IT安全，项目管理和云运营）的员工也得到适当认证。 13.4金融机构必须向其董事会成员提供有关技术发展的定期培训和信息，以使董事会能够有效地履行其监督职责。	客户应建立网络安全培训机制，定期对全体员工进行安全意识培训，对专业人员进行安全风险管理和技术培训，以确保其能够有效履行职责。	作为云服务提供商，为了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，华为对全体员工从意识教育普及、宣传活动开展、商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育。参考业界优秀实践，华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，提升员工能力，向客户交付安全的产品、解决方案与服务。为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，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。更多关于内容请参见**《华为云安全白皮书》**4.4人力资源管理。

6 华为云如何遵从及协助客户满足 BNM《外包》的要求

马来西亚国家银行于2019年10月23日发布了《外包》。该规定从董事会和高级管理层的职责、外包流程与风险管理、马来西亚境外的外包、涉及云服务的外包、外包安排的批准、外包计划的提交等领域提出对金融机构外包管理相关要求。其中外包流程与风险管理包括服务提供商评估、外包协议、数据机密性保护、业务连续性计划领域的要求。

金融机构在遵循《外包》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《外包》中与云服务供应商相关的控制要求，并阐述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。

6.1 外包流程与风险管理

原文编号	具体控制要求	客户的关注	华为云的内部实践
服务提供商评估 9.3	金融机构在考虑所有新安排、更新或重新谈判现有安排时，必须对服务提供商进行适当的尽职调查。尽职调查过程的范围和深度必须与外包活动的重要性相称。尽职调查过程必须至少包括： （a）容量、能力、财务实力和商业信誉； （b）风险管理和内部控制能力，包括物理和IT安全控制以及业务连续性管理； （c）外包活动的地点（如城市和国家），包括主要和备用地点； （d）金融机构和央行对服务提供商的访问权； （e）确保数据保护和机密性的措施和程序； （f）对分包商的依赖（如有），特别是在分包对外包安排的执行增加了更多复杂性的情况下； （i）服务提供商遵守本政策文件相关法律、法规和要求的能力。	客户应在所有新服务开始或服务发生变更前，对服务提供商进行适当的尽职调查,应包括技术能力、财力、商业信誉、风险管理能力、外包活动的地点、数据安全、分包商的依赖等等。	作为云服务供应商，华为云在上述方面的情况如下： **（1）技术能力：**华为云用在线提供云服务的方式，将华为30多年在ICT基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 **（2）财力：**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《Market Share: IT Services, worldwide 2019》报告显示，华为云全球IaaS市场排名第六，中国市场排名前三，全球增速最快，高达222.2%。 **（3）商业声誉：**华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现大突破。 **（4）风险管理能力：**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。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

原文编号	具体控制要求	客户的关注	华为云的内部实践
			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。 **（5）数据中心地理位置：**客户购买云服务时可自行选择数据中心，华为云遵循客户的选择。华为云不会在未经客户同意的情况下将客户内容从选择的区域中迁移，除非（a）必须迁移以遵守适用的法律法规或者政府机关的约束性命令;（b）为了提供账单、管理、技术服务或者出于调查安全事件或调查违反合同规定的行为。 **（6）金融机构与监管机构的访问权：**参见本文档**6.1外包流程与风险管理**下的**“外包协议”**相关内容。 **（7）数据安全：**参见本文档**6.1外包流程与风险管理**下的**“数据机密性的保护”**相关内容。 **（8）分包管理：**为配合客户行使对服务提供商监管，华为云线上的**《华为云用户协议》**对客户和华为云的安全职责进行划分，**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的具体要求，在其中规定华为云若聘用分包商，需通知客户，并对分包的服务负责。华为云制定了自身的供应商管理机制，从供应商的产品和供应商本身的内部管理都提出了安全需求。此外，华为云会对供应商进行定期的稽核。此外会与涉及网络安全的供应商签署网络安全协议，在服务过程也中会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应商进行合作降级处理。 **（9）适合金融机构的企业文化和服务政策：**华为云在产品和服务规划和阶段会根据客户业务场景、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

原文编号	具体控制要求	客户的关注	华为云的内部实践
			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。
外包协议 9.6、9.7	9.6外包协议必须由具有法律效力的书面协议管辖。外包协议至少必须规定以下方面内容：服务期限、服务提供商的责任、服务的安全性控制、数据的使用范围、服务提供商审查、业务连续性计划、通知义务、违约条款、终止条款等。 9.7 外包协议还必须包含以下条款：（a）使央行能够直接、及时和不受限制地访问与外包活动有关的系统和任何信息或文件；（b）在央行认为必要时，使央行能够对服务提供商进行现场监督；（c）央行认为必要的情况下，使央行能够指定一个独立方对服务提供商与外包活动相关的系统、信息或文件进行审查；以及（d）当央行向金融机构发出指示时，允许金融机构修改或终止安排。	客户应与服务提供商签订具有法律效力服务协议，并保证协议条款的合法性和适宜性。	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。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。

原文编号	具体控制要求	客户的关注	华为云的内部实践
数据机密性的保护 9.8、9.9	9.8金融机构必须使自己确信，服务提供商的安全控制、治理、政策和程序水平是可靠的，以保护外包安排下共享信息的安全和机密性。 9.9金融机构必须确保适当的控制措施到位，并有效地保护与服务提供商共享的任何信息的安全性、机密性和完整性。在满足这一要求时，金融机构必须确保： （d）如果服务提供商位于马来西亚境外或执行外包活动，则服务提供商须遵守与马来西亚相当的数据保护标准; （e）当服务提供商向多个客户提供服务时，金融机构的信息必须与服务提供商的其他客户的信息分开; （f）即使在协议终止后，服务提供商仍受外包协议规定的保密条款的约束；以及 （g）一旦外包安排终止或终止，与服务提供商共享的信息将被销毁、无法使用或及时、安全地返还给金融机构；	客户应采取协议约束、审查监督等方式确保服务供应商的安全政策、程序和控制措施的安全可靠，并能够有效保护其客户信息的保密性和安全性。 在服务协议终止时，客户可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移服务（Server Migration Service，简称SMS）**，将内容数据从华为云中迁移出去，如迁移至本地数据中心。	为配合客户满足监管要求： **（1）**华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户所在国家或地区的安全法规以及行业监管要求的基础上，参考业界最佳实践从组织、流程、规范、技术、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，助力客户的安全需求。同时，华为云目前获得了国际上多项权威的安全与隐私保护认证，第三方测评公司也会定期对华为云展开保密性、安全充分性和合规性的审核并出具专家报告。 **（2）**华为云不用客户数据做商业变现，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，或者为遵守适用的法律法规或政府机关的约束性命令，并遵守马来西亚《个人数据保护法》所述的数据保护原则。 **（3）**华为云各服务产品和组件从设计之初就规划并实现了合理的隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。 **（4）**在客户确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，使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，使其上的数据无法恢复。

原文编号	具体控制要求	客户的关注	华为云的内部实践
业务连续性计划 9.10、9.13、9.14	9.10 金融机构负责确保其业务连续性计划应考虑服务提供商的任何运营中断或故障。 9.13 金融机构必须始终确保能够随时查阅服务提供商关于外包活动的所有记录和信息，这是金融机构开展业务和履行其法律和监管义务所必需的。 9.14金融机构必须定期测试自己的业务连续性计划，并主动寻求对服务提供商和相关的替代服务提供商的业务连续性计划准备状态的保证。业务连续性计划测试和评估的强度和规律性必须与外包安排的重要性相称。在评估这种准备时，金融机构至少必须： （a）确保备用装置可用，并在必要时准备好运行； （b）确保服务提供商定期测试其业务连续性计划，并提供可能影响外包服务提供的任何测试报告，包括任何已确定的缺陷，以及尽快解决此类缺陷的措施；以及 （c）对于重大外包安排，与服务提供商的联合测试，以便金融机构能够对这些安排进行端到端业务连续性计划测试。	客户应确保其指定的的业务连续计划考虑服务提供商的运营中断或故障，与服务提供商约定其对外包活动记录和信息访问权。另外，客户还应定期测试业务连续性计划，同时也确保服务提供商测试其业务连续性计划，并持续改进。	为配合客户满足监管要求： **（1）**为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得ISO22301认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 **（2）**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。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。 **（3）**客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵循相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。 **（4）**华为云作为客户的供应商，会积极配合客户发起的测试需求，协助客户测试其业务连续性计划的有效性。 同时，华为云根据内部业务连续性管理体系的要求，每年对业务连续性计划和灾难恢复计划进行测试，所有的应急响应人员，包括后备人员均需参与。测试的类型包括桌面演练、功能演练和全面演练三种，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，若测试结

原文编号	具体控制要求	客户的关注	华为云的内部实践
			果表明业务连续性计划、恢复策略或应急预案等存在不足之处，将对相关文件进行更新。

6.2 马来西亚境外的外包

原文编号	具体控制要求	客户的关注	华为云的内部实践
马来西亚境外的外包 10.1-10.3	10.1 如果服务提供商位于马来西亚境外或执行外包活动，外包安排会使金融机构面临额外风险（例如国家风险）。金融机构应建立适当的控制和保障措施，以管理这些额外的风险，同时考虑到社会和政治条件、政府政策以及法律和监管发展。 10.2在进行尽职调查过程中，金融机构必须确保此类评估涉及与马来西亚境外外包相关的额外风险，以及金融机构或服务提供商及时对新出现的风险事件采取适当应对措施的能力。 10.3金融机构必须确保在马来西亚境外进行的外包安排不会影响： （a）金融机构有效监控服务提供商和执行机构业务连续性计划的能力； （b）金融机构在服务提供商失败的情况下根据特定管辖区的法律迅速恢复数据；以及 （c）央行行使其监管或监督权力的能力，特别是央行及时和不受限制地获取与外包活动有关的系统、信息或文件的能力。	客户在选择境外的外包服务供应商时，应提前对其进行尽职调查，保证外包服务供应商的政府政策、经济情况、法律监管以及服务能力符合客户业务发展的需要以及监管要求。	为配合客户满足监管要求，华为云会安排专人积极配合客户的尽职调查。此外，华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户所在国家或地区的安全法规以及行业监管要求的基础上，参考业界最佳实践从组织、流程、规范、技术、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，助力客户的安全需求。 更多信息请参见本文档**6.1外包流程与风险管理**下的“**业务连续性计划**”的相关内容。

6.3 涉及云服务的外包

原文编号	具体控制要求	客户的关注	华为云的内部实践
涉及云服务的外包 11.3、11.4	11.3 关于金融机构根据第9.6（f）款对云服务提供商和分包商进行审计和检查的能力，金融机构可依赖云服务提供商为审计提供的第三方认证和报告，前提是这种依赖基于对审计范围和第三方采用的方法有充分的了解和审查，并能与第三方和服务提供商联系，澄清与审计有关的事项。 11.4 关于根据第9.6（i）款对云服务提供商的业务连续性计划进行的测试，金融机构必须能够获取有关此类云服务提供商因业务连续性计划测试而实施的控制的稳健性状态的信息。	客户应定期对云服务供应商进行审查，或者获取第三方的认证和报告。另外，客户还应获取云服务提供商在业务连续性管理方面的信息。	为配合客户满足监管要求，华为云会安排专人积极配合客户发起的审计要求。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。 关于华为云在业务连续性管理方面的信息请参见本文档**6.1 外包流程与风险管理**下的“**业务连续性计划**”的相关内容。

7 华为云如何遵从及协助客户满足 BNM《客户信息管理与许可披露》的要求

马来西亚国家银行于2021年10月21日发布了《客户信息管理与许可披露》，取代2017年10月17日发布的《客户信息管理和允许披露》。该规定从董事会监督、高级管理层、控制环境、客户信息泄露、外包服务提供商等领域提出对金融机构客户信息管理相关要求。其中控制环境包括风险评估、政策和程序、信息和通信技术控制、访问控制、物理安全、独立审查等方面的要求。

金融机构在遵循《客户信息管理与许可披露》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《客户信息管理与许可披露》中与云服务供应商相关的控制要求，并阐述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。

7.1 控制环境

原文编号	具体控制要求	客户的关注	华为云的内部实践
风险评估 10.1、10.2	10.1 金融服务提供商必须识别可能导致盗窃、丢失、误用或未经授权的访问、修改或泄露的潜在威胁和漏洞。 10.2 金融服务提供商还必须评估此类威胁和漏洞出现的可能性，以及在发生客户信息泄露事件时对金融服务提供商及其客户造成的潜在影响。	客户应识别潜在的安全威胁和漏洞，并评估威胁和漏洞发生的可能性，以及在发生安全事件时造成的潜在影响。作	为云服务供应商，华为云已制定并实施了完善的物理和环境安全防护策略、规程和措施，满足GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中的T3+ 标准。同时，华为云运维运营团队定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急响应等措施。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，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。
政策和程序 10.6、10.11	10.6 金融服务提供商必须制定并实施书面政策和程序，以保护客户信息，包括客户信息的收集、存储、使用、传输、共享、披露和处置。 10.11 金融服务提供商必须不断审查其政策和程序，以确保其充分、相关，并有效地应对运营环境的变化。	客户应制定并实施数据安全政策和程序，对客户信息的全生命周期进行保护。另外，客户持续审查其政策和程序，以确保其充分性和有效性。	为保障客户安全的处理云上数据，华为云对数据生命周期的各阶段进行层层防护，具体请参见本文档**5.2网络安全管理**下的**“数据防泄漏管理”**的相关内容。此外，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	具体控制要求	客户的关注	华为云的内部实践
控制措施-信息和通信技术(ICT)控制 10.12、10.13、10.20、10.21	10.12 金融服务提供商必须部署预防性和检测性的信息通信技术控制，以防止盗窃、丢失、误用或未经授权访问、修改或披露客户信息，并在发生错误和违规行为时进行检测。 10.13 金融服务提供商必须定期监测这些控制措施的有效性，以确保它们能够对不断变化的威胁作出反应。 10.20 金融服务提供商必须建立机制，对员工以任何未经授权的方式披露客户信息的行为产生强大的威慑作用。 10.21 未经授权的披露可能以多种方式和形式发生，如员工拍摄包含客户信息的文件或屏幕。第10.20段所述机制可包括提高工作人员对以任何方式进行未经授权披露的纪律处分的认识，在相关区域安装闭路电视，实行开放式办公室概念，鼓励检举，或在数据中心、交易室、呼叫中心等高风险区域限制使用个人电子设备。	客户应部署预防性和检测性的信息通信技术控制，并定期进行监控，同时建立信息泄露的问责机制。 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。 华为云的**云审计服务（Cloud Trace Service，简称CTS）**，可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。	为配合客户满足监管要求： （1）华为云的**统一身份认证服务（IAM）**为客户提供云上资源访问控制。使用 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；**云审计服务（CTS）**可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。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触发的操作。 同时，华为云不用客户数据做商业变现，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，或者为遵守适用的法律法规或政府机关的约束性命令。内部运维人员接入华为云管理网络对系统进行集中管理时，需采用双因子认证进行身份认证，如 USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。 （2）华为建立了严密的安全责任体系，贯彻违规问责机制。一方面，华为云恪守责任共担模型，履行华为云的各项责任，对华为云一方造成的安全违规，华为云对用户直接负责，最大限度控制对用户业务的影响。另一方面，华为云要求每个员工都对自己工作中的行为和结果负责，不仅要对技术和服务负责，也要承担法律的责任。华为云员工深知，安全问题一旦发生，可能会对用户、公司带来极大影响。因此不管故意还是无意，华为云都会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。对触犯法律法规的，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

原文编号	具体控制要求	客户的关注	华为云的内部实践
			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。 （3）华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行7*24 小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。
访问控制 10.26、10.27	10.26 金融服务提供商必须确定客户信息在不同系统中的位置，并确保在不同级别（即应用程序级别、数据库级别、操作系统级别和网络级别）有足够的访问控制，以防止通过任何手段向外部进行的未经授权的访问、修改或披露。 10.27 金融服务提供商必须定期审查员工的访问权限，并立即撤销离开金融服务提供商或换到不需要访问客户信息的新角色或职位的员工的访问权限，以防止客户信息被盗。	客户应建立对客户信息的访问控制机制，以防止对系统未经授权的访问，并定期审查员工的访问权限，及时收回离职人员权限和更新调岗人员权限。 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。 华为云的**云审计服务（Cloud Trace Service，简称CTS）**，可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。	为配合客户满足监管要求： （1）IAM除了支持密码认证之外还支持多因子认证，客户可自主选择是否启用。如果用户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问用户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。 （2）华为云内部建立了运维和运营账号管理机制。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证。所有运维账号由LDAP集中管理，通过统一运维审计平台集中监控并进行自动审计。以实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行RBAC权限管理。保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。

原文编号	具体控制要求	客户的关注	华为云的内部实践
物理安全 10.28、10.29、10.32	10.28 金融服务提供商必须实施充分的物理安全控制，以确保以纸质或电子形式存储的客户信息得到适当保护，以防任何形式的盗窃、丢失、误用或未经授权的访问、修改或披露。 10.29 金融服务提供商必须限制访问，并在可以访问和存储大量客户信息的区域（例如服务器和文件室）使用强大的入侵者威慑。 10.32为了在客户信息的整个生命周期内有效地保护客户信息，金融服务提供商必须有适当的程序来识别从操作角度或任何成文法的要求来看不再需要的客户信息。金融服务提供商应采用适当的方法，安全地处理此类客户信息，包括客户信息的任何纸质和数字记录。	客户应当建立物理安全管理机制，在可访问和存储大量客户信息的区域采取访问控制措施，防止客户信息被窃取、丢失或未经授权的使用。另外，客户还应识别不再需要的客户信息，并采用实当的方式进行处置。	作为云服务提供商： **（1）**华为云已制定并实施了物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3+标准。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，而且提供了合理足够的物理空间、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定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急响应等措施。 **（2）**华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了全天候保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，使非授权人员不可访问数据中心。 **（3）**华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、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

原文编号	具体控制要求	客户的关注	华为云的内部实践
			供有效的数据保护能力，助力用户对其数据的隐私权、所有权和控制权不受侵犯。在客户终止使用华为云服务，需要对内容数据进行销毁时，华为云会对指定的数据及其所有副本进行清除。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，使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，使其上的数据无法恢复。

原文编号	具体控制要求	客户的关注	华为云的内部实践
员工，代表，代理商和外部供应商的人员 10.39、10.40、10.42-10.45、10.49、10.50	10.39金融服务提供商必须确保雇佣合同包含一项条款，要求所有员工签署一份保密承诺，明确规定任何书面法律保护客户信息的义务和要求，以及未能遵守该义务和要求的后果。 10.40如果金融服务提供商与外部供应商合作，在金融服务提供商的场所内履行职责或提供服务（如保安、清洁工和维护人员/工程师），金融服务提供商必须确保外部供应商对其人员进行适当程度的审查和监控，以降低客户信息被盗的风险。 10.42 金融服务提供商必须进行强有力的监控，以确保金融服务提供商制定的相关政策、程序和控制措施得到员工的遵守。 10.43 金融服务提供商必须提供相关培训，并定期提醒所有员工正确处理客户信息的义务。 10.44 金融服务提供商必须在其新员工培训计划中包括一项具体培训，以解释有关保护客户信息的政策和程序。 10.45金融服务提供商应向新员工进行提醒，告知其可能因不遵守政策和程序而采取的行动。	客户应要求所有员工签署保密承诺，明确保护客户信息的业务和要求。客户应对员工进行监控确保其遵守公司安全政策，并要求外部供应商对其人员进行适当的审查和监控。此外，客户还应对员工进行信息安全意识培训，并对违反安全政策的员工进行调查和适当处置。	作为云服务提供商： （1）华为云参照各类法规要求、监管要求、国际或行业标准建立了一套完善的信息安全和隐私保护管理体系，并持续改进。该管理体系在物理安全管控、系统安全、安全意识培训等众多安全领域均有详细的政策和程序。华为云持续践行管理体系的要求，保障客户的业务和数据安全。 （2）华为云制定了完善的安全意识培训计划，在员工入职、在岗、转岗等环节纳入多种形式的安全意识培训，使员工行为符合所有适用的法律、政策、流程以及华为商业行为准则的要求。 （3）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。客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。 （4）华为建立了严密的安全责任体系，贯彻违规问责机制。一方面，华为云恪守责任共担模型，履行华为云的各项责任，对华为云一方造成的安全违规，华为云对用户直接负责，最大限度控制对用户业务的影响。另一方面，华为云要求每个员工都对自己工作中的行为和结果负责，不仅要对技术和服务负责，也要承担法律的责任。华为云员工深知，安全问题一旦发生，可能会对用户、公司带来极大影响。因此不管故意还是无意，华为云都会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。对触犯法律法规的，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

原文编号	具体控制要求	客户的关注	华为云的内部实践
	10.49 金融服务提供商必须在发现员工以任何方式窃取、丢失、滥用或未经授权访问、修改或披露客户信息时进行彻底及时的调查，并对相关员工采取适当行动。 10.50 根据第10.49段采取的行动必须向所有工作人员发出强烈的信息，并起到威慑作用，防止今后再次发生客户信息泄露事件。		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。
独立审查 10.53	金融服务提供商必须至少每两年对其保护客户信息的政策、程序和控制措施进行一次独立审查。	客户应定期对其保护客户信息的政策、程序和控制措施进行独立审查。	作为云服务提供商，华为云会安排专人积极配合客户发起的审计要求。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。

7.2 客户信息泄露

原文编号	具体控制要求	客户的关注	华为云的内部实践
客户信息泄露 11.1-11.6、11.12、11.13	11.1 在客户信息被盗、丢失、误用或未经授权的访问、修改或泄露的情况下，金融服务提供商必须制定客户信息泄露处理和响应计划。 11.2 金融服务提供商根据第11.1款制定的计划必须至少包括上报程序和明确的责任线，以遏制客户信息泄露并采取补救措施。 11.3金融服务提供商必须确保员工了解上报程序，并对相关员工进行培训，以便对客户信息泄露采取适当的补救措施，有效地保护受影响客户的利益。 11.4金融服务提供商必须建立一种机制，以识别客户信息泄露，包括因客户投诉而产生的信息泄露，并及时、适当地调查投诉。 11.5金融服务提供商必须采取适当的缓解措施，立即遏制客户信息泄露。 11.6金融服务提供商必须评估因盗窃、丢失、滥用或未经授权访问、修改或披露客户信息而产生的影响。 11.12如果客户信息泄露影响到大量客户，金融服务提供商必须评估潜在影响，并采取适当措施避免	客户应当建立客户信息泄露事件管理机制，制定客户信息泄露处理和响应计划，明确上报流程和人员职责，建立客户事件泄露识别程序，并采取适当缓解措施。此外，客户还应评估客户泄露事件的影响，并及时通知客户。	作为云服务提供商： （1）华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM – Security Information and Event Management）系统如ArcSight、Splunk对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。 （2）华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、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，会根据具体情况向客户提供事件报告。 （3）华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。测试场景将结合当下常见的网络安全威胁，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，若测试结果表明信息安全事件管理程序和流程等存在不足之处，将对相关文件进行更新。同时，根据内部信息安全

原文编号	具体控制要求	客户的关注	华为云的内部实践
	或减少对受影响客户的任何损害。 11.13第11.12段中提到的行动可包括： （a）发布公告，及时通知客户，恢复客户信心； （b）为客户提供联系方式，以便客户获取进一步信息或提出与违规有关的任何问题；或 （c）向受影响的客户提供有关保护措施的建议，以防止违规可能造成的潜在损害。		管理体系和业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。

7.3 外包服务提供商

原文编号	具体控制要求	客户的关注	华为云的内部实践
外包服务提供商 12.2-12.4、12.6、12.7	12.2 金融服务提供商在选择能够访问客户信息（包括处理、存储或处置客户信息）的外包服务提供商时，必须进行充分和相关的尽职调查评估。 12.3金融服务提供商必须确保外包服务提供商制定了与金融服务提供商相当的政策、程序和控制措施，以确保客户信息始终得到妥善保护。 12.4为了确保在与外包服务提供商签订的服务水平协议（SLA）中充分体现保护客户信息的义务，SLA中必须要求外包服务商： (a)承诺保护客户信息，防止任何以任何方式进行盗窃、丢失、误用或未经授权的访问、修改或披露; (b)确保其政策和程序的充分性和有效性，以保护金融服务提供商的客户信息; (c)对处理客户信息的人员进行严格审查; (d)只允许其人员严格获取客户信息，以履行其职能; (e)确保其人员理解并承诺遵守禁止任何人以任何方式披露任何客户信息的要求，但SLA规定的其他目的，如根据书面法律允许或经银行批准，则应视情况（包括在合同期结束后）而定;	客户应建立外包服务提供商安全管理机制，对服务提供商进行尽职调查，并确保服务提供商制定适当的安全政策、程序和控制措施。客户还应与服务供应商签署服务水平协议和保密协议，约定服务供应商保护客户信息的义务。此外，客户还应要求服务供应商对其员工进行客户信息安全的培训，并定期审查其培训计划的充分性和有效性。	为配合客户满足监管要求： （1）华为云会安排专人积极配合客户发起的审计要求和尽职调查。华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界标准，在身份认证与访问控制、权限管理、数据隔离、传输安全、存储安全、数据删除、物理销毁、数据备份恢复等方面，采用主流技术、实践和流程，助力用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供有效的数据保护。另外，华为云制定了突发事件应急预案，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，使云服务持续运行，保障客户的业务和数据安全。 （2）华为云参照ISO27001构建了完善的信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性。全方位保护客户系统和数据的保密性、完整性和可用性。 （3）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。 （4）华为云不用客户数据做商业变现，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，或者为遵守适用的法律法规或政府机关的约束性命令。华为云会安排专人积极

原文编号	具体控制要求	客户的关注	华为云的内部实践
	(f)调查任何客户信息泄露，以确定违规发生的时间及方式; (g)在规定的时限内向金融服务提供商报告任何客户信息泄露事件; (h)根据第10.32段销毁，或在SLA到期或终止时将所有客户信息退还给金融服务提供商;和 (i)允许金融服务提供商审核或检查如何保护客户信息。 12.6金融服务提供商必须要求外包服务提供商就客户信息的处理签署具有约束力的保密承诺。 12.7金融服务提供商必须确保外包服务提供商定期对其员工进行有关正确处理客户信息的相关政策和程序的培训，并审查培训计划的充分性和有效性。		配合客户发起的保密要求。华为云避免未经授权的信息披露的责任和行动、违反或终止协议时应采取的预期行动、客户对华为云的审计和监督权利等内容，会根据实际情况在与客户签订的协议中进行约定。 **（5）**华为云制定了完善的安全意识培训计划，在员工入职、在岗、转岗等环节纳入多种形式的安全意识培训，使员工行为符合所有适用的法律、政策、流程以及华为商业行为准则的要求。

8 华为云如何遵从及协助客户满足 BNM《发展金融机构的数据管理和管理信息系统框架指引》的要求

马来西亚国家银行于2011年5月9日发布了《发展金融机构的数据管理和管理信息系统框架指引》。该规定从数据治理、数据架构、内部控制与审查等领域提出对金融机构建立数据管理和管理信息系统框架的相关指导原则。

金融机构在遵循《发展金融机构的数据管理和管理信息系统框架指引》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《发展金融机构的数据管理和管理信息系统框架指引》中与云服务供应商相关的控制要求，并阐述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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
指导原则-原则 2 数据治理 4.12	如果数据由第三方服务提供商根据外包安排进行管理，高级管理层必须确保建立有效的监督、审查和报告安排，以确保始终遵守关于数据质量、完整性和可访问性标准的服务水平协议。	请参见本文档**5.3 科技审计**的相关内容。	请参见本文档**5.3 科技审计**的相关内容。
指导原则-原则 3 数据架构 4.14（VI）	应建立适当的数据存储和备份流程，这些流程可优化数据系统的功能，且能够高效及时地访问数据，以实现业务连续性管理。	请参见本文档**5.1 科技运营管理**下**“数据中心弹性-数据中心运营”**的相关内容。	请参见本文档**5.1 科技运营管理**下**“数据中心弹性-数据中心运营”**的相关内容。

原文编号	具体控制要求	客户的关注	华为云的内部实践
指导原则-原则 5 内部控制和审查 4.20、4.23、4.25、4.27	4.20金融机构必须建立充分的预防和检测控制，以确保系统和数据的逻辑和物理访问是安全的，并且只有被授权人出于特定目的才可以使用相关数据。 4.23对系统和数据的访问权限应明确定义、记录，并在适当的情况下进行隔离，以防止关键数据或系统受到危害。考虑到金融机构处理的大量数据的敏感性，通常应在“需要知道”的基础上提供访问权限。 4.25外部方（例如系统供应商和服务提供商）访问关键数据或系统必须得到适当授权。金融机构必须确保外部方的此类访问进行严格的监督，监视和适当限制，以保证其访问符合特定目的。签约服务的法律协议应明确禁止外部方未经授权披露机密数据，并应向金融机构提供适当的补救措施。 4.27应制定适当的保障措施，以确保个人数据不会被滥用或以不当方式披露。个人信息（客户、员工或金融机构可能与之开展业务的任何其他方的）应妥善处理，以确保信息的机密性并遵守相关法律。	请参见本文档**5.1 科技运营管理**下**“访问控制”**以及**7.1控制环境**下**“控制措施-信息和通信技术(ICT)控制”**的相关内容。	请参见本文档**5.1 科技运营管理**下**“访问控制”**以及**7.1控制环境**下**“控制措施-信息和通信技术(ICT)控制”**的相关内容。

9 华为云如何遵从及协助客户满足 BNM《业务连续性管理》的要求

马来西亚国家银行于2022年12月19日发布了《业务连续性管理》。该政策从董事会和高级管理层的责任、通知银行的中断情况、通知银行受到的干扰、向银行通知中断情况、业连管框架和方法等领域提出对金融机构的业务连续性管理相关要求。

金融机构在遵循《业务连续性管理》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《业务连续性管理》中与云服务供应商相关的控制要求，并阐述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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
9.15	为确保基本服务的持续可用性，金融机构必须制定应急安排，以便在中断期间提供这些基本服务，并将这些安排纳入BCP中。这包括由服务供应商根据外包安排代表金融机构提供的服务。	客户需制定根据风险偏好和场景制定BCP和应急安排，xu包括由服务供应商根据外包安排代表金融机构提供的服务。	为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管 理体系，并已获得IS0 22301认证。华为云每年会在组织内进行业务连续性的宣传和培 训，以及定期做应急演练和测试，持续优化应急响应机制。华为云安全演练团队定期 制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不 同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化 时，也会对业务连续性的有效性进行测试。 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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
9.25	为提高业连管的有效性，金融机构必须在与关键服务提供商、供应商和交易方的合同和外包安排中纳入以下要求和条款。 (a) 要求关键服务提供商、供应商和交易方为外包安排制定健全和有效的业连管计划，包括与金融机构的MTD和RTO相一致的具体MTD和RTO要求，以及在未达到MTD或RTO要求时的法律责任规定。 (b) 按照第9.50(d)段的规定，要求主要服务供应商参与金融机构的综合测试。 (c) 允许金融机构的内部审计或金融机构指定的其他独立方审查关键服务提供商、供应商和交易方的BCM；以及 (d) 允许金融机构查阅关键服务供应商、供应商和对手方保存的与外包安排有关的所有相关记录和资料。	客户需与关键服务提供商的合同和外包安排中要求关键服务提供商为外包安排：制定健全和有效的业连管计划；参与金融机构的综合测试；允许金融机构的内部审计或金融机构指定的其他独立方审查；允许金融机构查阅保存的与外包安排有关的所有相关记录和资料。	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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
9.37	金融机构必须建立其备用站点和恢复站点，以便在业务前提、基础设施或支持CBF的系统在发生中断时无法使用时可以使用。	客户需建立其备用站点和恢复站点，制定灾难恢复计划以支持CBF的连续运行。	技术恢复的备用地点： 为支撑云服务持续运行的关键业务制 定了恢复策略。客户可依赖华为云数 据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的 容灾和备份，数据中心按规则部署在 全球各地，客户可通过两地互为灾备 中心，如一地出现故障，系统在满足 合规政策前提下自动将客户应用和数 据转离受影响区域，保证业务的连续 性。同时，华为云还部署了全局负载 均衡调度中心，客户的应用在数据中 心实现N+1部署，即便在一个数据中心 故障的情况下，也可以将流量负载均 衡到其他中心。 华为云支持在一个数据中心的多个节 点内复制存放用户数据。单个节点一 旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。单个区 域内不同可用区之间，通过高速光纤 实现数据中心互联，满足跨可用区数 据复制基本要求，用户可根据业务需 求选择灾备复制服务。 灾难恢复测试： 华为云制定了业务连续性计划和灾难 恢复计划，并定期对其进行测试。华 为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中 心、数据中心、组织整体等）以及不 同场景的演练，以维护持续性计划的 有效性。
9.38	就第9.37段而言，备用站点和恢复站点的例子包括内部安排，或通过与服务提供商的协议提供，或两者的组合。		

原文编号	具体控制要求	客户的关注	华为云的内部实践
9.41	如果备用站点或恢复站点由第三方管理或拥有，金融机构必须确保其外包安排符合关于外包的政策文件，特别是以下内容。 (a) 金融机构与第三方供应商之间执行服务水平协议（SLA），确定向金融机构提供的服务水平和类型，以保障金融机构的利益。 (b) 缓解集中风险，即由第三方提供、管理或拥有的备用或恢复站点将被多个客户或同一地区或行业的客户所使用。在这方面，服务级协议必须具体确定在什么条件下可以使用备用或恢复站点，并具体说明如果同时发生的中断影响到服务提供者的几个客户，将如何安置客户。 (c) 评估服务提供商在合理的长时间内使用的容量和能力。 (d) 服务提供商提供的物理和逻辑访问控制是否充分，以保护备用或恢复站点；以及 (e) 定期测试、持续审查和监测金融机构所提供的服务水平和类型	客户应该建立外包管理机制， 持续监控并定期审查外包服务。华为云的**云监控服务（Cloud Eye Service，简称CES）**可实现对客户自身云资源的使用情况和绩效的监控。华为云可以根据客户的需求按照SLA向客户提供服务报告，华为云也会安排专人 负责客户方发起的尽职调查。 华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**为客户提 供云上资源访问控制。使用 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；**云审计服务（Cloud Trace Service，简称CTS）**可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。记录的操 作类型有三种：通过云账户登录管理控制台执 行的操作，通过云服务支持的API 执行的操 作，以及华为云系统内部触发的操作。	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。 **外包安排的监控**: 华为云可以根据客户的需求按照SLA向客户提供服务报告，华为云也会安排专人 负责客户方发起的尽职调查。 **容量与性能管理**: 华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华 为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资 源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能 瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对租 户云服务的系统性能造成影响。 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。 同时，华为云的云监控服务（Cloud Eye）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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
	以及所采取的风险缓解措施。		云监控服务提供实时监控 告警、通知以及个性化报表视图，精准掌握业 务资源状态。用户可以自主设置告警规则和通 知策略，以便及时了解各服务的实例资源运行状况和性能。 **逻辑访问控制**： 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。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。 在权限复核与调整方面，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。在身份认证方面，当运维人员接入华 为云管理网络对系统进行集中管理 时，需使用员工身份账号，且要求使 用双因子认证，如USB key、 SmartCard等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度 审计。 **物理访问控制**： 华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小 时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同 的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。华为云要求来访 者必须由内部人员全程陪同，并且只能在一般

原文编号	具体控制要求	客户的关注	华为云的内部实践
			限制区域活动。 华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、 出入口、走廊、电梯、机房等进行7*24小时闭路电视监控，并与红外感应、门禁等联 动。保安人员对数据中心定时巡查，并设置在线巡更系统，对非法闯入和其他安保事 件及时进行声光报警。
9.50	金融机构必须根据其规模、性质、复杂性和风险状况，在合理的大范围内定期对所有关键业务功能进行综合测试，包括由关键服务供应商承担的测试。在此过程中，该金融机构必须 (a) 使用备用信息技术系统来衡量和评估其应用系统的联系和网络连接。 (b) 校准支持中断期间所提供的最低服务水平所需的负载或容量要求。 (c) 在随后的几轮测试中包括这种校准；以及 (d) 确保关键的服务供应商参与，以评估他们是否有能力和准备好应对金融机构在中断期间需要部署的恢复措施。	客户应建立自身的业务连续性机制，制定BCP和BIA，并制定保证其关键业务连续的MTD、RPO指标，定期对BCP进行测试。	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。 为配合客户满足合规要求，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，华为云制定了符合自身业务特色的 业务连续性管理体系，并已获得IS022301认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。

原文编号	具体控制要求	客户的关注	华为云的内部实践
9.51	在设计和实施测试时，金融机构必须 (a) 利用现实的模拟 和活动量，制定具有预先确定的测试目标、范围和测试评估标准的测试计划。 (b) 制定衡量BCP和DRP的有效性以及各种业务连续性目标实现程度的指标。 (c) 在测试失败的情况下制定必要的应急措施，以避免业务中断；以及 (d) 保留正式的测试文件，包括测试计划、目标、情景、程序和结果，以便将来参考和审计。	客户需制定BCP和DRP，建立应急预案，并定期进行测试，保留正式的测试文件。	为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管 理体系，并已获得ISO 22301认证。华为云每年会在组织内进行业务连续性的宣传和培 训，以及定期做应急演练和测试，持续优化应急响应机制。华为云安全演练团队定期 制定针对不同产品类型（ 包含基础服务、运营中心、数据中心、组织整体等 ）以及不 同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化 时，也会对业务连续性的有效性进行测试。 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。 应急过程记录 :华为云会对应急处置中所有相关的信息和处理过程进行严格记录，所有过程资料应由 专人存档保管。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。

10 华为云如何遵从及协助客户满足 BNM《云技术风险评估指南（CTRAG）- 技术风险管理（RMIT）政策文件附录》（征求意见稿）的要求

马来西亚国家银行于2022年6月3日发布了《云技术风险评估指南（CTRAG）- 技术风险管理（RMIT）政策文件附录》（征求意见稿）。该征求意见稿从云治理、云架构、云应用交付模式、虚拟化和容器化管理、变更管理、云备份和恢复、退出战略、加密密钥管理、访问控制、网络安全行动、分布式拒绝服务(DDoS)、数据丢失预防（DLP）、安全运营中心(SOC)、网络响应和恢复等方面的要求。

金融机构在遵循《云技术风险评估指南（CTRAG）- 技术风险管理（RMIT）政策文件附录》（征求意见稿）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《云技术风险评估指南（CTRAG）- 技术风险管理（RMIT）政策文件附录》（征求意见稿）中与云服务供应商相关的控制要求，并阐述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。

10.1 云治理

原文编号	具体控制要求	客户的关注	华为云的内部实践
A部分：3. 尽职调查	对潜在的云服务提供商的尽职调查应以风险为基础，并按照与将在云上托管的信息和技术资产的重要性相称的审查水平进行。它至少应 (a) 包括所有金融机构的数据将被处理和存储的所有地点。 (b) 包括评估云外包安排对金融机构的法律、合规、运营、信息安全、数据隐私和声誉风险的潜在影响。 (c) 处理RMiT政策文件中的第三方服务供应商管理部分和外包政策文件（外包流程和风险管理）中的相关部分规定的相关要求和指导；以及 (d) 在云风险状况发生重大变化时，应及时审查或重新进行风险评估，例如，由于国外立法和 地缘政治发展的演变，海外托管数据的司法风险。	客户应按照与将在云上托管的信息和技术资产的重要性相称的审查水平对云服务提供商进行尽职调查，包括数据存储和处理地点、法律、合规、运营、信息安全、数据隐私和声誉风险的等方面。	数据存储和处理地点：华为云目前已陆续在全球多个国家或地区提供云服务，其基础设施部署在全球多个地 理区域（Region）和多个可用区（AZ）。华为云以区域（Region）为单位向客户提供服务。区域即客户内容数据的存储位置， 华为云绝不会在未经用户授权的情况下，跨区域移动客户的内容数据。客户在使用云 服务时，建议根据就近接入原则并遵从不同地域的法律法规要求选择区域，确保其内 容数据存储在目标位置。 对于区域服务，客户可以在购买服务初期按需选择区域，其服务部署位置及数据留存 地可以通过华为云门户进行变更。 运营能力：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。 云安全合规：面向提供云服务的地区，华为云积极与监管机构对话，理解他们的担忧和要求，贡献华为云的知识和经验，不断巩固华为在云技术、云服务和云安全方面与相关法律法规的契合度。同时，华为也将法律法规的分析结果共享给租户，避免信息缺失导致的违规风险，通过合同明确双方的安全职责。华为一方面通过跨行业、跨区域的云安全认证满足监管机构要求，另一方面通过获得重点行业、重点区域所要求的安全认证，建立并巩固华为云业务的客户信赖度，

原文编号	具体控制要求	客户的关注	华为云的内部实践
			最终在法律法规制定者、管理者、租户三者间共建安全的云环境。 信息安全：依托华为自身强大的安全研发能力，以数据保护为核心，开发并采用世界领先的云安全技术，致力于实现高可靠、智能化的云安全防护和自动化的云安全运维运营体系。同时，通过对现网安全态势的大数据分析，有目的地识别出华为云存在的重要安全风险、威胁和攻击，并采取防范、削减和解决措施；通过多维、立体、完善的云安全防御、监控、分析和响应等技术体系支撑云服务运维运营安全，实现对云安全风险、威胁和攻击的快速发现、快速隔离和快速恢复，让租户受益于华为云先进技术带来的便捷、安全与业务增值。 商业声誉：华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华 为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等 行业，华为云已实现大突破。 数据隐私：华为云建立了完善的隐私保护体系，从公司、流程层面建立了一系列隐私保护的政策用于管理制度保护客户的隐私，同时建立了专注于隐私保护的部门及专职人员，每年对华为云的隐私保护情况进行稽查、减低、核查隐私保护措施在华为云内部的有效执行。

原文编号	具体控制要求	客户的关注	华为云的内部实践
A部分：4.获得权威的第三方认证	金融机构在采用云技术之前，应审查其云服务提供商的认证。至少，金融机构应 (a) 确保云服务提供商继续遵守相关法律或监管要求以及合同义务的保证，并评估云服务提供商为减少任何不合规行为而制定的行动计划；以及 (b) 在进行风险评估时，获取并参考可靠的独立外部方的云平台报告。这应涉及RMiT政策文件中的云服务部分和外包政策文件中涉及云服务部分规定的要求和指导。	客户在采用云技术之前，应审查其云服务提供商的认证。	华为云已通过ISO 27001、ISO 27017、ISO 27018、SOC、CSA STAR等多项国际 安全与隐私保护认证，并且每年会接受第三方的审计。 同时，华为云也将法律法规的分析结果共享给租户，避免信息缺失导致的违规风险，通过合同明确双方的安全职责。华为一方面通过跨行业、跨区域的云安全认证满足监管机构要求，另一方面通过获得重点行业、重点区域所要求的安全认证，建立并巩固华为云业务的客户信赖度，最终在法律法规制定者、管理者、租户三者间共建安全的云环境。
A部分：5.合同管理(a)	金融机构应就预期云服务提供商的信息安全和运营标准制定明确的、可衡量的、合同约定的条款和参数。此类合同条款和参数应与金融机构的业务战略、信息安全政策和监管要求保持一致。金融机构与云服务提供商之间的合同条款应解决RMiT政策文件中云服务部分规定的与云服务有关的风险。	客户应与预期云服务提供商制定明确的、可衡量的、合同约定的条款和参数，合同条款应解决RMiT政策文件中云服务部分规定的与云服务有关的风险。k	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。 华为云已获得众多国际和行业安全合规资质认证，包括ISO27001、ISO27017、ISO27018、PCI-DSS、CSA STAR等。华为云遵循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	具体控制要求	客户的关注	华为云的内部实践
A部分： 5.合同管理(b)	合同条款、义务和所有订约方的责任（如果分包商对提供关键功能至关重要，这可能包括分包商）应在合同中明确说明。至少，合同应涉及RMiT政策文件的第三方服务供应商管理部分和外包政策文件的相关部分（外包协议和数据机密性保护）中规定的要求和指导。	客户与云服务提供商签订的合同协议应明确合同条款、义务和所有订约方的责任，并涉及RMiT政策文件的第三方服务供应商管理部分和外包政策文件的相关部分（外包协议和数据机密性保护）中规定的要求和指导。	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。 客户以及其监管机构对华为云的审计和监督权益，会根据实际情况在与客户签订的协议中进行约定。
A部分： 5.合同管理(d)	云服务可能会出现与事件响应和调查有关的困难，因为与内部解决方案相比，金融机构可能不再能够完全接触到云服务提供商管理的计算组件。金融机构至少应评估潜在的影响，并与云服务提供商作出正式协议安排，以遵守当地法律和监管要求，进行事件调查和执法。这将包括遵守数据保留要求和数据访问程序安排，以确保客户的保密性和隐私得到保护。	客户应通过与云服务提供商的协议安排要求其遵守当地法律和监管要求，进行事件调查和执法。	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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
A部分：5. 合同管理 (e)	主要云服务提供商提供的云服务可能与其他第四方云服务提供商（分包商）的多个层次相互连接，这可能会迅速变化。例如，由于第四方所做的曝光，客户数据被泄露。为了减轻第四方的风险，金融机构应该 i) 了解整个供应链共享的客户信息的范围，并确保相关的信息安全控制可以由[金融机构]依法执行；以及 ii) 确保服务水平协议（SLA）谈判和合同条款涵盖服务的性能矩阵、可用性和可靠性，以确保所有各方都同意并在所提供服务的要求和标准上正式保持一致。	客户应确保与云服务提供商签订的服务水平协议（SLA）谈判和合同条款涵盖服务的性能矩阵、可用性和可靠性。	华为云线上的**《华为云用户协议》**对客户和华为云的安全职责进行划分，华为云**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的要求，在其中规定华为云若聘用分包商，需通知客户，并对分包的服务负责等要求。 华为云制定了自身的供应商管理机制，从供应商的产品和供应商本身的内部管理都提出了安全需求。此外，华为云会对供应商进行定期的稽核。此外会与涉及网络安全的供应商签署网络安全协议，在服务过程也中会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应商进行合作降级处理。 华为云国际站SLA约定了华为云各项产品/服务的服务等级，包括对服务可用性的承诺，以及未达到承诺的服务补偿。

原文编号	具体控制要求	客户的关注	华为云的内部实践
A部分：6. 对云服务提供者的监督	金融机构应确保对云服务提供商和云服务提供商的分包商进行有效监督。这至少包括以下内容。 (a) 建立并定义一个与企业供应商管理框架（或同等框架）相一致的持续监督机制，以确保遵守商定的服务水平协议，云服务提供商遵守任何适用的法律和监管要求，以 及持续保持外包技术服务的弹性。 (b) 确定、分配和记录金融机构内对云服务提供商进行持续监控的主要责任，以确保责任得到明确界定；以及 (c) 定期评估云服务提供商的控制环境，包括业务连续性管理，以评估对金融机构业务复原力的潜在影响。这应涉及外包政策文件中涉及云服务部分的要求和指导。	客户应对云服务提供商和云服务提供商的分包商进行有效监督。 客户可适用华为云提供的**云监控服务（Cloud Eye Service，简称CES）**实现对客户自身云资源的使用情况和绩效的监控。	华为云可以根据客户的需求按照SLA向客户提供服务报告，华为云也会安排专人负责客户方发起的尽职调查。 客户对华为云的审计和监督权益会根据实际情况在与金融机构签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。 华为云遵循ISO22301业务连续性管理国际标准，建立了一套完善的业务连续性管理体系。在该体系框架下，定期进行业务影响分析和风险评估，为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面，并定期测试备份和恢复程序。如果需要华为云协助执行客户的灾难恢复计划，华为会积极配合。如果华为云的灾难测试过程中需要客户的参与，华为云会提前通知。 同时，华为云在提供高可用基础设施、冗余数据备份、可用区灾备等服务外，还制定了自身的业务连续性计划。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。

10.2 云设计和控制

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：1. 云结构(b)	鼓励金融机构采用零信任原则，通过对应用程序和基础设施的微观分割，以 "默认拒绝"、"最小特权 "的访问权限或以 "需要 "为基础提供增强的访问控制。	客户可通过华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**对使用云资源的用户账号进行管理。IAM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。	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。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。 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。在权限复核与调整方面，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。 在特权账号管理方面，华为云的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。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。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（提供账号/密码）登陆租户的控制台或者资源实例协助客户进行维护。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：1. 云架构(d)	金融机构应建立并利用安全和加密的通信渠道，将物理服务器、应用程序或数据迁移到云平台。这包括使用与生产网络隔离的网络进行云迁移和管理平面的持续管理。	客户应立并利用安全和加密的通信渠道，将物理服务器、应用程序或数据迁移到云平台。 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。针对金融机构业务混合云部署和全球化布局的场景，可以使用华为云提供的**虚拟专用网络（Virtual Private Network，简称VPN）**、**云专线（Direct Connect，简称DC）**、**云连接（Cloud Connect，简称CC）**等服务，实现不同区域之间业务的互联互通和数据传输安全。 华为云为客户提供上云迁移服务。华为云将基于客户提供的信息，与客户一同商定并确认具体业	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。 针对于传输中的数据，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虚拟专用网络（VPN）和应用层TLS与证书管理，华为云服务为客户提供控制台和API两种访问方式，均采用加密传输协议构建 安全的传输通道，有效地降低数据在 网络传输过程中被恶意嗅探的风险。

原文编号	具体控制要求	客户的关注	华为云的内部实践
		务目标及范围，通过需求分析为客户设计迁移方案并制 定迁移计划和迁移演练等。 客户可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移服务（Server Migration Service，简称SMS）**将本 地数据中心数据迁移至华为云。OMS和SMS支持国内外主流公有云厂商，SMS还支持 国私有云平台虚拟机迁移、x86物理服务器迁移（覆盖约40种主流操作系统）。	

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：2.云应用交付模式(b)	云应用交付模式可能会不断发展，以支持更快的上市时间，满足消费者的需求。目前，DevOps和持续集成/持续开发（CI/CD）7 是云应用交付的普遍做法和流程之一。例如，在应用开发人员可能需要访问管理平面以进行服务配置的情况下，为CI/CD执行职责分离的能力。金融机构应确保CI/CD渠道配置得当，以提高自动化部署和不可改变的基础设施的安全性。	客户应建立自身的云应用交付流程，确保服务配置得当。	由于华为云服务商业模式的变化，华为云已经建立起新的组织结构、管理体系并采用更适合云服务的 DevOps 模式进行开发、部署和运营。相较于适合传统 ICT 业务的研发流程，华为云已经采用全新的持续集成、持续交 付、持续部署、快速迭代 DevOps 流程。并且，华为云将高可靠、高稳定的安全研发 和运维运营要求结合在 DevOps 流程中，形成适合华为云的 DevSecOps流程。 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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：3. 虚拟化和容器化管理	本段提供的指导与 PaaS 和 IaaS 云服务模式有关。 (a) 金融机构应确保虚拟化服务的配置符合云服务提供商的现行指导和行业最佳做法，并与云计算技术的发展相适应。 (b) 金融机构应确保虚拟机和容器镜像得到适当的配置、加固和监控。这包括以下内容。 i) 使用最新的镜像并保持镜像的更新。 ii）存储和使用来自受信任的存储库或注册处的镜像。 iii) 扫描镜像的漏洞，在生产中运行之前补救任何漏洞。 iv) 执行 "最小权限 "访问。 v) 根据行业最佳实践加固镜像；以及 vi) 对存储的镜像进行安全监控，防止未经授权的访问和更改。	客户应考虑建立标准化的发布流程管理虚拟机和容器镜像得到适当的配置、加固和监控。 华为云**镜像服务（Image Management Service,简称IMS）**提供简单方便的镜像自助管理 功能。用户可通过服务控制台或 API 对自己的镜像进行管理。用户可以直接使用公共镜像，或者通过已有的云服务器或使用外部镜像文件自行创建私有镜像，也可以参与创建和维护共享镜像。用户能灵活选择上述任何镜像申请弹性云服务器。 **容器镜像服务（SoftWare Repository for Container, 简称SWR）**是一种支持容器镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，帮助用户快速部署容器化服务。通过使用SWR，租户无需自建和维护镜像仓库，即可享有云上的镜像安	华为云针对弹性云服务器（Elastic Cloud Server，简称ECS）配套提供了镜像服务，租户可自行选择华为云官网提供的标准镜像或者私有化镜像，通过控制台（Console）的管理，可以方便地进行版本管理和发布管理。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。 IMS 基于华为云统一身份认证服务（IAM）来进行认证，IMS对租户的所有操作进行权限判断，只有符合权限要求才允许执行，并对所有关键操作进行审计记录。同时，通过完善的变更管理程序，防止华为云内部运维人员对系统配置参数进行未授权变更。IMS支持镜像的传输和存储加密以及完整性检测。另外，华为云从网络隔离、数据隔离、外部威胁防御以及身份认证与访问控制等多方面保证在多租户场景下客户信息的安全性。更多详细资料请参见《华为云安全白皮书》。 当发生软硬件故障后，如果相应的资源被释放掉后，客户内容会自动进行销毁，华为云会通过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恢复。 针对镜像安全扫描，租户可一键对上传的镜像执行安全扫描，识别中镜像中的漏洞并显示出修复建议，帮助用户得到一个安全的镜像。 针对于安全配置，华为云对主机操作系统、虚拟机、数据库、web应用组件等均进行安全配置加固，同时支持客户根据自身业务需求选择适合于自身的安全配置。如在主机安全

原文编号	具体控制要求	客户的关注	华为云的内部实践
		全托管及高效分发服务，并且可配合云容器引擎 CCE、云容器实例 CCI 使用，获得容器上云的顺畅体验。 华为云的**云监控服务（Cloud Eye Service，简称CES）**为客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。可协助用户快速获取对云资源的告警，并采取相应的应对措施。	方面，主机操作系统使用华为统一虚拟化平台（UVP），对CPU，内存和I/O 资源隔离管理，主机操作系统已进行最小化裁剪并对服务做安全加固；在虚拟机安全方面，华为云提供镜像加固、网络与平台隔离、IP/MAC仿冒控制、安全组等安全配置。 华为云的虚拟机安全有镜像加固。华为云通过镜像工厂，由专业安全团队对虚拟机操作系统公共镜像进行安全加固，并及时修复系统安全漏洞，最终生成安全更新了的公共镜像，并通过IMS持续提供给租户。同时提供相关加固和补丁信息以供用户对镜像进行测试、排除故障及其他 运维活动时参考。由客户根据相关应 用运行及安全运维策略，选择直接使用最新的公共镜像重新创建虚拟机或自行创建已安装安全补丁的私有镜 像。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：5. 云备份和恢复(a)	作为有效恢复能力的一部分，金融机构应确保将现有的备份和恢复程序扩展到云服务，其中包括以下内容。 i) 在采用云技术的规划阶段，定义并正式确定备份和恢复策略。 ii) 对云服务提供商的恢复和复原能力进行定期审查。 iii) 对于托管在云上的关键系统，在部署系统之前进行恢复策略的测试。	客户应建立云备份和恢复程序，确保在灾难发生时数据不丢失。 客户可以使用华为云提供的**云备份（Cloud Backup and Recovery，简称CBR）**服务实现对**云硬盘（Elastic Volume Service，简称EVS）**、**弹性云服务器（Elastic Cloud Server，简称ECS）**和**裸金属服务器（Bare Metal Server，简称BMS）**的备份保护。云备份支持基于快照技术的备份服务以及利用备份数据恢复服务器和云硬盘的数据。同时云备份支持同步线下备份软件BCManager中的备份数据以及对备份数据的完整性校验。 华为云为金融机构提供**存储容灾服务（Storage Disaster Recovery Service，简称SDRS）**，可帮助金融机构在容灾站点迅速恢复业务，缩	华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联（DCI–Data CenterInterconnect），满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。 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。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。 华为云还部署了全球负载均衡管理中心，客户的应用在该中心实现了N+1 部署规模华为云建立了可指导人员的 管理备份流程。

原文编号	具体控制要求	客户的关注	华为云的内部实践
		短业务中断时间。该服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。	

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：5. 云备份和恢复(c)	金融机构应确保对虚拟机和容器进行充分的备份和恢复，包括备份配置设置（针对IaaS和PaaS，如相关），其中包括以下内容。 i) 确保有能力按照业务恢复目标在时间点恢复虚拟机和容器。 ii) 提供虚拟机和容器镜像，使金融机构能够在备用和恢复站点复制这些镜像；以及 iii) 允许下载虚拟机和容器镜像，并将其移植到新的云服务提供商。	客户应对虚拟机和容器进行充分的备份和恢复，包括备份配置设置。 客户可以使用华为云提供的**云备份（Cloud Backup and Recovery，简称CBR）**服务实现对**云硬盘（Elastic Volume Service，简称EVS）**、**弹性云服务器（Elastic Cloud Server，简称ECS）**和**裸金属服务器（Bare Metal Server，简称BMS）**的备份保护。云备份支持 基于快照技术的备份服务以及利用备份数据恢复服务器和云硬盘的数据。同时云备份支持同步线下备份软件BCManager中的备份数据，可以在云上对备份数据进行管理，并支持将备份数据恢复至云上其他服务器中。 客户可通过华为云提供的**云数据迁移服务（Cloud Data Migration，简称CDM）**支持在多种类型数	在备份容灾方面，客户选择相应的备份和容灾服务，在硬盘层面、服务器层面、虚拟机层面实现自身业务所需的备份和容灾保护。 华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用对象存储服务的版本控制、云硬盘备份、云服务器备份等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云。 通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。 此外，为了减小由硬件故障、自然灾害或其他灾难带来的服务中断，华为云为所有数据中心提供灾难恢复计划： ● 华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一 旦出现故障，用户数据不会丢失，系 统做到自动检测和自愈。 ● 单个区域内不同可用区之间，通过高 速光纤实现数据中心互联（DCI – Data Center Interconnect），满足 跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。 华为云为金融机构提供上云迁移服务。华为云将基于金融机构提供的信息，与金融机构一同商定并确认具体业务目标及范围，通过需求分析为金融机构设计迁移方案并制定迁移计划和迁移演练等。

原文编号	具体控制要求	客户的关注	华为云的内部实践
		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。 客户还可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移服务（Server Migration Service，简称SMS）**将本地数据中心数据迁移至华为云。OMS和SMS支持国内外主流公有云厂商，SMS还支持 国私有云平台虚拟机迁移、x86物理服务器迁移（覆盖约40种主流操作系统）。	

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：5. 云备份和恢复(d)	金融机构应评估云服务的弹性要求，并确定与系统的重要性相称的适当措施，以确保在极端不利情况下的服务可用性。为确保服务的可用性，金融机构应考虑采取基于风险的方法，并逐步采用一种或多种冗余方法，包括从单一的 CSP 中分散出来。其中可行的方案有 i) 利用云服务的高可用性和冗余功能，确保生产数据中心在不同的可用性区域具有冗余能力。 ii) 通过在不同的地理区域设立数据中心来实现地理冗余。 iii) 采用混合云（结合企业内部和公共云设置）。 iv) 建立后备云服务提供商，并确定适当的数据和应用程序移植安排，以确保及时恢复服务；以及 v) 采用多云战略，使用不同云服务提供商的服务，以减少集中风险和地缘政治风险。	客户应确保云服务的高可用性和冗余功能，确保生产数据中心在不同的可用性区域具有冗余能力。	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。 华为云依赖数据中心集群的两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，可通过两地互为灾备中心，如一地出现故障，系统在遵循合规政策前提下自动将应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。用户可充分利用这些地域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下（包括自然灾害和系统故障）系统都能连续运行。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：6. 互操作性和可移植性	云服务的互操作性标准不断发展，因此在不同的云服务提供商之间移植数据、相关配置和安全日志可能具有挑战性。为促进内部IT系统与备用云服务提供商之间的互操作性和可移植性的顺利进行，我们鼓励金融机构 (a) 确保互操作性和可移植性的技术要求包含在与云服务提供商的合同协议中，以避免锁定供应商。 (b) 保持一份云服务提供商和工具的清单，以促进平稳过渡。 (c) 确保使用标准化的网络和通信协议，以方便与内部IT系统或其他云平台的互操作性和便携性。 (d) 确保使用通用的电子数据格式（如适用），以方便数据在云服务提供商之间或向企业内部的IT系统移动；以及 (e) 扩大补丁和EOL管理，以确保所采用的技术解决方案保持有效并防止系统漏洞。	客户应确保互操作性和可移植性的技术要求包含在与云服务提供商的合同协议中。 客户可通过华为云提供的**云数据迁移服务（Cloud Data Migration，简称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。 客户可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移服务（Server Migration Service，简称SMS）**将本地数据中心数据迁移至华为云。OMS和SMS支持国内外主流公有云厂商，SMS还支持国私有云平台虚拟机迁移、x86物理服务器迁移（覆	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。 华为云为金融机构提供上云迁移服务。华为云将基于金融机构提供的信息，与金融机构一同商定并确认具体业务目标及范围，通过需求分析为金融机构设计迁移方案并制定迁移计划和迁移演练等。

原文编号	具体控制要求	客户的关注	华为云的内部实践
		盖约40种主流操作系统）。	
B部分：7. 退出战略 (b)	金融机构的退出战略应得到退出计划的支持，该计划确定了促进有序退出云服务提供商的操作安排，其中包括以下内容。 i) 进行影响评估，以确定将云服务转移到其他云服务提供商或回到金融机构的内部安排的潜在成本、资源和时间影响。 ii) 确定适当的方法，将数据和应用移植到替代安排中。 iii) 从云服务提供商处获得书面确认，或通过独立的外部服务提供商证明，所有敏感数据在退出过程完成后已从云服务提供商的设施中完全删除和销毁；以及 iv) 进行测试以验证退出计划的有效性，以获得对其有效性的合理程度的保证。	客户应制定退出计划确保有序退出云服务提供商，包括云服务迁移以及敏感数据在退出过程完成后从云服务提供商的设施中完全删除和销毁。	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，华为云会严格遵循适用的法律法规，以及与客户之间的协议约定，按照数据销毁标准清除客户的数据。 在平台层面，在客户数据的销毁阶段，华为云会对指定的数据及其所有副本进行全面的清除。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。 在物理介质销毁层面，为保证数据中心介质生命周期末期数据安全，华为云参照相关 行业标准，实施了完善的存储介质处置机制。如参考NIST SP 800-88标准对存储介质 进行处理，针对需要重复使用的存储介质，进行随机数覆写、加密擦除等方式进行数据安全删除，针对不需要重复使用的存储介质则采取消磁、物理损毁等方式进行物理 销毁。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：8.加密密钥管理(a)	金融机构应实施适当和相关的加密技术，以保护存储在云上的敏感数据的保密性和完整性。	客户应实施适当和相关的加密技术以保护云上的敏感数据的保密性和完整性。 华为云为客户提供了**数据加密服务（Data Encryption Workshop，简称DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了金融机构云上数据的安全。	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。 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。 针对于加密，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 数据的保护通过虚拟专用网络（VPN）和应用层TLS与证书管理，华为云服务为客户提供控制台和API两种访问方式，均采用加密传输协议构建 安全的传输通道。 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。 针对于静态数据，华为云为保护租户数据的存储安全采取了一系列的保护机制。 首先，华为云提供了密钥管理服务（KMS）。它帮助用户集中管理密钥，保护密钥安全。它通过使用硬件 安全模块（HSM–Hardware Security Module），为租户创建和管理密钥， 防止密钥明文暴漏在HSM之外，从而 防止密钥泄露。与华为云服务对接 KMS的服务有OBS、云硬盘等。其次，专属加密满足租户更高合规性要求的加密场景，采用通过国家密码局认证或FIPS140-2第3级验证的硬件加密机，对租户业务进行专属加密，默认双机架构以提高可靠性。最后，华为云多款存储产品如EVS、VBS等均提 供存储加密的机制。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：8.加密密钥管理(c)	对于托管在云上的关键系统，金融机构应保留加密密钥的所有权和控制权（自己或与独立的密钥保管人），独立于云服务提供商，以尽量减少未经授权访问云上托管数据的风险。例如，可以通过在企业内部部署硬件安全模块（HSM）或利用不同云服务提供商的HSM即服务来实现。	客户应实施一个集中的密钥管理系统，制定统一密钥管理和加密政策，保留加密密钥的所有权和控制权，减少未经授权访问云上托管数据的风险。 华为云为客户提供了**数据加密服务（Data Encryption Workshop，简称DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了金融机构云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。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。	针对于传输中的数据，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虚拟专用网络（VPN）和应用层TLS与证书管理，华为云服务为客户提供控制台和API两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分：9. 访问控制 (a)	管理层是传统基础设施和云计算之间的一个关键安全区别，在云计算中默认支持远程访问。这个访问层可能容易受到网络攻击，从而损害整个云计算部署的完整性。有鉴于此，金融机构应确保使用强大的控制措施来访问管理平面，包括以下内容。 i) 审查金融机构的补丁和EOL管理框架，以有效保证管理计划的安全。 ii) 分配专用和有效加固的端点，并对软件进行最新的修补，以访问管理平台。 iii) 实施 "最小特权 "和强大的多因素认证（MFA），例如，强密码、软令牌、特权访问管理工具和制造商检查器功能。 iv) 对特权用户采用细化的权利分配。 v) 对特权用户的活动进行持续监控。 vi) 采用强大的预防机制，防止网络钓鱼和密码猜测攻击、凭证填充和暴力攻击，例如，网络应用防火墙（WAF）、反钓鱼工具；以及 vii) 确保访问管理平面的安全通信协议到位，例如，安全的端到端通信渠	客户可通过华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**对使用云资源的用户账号进行 管理。IAM除了支持密码认证之外还支持 多因子认证，客户可自主选择是否启用。 如果租户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的 华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划 使用云资源的权限，还可以通过设置用户 访问云服务系统的安全策略，例如设置访 问控制列表来限制未信任网络的恶意接入。 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	华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，如USBkey、SmartCard等。 客户除了通过统一身份认证服务（IAM），对远程接入人员的身份和权限进行管理外，华为云还提供了加密传输的方式供客户自行选择，比如VPN、HTTPS等。同时，对于华为云内部系统的远程访问仅可以通过堡垒机和SVN的方式。华为云统一管理堡垒机和SVN的权限，对华为云运维人员进行身份认证，并且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。 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。在权限复核与调整方面，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。 在特权账号管理方面，华为云的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。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。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（提供账号/密

原文编号	具体控制要求	客户的关注	华为云的内部实践
	道，IP地址白名单等。	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，金融机构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。 **云堡垒机（Cloud Bastion Host，简称CBH）**是华为云的一款统一安全管控平台，可帮助金融机构实现集中的帐号、授权、认证和审计管理。云堡垒机提供云计算安全管控的系统和组件，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。 客户可以部署**Web应用防火墙 (Web Application Firewall，简称WAF)**，从多维度检测和保护网站业务流量。	码）登陆租户的控制台或者资源实例协助客户进行维护。 华为云严格执行相应的控制措施，确保华为云在架构设计、设备选型、主机网络（多种多层物理和虚拟网络安全隔离方法）、访问控制、边界防护技术、配置等方面的安全。为了检测和拦截来自Internet的攻击以及租户虚拟网络之间的东西向攻击，华为云的网络中部署了网络IPS设备，包括但不限于面向公众的网络边界、安全区域信任边界、租户空间边界。华为云的IPS可以实时分析网络流量，触发对协议攻击、暴力破解、端口和漏洞扫描、病毒和木马攻击、针对特定漏洞的攻击等各种入侵的拦截。此外，华为云还配置了防火墙设备，以此限制对华为生产网络的访问。应在机器上配置防火墙策略的配置，并每月进行一次审查，以确保防火墙规则基于标准配置。因改变防火墙规则而产生的偏差都将被跟踪和补救。华为云通过配置防火墙策略，限制高危端口的访问和高危协议的使用。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分： 10. 网络安全行动 (b)	互联的云服务供应链可能成为网络风险的来源。金融机构应确保建立对云服务的综合监测和全面可视性。这应包括以下内容。 i) 对云服务提供商、内部IT系统和其他第三方服务提供商之间的系统通信进行持续监测，以确保安全边界不被破坏；以及 ii) 确保第三方服务供应商（包括提供辅助功能的供应商）有足够的能力来监测、发现和应对异常活动，并及时向金融机构通报相关的网络事件。	华为云的**云监控服务（Cloud Eye Service，简称CES）**为客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。可协助 用户快速获取对云资源的告警，并采 取相应的应对措施。同时华为云还可提供**Anti-DDoS流量清洗服务**、**DDoS 高防（Advanced Anti-DDoS，简称AAD）**、**Web应用防火墙服务（Web Application Firewall，简称WAF）**、**数据库安全服务（Database Security Service，简称DBSS）**、**云审计服务（Cloud Trace Service，简称CTS）**可帮 助用户精准有效地实现对流量型攻击 和应用层、数据层攻击的全面防护， 以及事后对安全事件进行追溯和审计的功能。	华为云为客户提供基础设施，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，在物理环境、网络、平台、应用程序接口、数据等主要方面提供了多层次的安全防护。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。 华为云使用态势感知（Situation Awareness，简称SA）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。 事件检测和响应：华为云内部制定了完善的安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。在事件解决后，会根据具体情况向客户提供事件报告。 事件披露与监管上报:为配合客户满足重大风险上报利益相关

原文编号	具体控制要求	客户的关注	华为云的内部实践
			方的要求，华为云设置7*24的专业安全事件响 应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户， 同时执行应急预案及恢复流程，降低业务影响。除此之外，华为云已建立了数据泄露 事件处理机制，如有必要，华为云会按照适用法律法规的要求进行事件通报。如客户需进行监管上报的工作，华为云将配合客户提供相关材料。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分： 10. 网络安全行动 (c)	金融机构应了解安全管理方面的责任划分，这种划分在不同的云服务模式中是不同的。金融机构应适当地管理漏洞的来源，包括 i) 管理云服务的漏洞评估和渗透测试（VAPT）。 ii) 主动寻求其云服务提供商的保证，定期对云基础设施进行VAPT，以确保租户隔离和整体安全态势保持健康。 iii) 鉴于金融机构对云环境的访问程度不同，了解云服务提供商对云基础设施的VAPT政策，并预先建立VAPT安排。 iv) 根据金融机构所负责的云配置范围，调整金融机构的 VAPT 标准操作程序。这包括在部署云服务之前进行VAPT。 v) 建立适当的工具，对金融机构负责的云服务进行VAPT，与云环境的复杂性相称。 vi) 渗透测试的范围应强调对管理平面的 API 调用和特权用户（例如，云管理员）的凭证，这 些构成了网络攻击面的关键因素；以及 vii) 采用高速方法的金融机构，如持续集成/持续开发（CI/CD），应将代码审查、安全测试和漏洞评估纳入	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，以便快速识别资产的漏洞并进行修复。 客户可通过华为云的**漏洞扫描服务（Vulnerability Scan Service，简称VSS）**实现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、弱密码检测等功能，自动发现网 站或服务器暴露在网络中的安全风险，可协助用户对其云上的业务进行多维度的安全检测。	华为云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，能确保基础设 施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在SLA 时间内完成响应和修复，降低并最终避 免漏洞被恶意利用而导致影响租户业务的风险。对于涉及云平台、租户服务等的漏洞， 在确保不会因主动披露而导致更大攻击风险 的情况下，向最终用户/租户及时推送漏洞规避和修复方案和建议，与租户共同面对安全 漏洞带来的挑战。 为配合客户满足合规要求，华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。华为云已与合作伙伴联合推出了主机入侵检测、Web应用防火墙、主机漏洞检测、网页防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力。 华为云产品安全事件响应团队（CSIRT）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CSIRT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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
	系统开发生命周期（SDLC）流程，以尽量减少应用程序的漏洞。		针对公有云攻击的手段多样、流量巨大的特点，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，快速识别已 经发生的攻击，并预判尚未发生的威胁。
B部分： 13. 安全运营中心(SOC) (b)	在金融机构与云服务提供商之间的合同协议中，应正式规定云服务提供商在安全运营方面的责任，包括用于取证的相关日志所需的保留期，以及金融机构访问日 志的权利，以满足RMiT关于访问控制和数字服务安全的要求。	客户应在与云服务提供商之间的合同协议中规定云服务提供商在安全运营方面的责任，包括用于取证的相关日志所需的保留期，以及金融机构访问日志的权利。	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。 华为云针对所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志也会进行管理，确保所有日志保存时间超过180天，90天内可以实时查询。华为云内部已根据法规要求建立了法证调查管理机制，制定了规范的取证流程，以支持安全事件的法证调查。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分： 14. 网络响应和恢复(b)	金融机构应扩展其网络事件响应计划(CIRP)，以包括可能影响云服务的不利情况，并在金融机构和云服务提供商之间建立明确的角色和责任，以应对事件和补救措施。应与云服务提供商建立事件升级流程和周转时间，并尽可能定期审查，以实现有效的事件响应。	客户应建立包括云服务的事件响应计划，与云服务提供商之间建立明确的角色和责任，以应对事件和补救措施。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。 华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。

原文编号	具体控制要求	客户的关注	华为云的内部实践
B部分： 14. 网络响应和恢复(f)	对于托管在云上的关键系统，金融机构应与云服务提供商建立安排，每年进行网络演习，以测试金融机构CIRP的有效性。	客户应与云服务提供商建立安排，每年进行网络演习。	客户应建立网络安全监控机制，采取有效的监控措施，包括部署网络监控、渗透测试、内部和外部审计。此外，客户还应每年对其网络安全框架的有效性进行测试，测试方式可考虑安全漏洞评估、情景模拟演练、渗透测试等。 为配合客户满足监管要求： （1）针对公有云攻击的手段多样、流量巨大的特点，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，快速识别已经发生的攻击，并预判尚未发生的威胁。 （2）华为云定期会开展内部网络安全实战演练（如红蓝对抗）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。 （3）华为云产品安全事件响应团队（CSIRT）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CSIRT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。

11 华为云如何遵从及协助客户满足 SC《网络风险管理指引》的要求

马来西亚证券委员会于2016年10月31日发布了《网络风险管理指引》。该规定从网络风险的预防、监测、恢复等领域提出对金融机构网络风险管理相关要求。

金融机构在遵循《网络风险管理指引》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《网络风险管理指引》中与云服务供应商相关的控制要求，并阐述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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
网络风险管理-预防 4.5-4.10	4.5金融机构必须将进行定期评估作为实体合规计划的一部分，以识别其运营环境中可能破坏信息资产、系统和网络的安全性、机密性、可用性和完整性的潜在漏洞和网络威胁。 4.6金融机构必须对业务实体的潜在漏洞进行全面评估，包括与业务相关的业务流程、人员、采用的系统和技术及外包相关安排。 4.7金融机构必须制定并实施预防措施，最大限度地降低实体面临的网络风险。 4.8上文第4.7段所述的预防措施可包括： （a）部署防病毒软件和恶意软件程序，以检测和隔离恶意代码； （b）系统和系统组件分层； （c）建立防火墙以减少攻击者能够访问金融机构网络的弱点； （d）在软件开发阶段进行严格的测试，以限制漏洞的数量； （e）现有系统和网络的渗透测试；以及 （f）使用权限矩阵限制对系统和数据的内部或外部特权访问权限。 4.9金融机构必须确保董事会、管理层、员工和代理人定期接受适当的培训，以提高他们应对各种网络风	客户应定期识别并评估潜在的漏洞和网络威胁，制定降低网络安全风险的预防措施，包括部署防病毒软件、设置防火墙、在开发过程进行安全测试、对系统和网络进行渗透测试等。此外，客户还应定期全体员工进行适当的安全意识培训，并定期审查其培训计划的充分性和有效性。 客户可通过华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**对使用云资源的用户账号进行管理。IAM 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	作为云服务提供商： **（1）**华为云产品安全事件响应团队（CSIRT）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，使基础设施、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，华为云CSIRT和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在SLA时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响用户业务的风险。 **（2）**为配合客户遵从监管要求，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。 **（3）**华为云建立了合理、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；Anti-DDoS 快速发现和防护DDoS 攻击；WAF 实时检测和防御Web 攻击；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。针对公有云攻击的手段多样、流量巨大的特点，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。 **（4）**华为的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。为配合客户遵从监管要求，华为云通过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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
	险、事件和情景的意识和准备。 4.10金融机构必须评估应对网络风险的意识和准备水平的提高，以确保实施的培训计划的有效性。	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。	华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，使发布的云服务满足安全要求，测试在与生产环境隔离的测试环境中进行，并避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱敏，使用完成后需要进行数据清理。 **（5）**华为云制定了完善的安全意识培训计划，在员工入职、在岗、转岗等环节纳入多种形式的安全意识培训，使员工行为符合所有适用的法律、政策、流程以及华为商业行为准则的要求。

原文编号	具体控制要求	客户的关注	华为云的内部实践
网络风险管理-监测 4.11-4.15	4.11除了实施预防措施外，金融机构必须持续监控其系统和网络中的任何网络事件和漏洞。 4.12金融机构必须确保在明确界定的上报和决策过程中及时发现和响应网络违规行为，以确保网络事件的任何不利影响得到妥善管理，并迅速启动恢复行动。 4.13为确保充分准备应对检测到的网络事件，金融机构必须： （a）确定实体最有可能面临的网络风险情景； （b）考虑资本市场和更广泛的金融服务业的事件； （c）评估这些事件对金融机构的可能影响；以及 （d）确定适当的应对计划和应采取的沟通策略。 4.14金融机构必须定期测试、审查和更新已识别的网络风险情景和应对计划。这是为了确保考虑到运行环境、系统的变化或新的网络威胁的出现时，场景和响应计划仍保持相关性和有效性。 4.15金融机构必须确保根据实体的业务连续性计划和危机管理计划，将检测到的网络漏洞上报给事件响应团队、管理层和董事会，并及时实施适当的响应。	客户应持续监控起系统和网络中的网络事件和漏洞，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。另外，客户还应定期开展网络安全实战演练，测试其应对计划的有效性。当检测到漏洞时，应及时进行向相关人员上报并实施适当的响应。	作为云服务提供商： **（1）**华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM – Security Information and Event Management）系统如ArcSight、Splunk对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。 **（2）**华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、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，会根据具体情况向客户提供事件报告。 **（3）**基于云面临环境下存在复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，从而在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。同时，根据内部信息安全管理体系和业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。

原文编号	具体控制要求	客户的关注	华为云的内部实践
网络风险管理-恢复 4.17-4.19	4.17金融机构必须确保所有关键系统能够在实体规定的恢复时间目标内从网络漏洞中恢复，以便在短期内提供重要服务或某种程度的最低服务。 4.18金融机构必须确定其操作环境中应优先恢复的关键系统和服务，以便在停机期间提供一定的最低服务水平，并确定实体恢复全面服务和运营所需的时间。 4.19金融机构必须确保其业务连续性计划是全面的，并包括因网络漏洞而产生的系统、运营和服务的恢复计划。	客户应确定关键系统的恢复时间目标，并制定全面的恢复计划，以确保服务的及时恢复。	作为云服务提供商： **（1）**为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得ISO22301认证。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。 **（2）**为配合客户遵从监管要求，华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面。

12 华为云如何遵从及协助客户满足 SC《业务连续性指导原则》的要求

马来西亚证券委员会于2019年5月14日发布了《业务连续性指导原则》。该规定从重大运营中断、恢复目标和策略、沟通、测试与培训、维护与审查等领域提出对金融机构的业务连续性管理相关要求。

金融机构在遵循《业务连续性指导原则》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《业务连续性指导原则》中与云服务供应商相关的控制要求，并阐述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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
业务连续性指导原则2-重大运营中断	金融机构应确定由于关键业务功能的相互依赖和集中以及外包安排而引起的主要运营中断和风险。彻底评估和分析此类中断带来的任何不利影响和隐含风险。	客户应建立业务影响分析和风险评估机制。	作为云服务提供商： （1）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。 （2）华为云根据内部业务连续性管理体系的要求，定期开展风险评估，识别并分析支撑云服务持续运行的关键资源所面临的潜在风险。针对突出风险，进一步考虑突发事件发生的场景，并制定应对各种突发事件场景的危机管理程序，以最大程度地降低突发事件的影响。危机管理程序中详细规定了突发事件的预警和报告流程、事件升级流程、应急预案启动的条件、事件进展的通报流程、内外部沟通流程等。

原文编号	具体控制要求	客户的关注	华为云的内部实践
业务连续性指导原则3-恢复目标和策略	恢复目标和策略是根据基于风险的原则制定的，其中恢复的优先级基于金融机构业务部门对整个业务运营构成的风险程度或水平。	客户应考虑针对业务影响分析和风险评估的结果制定恢复策略。	作为云服务提供商商，华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面。
业务连续性指导原则4-沟通	为内部和外部利益相关者制定了全面的升级程序和重大运营中断期间的沟通计划，并将其嵌入业务连续性框架中。这些程序应能及时、透明和协调地传递信息，以应对因重大业务中断而产生的任何声誉风险。	客户应与内外部利益相关方建立沟通机制。	作为云服务提供商： **（1）**华为云会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。 **（2）**华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。 **（3）**为配合客户满足通知的要求，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。根据内部的客户通知通报流程，在底层基础平台发生严重事件，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。

原文编号	具体控制要求	客户的关注	华为云的内部实践
业务连续性指导原则5-测试与培训	金融机构至少每年进行一次测试和培训，以确保持续的可靠性和相关性，并结合不断发展的市场实践，日常业务运营中使用的关键人员和技术的变化以及法规政策的更新。	客户应建立业务连续性计划的测试和培训机制。	华为云作为云服务提供商，会积极配合客户发起的测试需求，协助客户测试其业务连续性计划的有效性。同时，华为云根据内部业务连续性管理体系的要求，每年对业务连续性计划和灾难恢复计划进行测试，所有的应急响应人员，包括后备人员均需参与。测试的类型包括桌面演练、功能演练和全面演练三种，其中对高风险的场景进行重点演练测试。测试过程中，华为云将根据流程，选择测试场景，制定完整的测试计划和程序，并记录测试结果。在测试完成后，相关人员编写测试报告，对测试过程中的问题进行总结。同时，若测试结果表明业务连续性计划、恢复策略或应急预案等存在不足之处，将对相关文件进行更新。
业务连续性指导原则6-维护与审查	金融机构定期维护和审查业务连续性的方法或框架。董事会和高级管理层确认，批准并认可任何重大更新或变更。 鼓励员工注意此类更新或更改。	客户应考虑定期对业务连续性计划进行维护和审查。	作为云服务提供商，华为云根据内部业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。业务连续性计划、突发事件应急预案、灾难恢复操作手册等文件通过电子和纸质的方式保留多个副本，并分发给相应的管理层及其他主要人员。

13 结语

本文描述了华为云为客户提供的云服务如何遵从马来西亚金融行业监管要求，并表明华为云遵守马来西亚国家银行（BNM）和马来西亚证券委员会（SC）发布的重点监管要求，有助于客户详细了解华为云对马来西亚金融行业监管要求方面的遵从性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署遵从马来西亚金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

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

14 版本历史

日期	版本	描述
2023年2月	2.0	合规要求更新
2022年4月	1.1	例行刷新
2020年9月	1.0	首次发布