# 华为云泰国金融行业监管遵从性指南

文档版本 2.0

发布日期 2024-12-26

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/intl/zh-cn/

# 目 录



# 1 概述

## 1.1 背景与发布目的

在科技发展的浪潮中，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降低成本、提升运营效率、实现业务模式的创新。为了规范金融行业对于信息科技的运用，泰国央行（BoT）、证券交易委员会办公室（OSEC）、保险委员会办公室（OIC）发布了一系列监管要求和指南，针对泰国金融机构科技风险管理、科技外包管理以及云计算实施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。本文将针对泰国金融机构在使用云服务时通常需遵循的监管要求和指南，详细阐述华为云将如何协助其满足监管要求。

## 1.2 适用的泰国金融监管要求简介

**泰国央行（BoT）**

- **No. FPG 8/2557 金融机构外包管理规定**（Regulations on Outsourcing of Financial Institutions）：针对利用服务供应商提供外包服务的金融机构，提出金融机构需要遵守的外包管理相关要求，为金融机构外包活动的风险管理提供指导。
- **No. FPG 21/2562 金融机构信息科技风险管理规定**（Information Technology Risk Regulations of Financial Institutions）：规定了科技风险管理原则和实施指引，指导金融机构建立健全、可靠的科技风险管理框架。
- **No. Sor Nor Chor. 6/2561 关于开展指定支付服务业务综合监管的规定**（Regulations on General Supervision of Undertaking Designated Payment Service Business）：为泰国指定的支付服务业务提供商制定了开展支付业务的综合监管条例，包括治理、风险管理、用户保护等，形成了明确的监管框架。
- **No. Sor Nor Chor. 11/2561 维护信息系统安全的政策和措施**（Policies and Measures on Security of information Technology Systems）：为泰国的支付系统、指定支付系统和指定支付服务的提供者提供信息技术体系安全政策和标准。
- **No.FPG.16/2563 关于使用金融机构业务伙伴提供的服务的规定**（Regulations on the Use of Services From Business Partners of Financial Institutions）：该规定针对金

融机构选择第三方或业务合作伙伴进行金融服务部分职能的外包提出监管要求，泰国央行特此发布金融机构业务伙伴服务使用条例，以使金融机构遵守。

**证券交易委员会办公室（OSEC）**

- **No. Sor Thor. 38/2565 信息技术系统建设细则 2023**（Rules in Detail on Establishment of Information Technology System）：为从事证券服务的中介机构提供在信息技术系统建设中应当遵循的企业 IT 治理和信息安全管理要求。
- **No. Nor Por. 7/2565 信息技术系统建设指南 2023**（Guidelines for Establishment of Information Technology System）： 是对《信息技术系统建设细则》中企业 IT 治理和信息安全管理要求的解读，提供满足企业 IT 治理和信息安全管理要求的注意事项和最佳实践。
- **云计算实施指南**（Cloud Computing Practice Guide）： 旨在指导金融机构了解云计算潜在的风险，以及如何在使用云计算时进行风险管理和安全控制。

**保险委员会办公室（OIC）**

- **人寿保险公司信息技术风险 （IT 风险） 治理和管理的标准 B.E. 2563 (2020)**（OIC Guidelines for Governance and Management for information Technology Risk for Life Insurance Companies）：对泰国寿险公司提供信息技术风险监督和管理的标准。
- **非人寿保险公司信息技术风险 （IT 风险） 治理和管理的标准 B.E. 2563（2020）**（OIC Guidelines for Governance and Management for information Technology Risk for Non-Life Insurance Companies）： 对泰国非寿险公司提供信息技术风险监督和管理的标准对泰国非寿险公司提供信息技术风险监督和管理的标准。

# 1.3 名词定义

- **华为云**

  华为云是华为云旗下的云服务品牌，包括华为技术（泰国）有限公司和 Sparkoo Technologies（泰国）有限公司，致力于提供稳定、安全、可靠、可持续发展的云服务。
- **客户**

  指与华为云达成商业关系的注册用户。
- **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。
- **服务供应商**

  指通过订立合同，履行通常由金融机构自行履行的职能的其他法人，包括任何从原始服务供应商或分包商分包或转包服务的法人。
- **云计算**

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

# 2 华为云安全与隐私合规

华为云遵守业务开展地所有适用的隐私相关法律法规。华为云投入专业的法律团队紧密关注法律法规更新情况，对海内外法律法规保持持续跟踪并进行快速分析，以遵循法律法规的要求。

华为云隐私保护和个人数据安全的能力和成效在全球范围得到广泛认可，截至目前为止，华为云共取得海内外十余家机构的相关认证近 20 个，主要包括适用于全球的隐私标准类、数据安全标准类证书以及区域性数据安全认证。

关于更多华为云的隐私保护和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”。

**华为云部分标准类认证/鉴证：**

| 认证 | 描述 |
| --- | --- |
| ISO27001 | ISO27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。 |
| ISO27017 | ISO27017 是针对云计算信息安全的国际认证。ISO27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。 |
| ISO27018 | ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。 |
| TL 9000& ISO 9001 | ISO 9001 是 ISO 9000 族标准所包括的一组质量管理体系核心标准之一，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。<br>TL 9000 是一个建立在 ISO9001 基础上的，由全球电信业优质供应商联盟（QuEST Forum）针对全球信息和通讯技术（ICT）行业特定设计的、为 ICT 产品和服务供方提供的一套通用的质量管理体系要求。它包括了 ISO9001 的所有要求，ISO9001 将来的任何改动也会导致 TL9000 的改动。<br>华为云取得了 ISO9001 / TL9000 认证证书，表明华为云可以为您提供更快，更好和更具成本效益的服务。 |
| ISO20000-1 | ISO20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理 |

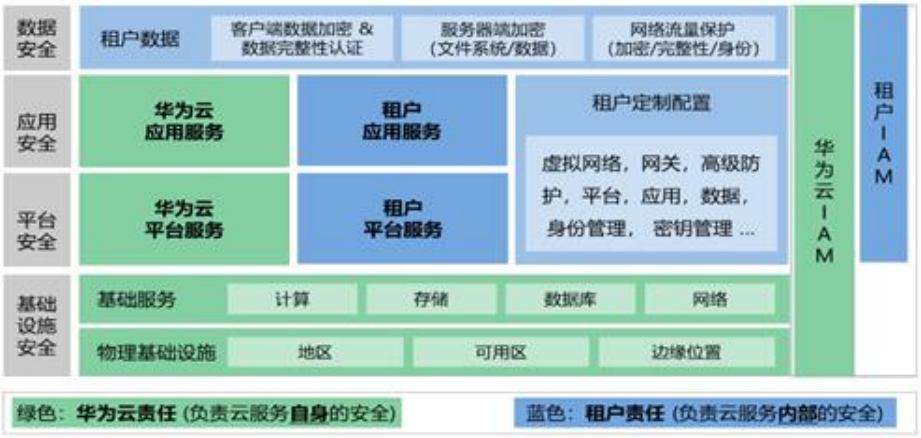
| | |
|---|---|
| | 体系的模型以保证服务供应商可提供有效的 IT 服务来满足客户和业务的需求。 |
| ISO22301 | ISO22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。 |
| CSA STAR 认证 | CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。 |
| ISO27701 | ISO27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。 |
| BS 10012 | BS10012 是 BSI 发布的个人信息数据管理体系标准，<br>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。 |
| ISO 29151 | ISO29151 是国际个人身份信息保护实践指南。ISO29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。 |
| PCI DSS | 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。 |
| PCI 3DS | PCI 3DS 标准，旨在保护执行特定 3DS 功能或者存储 3DS 数据的 3DS 环境，支持 3DS 的实施。PCI 3DS 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。 |
| ISO 27799 | ISO/IEC 27799 是专注于医疗行业的信息安全管理体系，为医疗行业和其相关机构提供了关于如何更好地保护个人健康信息的保密性、完整性、可审计性和可用性的指导。<br>华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。 |
| ISO 27034 | ISO/IEC 27034 是国际标准化组织 ISO 通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得 ISO/IEC 27034 认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。 |
| SOC 审计报告 | 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。 |

# 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 BoT《金融机构外包管理规定》的要求

《金融机构外包管理规定》：泰国央行按照工作职能对外包服务进行分类，并明确金融机构对不同类型外包的许可条件，并从金融机构的董事会的职责、服务供应商的选择、消费者保护、服务供应商的业务连续性管理、合同和协议等方面提出对金融机构外包管理相关要求，为金融机构外包活动的管理提供指导。

金融机构在遵循《金融机构外包管理规定》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《金融机构外包管理规定》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 服务供应商的选择

《金融机构外包管理规定》附件 3 第 2 条要求金融机构应当制定服务供应商选择标准，相关控制要求及华为云的应答如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 附件 3<br>第 2 条 | 服务供应商的选择 | 选择服务供应商金融机构在签订新合同或续签合同之前，必须具备适当的服务供应商选择标准，包括以下关键问题。<br>（1）技术能力、专业知识和操作经验；<br>（2）财力；<br>（3）商业信誉、投诉或诉讼记录；<br>（4）适合金融机构的组织文化和服务政 | 客户应建立制定服务供应商的选择标准。<br>**（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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 策；<br>（5）对新发展作出反应的能力；<br>（6）集中度风险。<br>（7）为董事会和高级管理人员考虑外包服务制订了清晰的规则。 | 算力之上，实现客户价值最大化。<br>**（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%。<br>**（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。在海外市场，华为云香港、俄罗斯、泰国、南非、新加坡大区相继开服。<br>**（4）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、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。华为云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。<br>**（5）对新发展作出反应的能力：**自上线以来，华为云一直坚持技术创新，发布了一系列业界领先的新品和升级，覆盖云安全、DevOps、云容器引擎和微服务引擎、服务网格、计算、云存储、网络、云容灾等多个领域，让产品始终保持先进性。<br>**（6）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。<br>**（7）运营能力：**华为云遵循 ISO27001、ISO20000、ISO22301 等国 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。 |

## 5.2 消费者保护

《金融机构外包管理规定》附件 3 第 3 条提到“金融机构必须始终意识到，外包只是将服务委托给服务供应商。金融机构继续对消费者负责，就像金融机构自己提供服务一样。”华为云若作为金融机构的云服务供应商，仅对金融机构负责。《金融机构外包管理规定》附件 3 第 3 条要求金融机构应当制定消费者的保护机制，相关控制要求及华为云的应答如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 附件 3 第 3 条（1） | 客户数据机密性 | 必须确保服务供应商能够提供良好的系统来维护客户信息和金融机构信息的安全和保密。 | 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，并遵守泰国《个人数据保护法》所述的数据保护原则。同时，在与金融行业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。<br>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。 |
| 附件 3 第 3 条（2） | 问题和事件管理 | 必须通过记录和监控客户投诉（包括客户信息泄露问题），配备足够的系统来处理客户投诉和解决问题，金融机构必须指定适当的指导方针来 | 客户应建立问题管理机制。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 解决此类问题。 | 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。<br>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。 |
| 附件 3 第 3 条（3） | 性能监控及容量规划 | 必须确保为客户提供的服务质量不会恶化并且通常由金融机构负担的成本不会由客户承担。 | 客户应建立性能监控及容量规划机制。<br>《华为云服务等级协议》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。<br>为配合客户满足合规要求，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。<br>同时，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。 |
| 附件 3 第 3 条（5） | 客户数据删除 | 无论出于何种原因终止或取消合同，金融机构必须确保客户信息被销毁或完全从服 | 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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 务供应商处移除。 | 容数据从华为云中迁移出去，如迁移至本地数据中心。<br>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，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。 |

## 5.3 服务供应商的业务连续性管理

《金融机构外包管理规定》附件 3 第 4 条要求金融机构应当对与服务供应商相关的业务连续性进行管理，相关控制要求及华为云的应答如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 附件 3 第 4 条（1） | 业务影响分析与风险评估 | 金融机构必须通过评估服务中断可能产生的风险和影响，明确外包活动的重要程度。 | 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。 |
| 附件 3 第 4 条（2） | 业务连续性计划的制定和测试 | 金融机构必须要求服务供应商制定业务连续性计划，特别是针对重大活动或影响广泛的活动，并为此类活动分配足够的资源，在符合金融机构自身业务连续性的情况下，应用泰国央行关于金融机构业务连续性管理（BCM）和 | 华为云遵循 ISO22301 业务连续性管理国际标准，建立了一套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，制定了业务连续性计划和灾难恢复计划。<br>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。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 业务连续性计划（BCP）的指导方针。<br>金融机构必须与关键服务供应商定期对业务连续性计划进行测试，并且必须以书面形式记录测试结果，供泰国央行审查。 | 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。 |

## 5.4 合同与协议

《金融机构外包管理规定》附件 3 第 5 条要求金融机构必须与服务供应商签订书面合同和协议，相关控制要求及华为云的应答如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 附件 3 第 4 条 | 合同与协议 | 金融机构必须与服务供应商签订书面合同和协议，至少考虑以下关键问题：<br>（1）金融机构的服务类型、职责范围、风险管理、内部控制流程、信息和资产安全保障体系；<br>（2）服务水平协议，规定服务供应商在正常和异常情况下必须执行的最低操作标准；<br>（3）服务供应商的业务连续性计划，以支持外包服务中断或无法提供连续服务的情况；<br>（4） 监控、审核和评估服务供应商性能 | 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 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 的过程；<br>（6）合同期限、规定和合同终止条件，包括金融机构修改或延长合同的权利；<br>（7）服务延误、差错等问题发生时对方的责任范围，以及解决问题的准则或赔偿损失；<br>（8）信息安全，维护客户信息、金融机构信息的机密性和保密性，以及访问权和信息所有权，以及数据传输、数据维护，客户信息、金融机构信息泄露的明确处罚；鉴于此，服务供应商应将金融机构客户的数据库与服务提供商或服务提供商其他客户的数据分开。<br>（12） 遵守监管条例；<br>（13）赋予泰国央行、金融机构、外部审计师或其他政府机构检查运营、内部控制流程以及向服务供应商或分包商（如有）索取相关信息的权利。 | |

## 5.5 外包活动的管控

《金融机构外包管理规定》附件 3 第 6 条要求金融机构应当监控、评估、审计和管理外包服务供应商的风险，相关控制要求及华为云的应答如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 附件 3<br>第 6 条<br>(2)(4)(5) | 外包活动的管控 | （2）安排或要求服务供应商编制操作手册和相关文件，并定期更新，以监测、评估和管理金融机构的风险；<br>（4）安排好书面的记录，包括问题或风险、数据丢失事件以及从外包服务相关管理部门接受到的指令，供泰国央行审查；<br>（5）根据职能分类的需要，安排定期审查所提供的服务。 | 华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT 服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。为配合客户满足合规要求，华为云根据内部管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。另外，华为云有专门的团队对云服务的产品说明和操作手册进行维护，在国际站上将至少提供英文版的文档。<br>同时，华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。<br>此外，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。 |

# 6 华为云如何遵从 BoT《金融机构信息科技风险管理规定》的要求

泰国央行于 2019 年 11 月发布了《金融机构信息科技风险管理规定》，该规定针对金融机构提出在信息科技风险管理方面需要遵循的准则，并提供信息科技风险管理和第三方风险管理的实施指南。

金融机构在遵循《金融机构信息科技风险管理规定》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《金融机构信息科技风险管理规定》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 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 5.3.2(2) | 数据安全 | 金融机构必须维护数据安全，包括通过通信网络的数据存储，信息系统和各种介质的数据存储及传输。<br>对信息分类和分级，通过适当的安全措施保存和销毁数据，包括使用国际标准的加密算法进行加解密，以维护信息安全 | 客户应考虑对所有存储信息的介质（包括纸质和电子）进行保护。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。<br>针对存储金融行业客户内容数据的存储介质，华为云制定了介质管理流程，确保存储在介质中的数据的安全。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。实现方式如下：当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。<br>目前，华为云云硬盘（Elastic Volume Service，简称 EVS）、对象存储服务（Object Storage Service，简称 OBS）、镜像服务（Image Management Service，简称 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。<br>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 FIPS 140-2（2 级和 3 级）的主流国际安全认证，满足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。 |
| 5.3.2(3) | 访问控制 | 金融机构必须对操作系统和数据库系统进行权限的管理和审计。基于风险级别进行权限管理和身份验证，防止 | 客户应建立信息系统的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。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 未授权的访问和系统或数据篡改。 | 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。<br>此外，华为云的云审计服务（Cloud Trace Service，简称 CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。<br>为配合客户满足合规要求，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。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。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。 |
| 5.3.2(4) | 物理和环境安全 | 金融机构必须确保数据中心、办公场所、关键系统区域的安全。必须要对计算机设备和支持性设施建立保护 | 客户应当制定和实施物理和环境安全管理机制。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 体系和维护流程，防止非法入侵或自然灾害造成的损害，保证持续地支持业务运行。 | 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。 |
| 5.3.2(5) | 通信安全 | 金融机构必须对其通信系统进行安全控制，以确保通过其传输的系统和数据受到安全保护，并免受任何可能的攻击或威胁。 | 客户应当建立网络安全管理机制，确保网络中的信息及信息处理设施得到保护。<br>华为云一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。<br>华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，进一步排除单点故障的风险。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 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。 |
| 5.3.2(6) | 运行安全 | 金融机构必须对其信息技术业务进行安全控制，以确保信息技术业务的安全，这必须包括但不限于以下内容：<br>（6.1）信息技术系统和设施系统的能力管理，例如对信息技术资源的未来需求进行评估，以便对信息技术资源进行适当管理，因为这些资源能够充分支持业务运营，而金融机构则可以管理信息技术资源以满足其未来需求；<br>（6.2）服务器和用户设备（终端设备）的安全控制，如安装防病毒或防恶意软件，以防止数据泄露或未经授权的访问；<br>（6.3）数据备份-必须在适当的时间范围内（如每天）使用适当的方法备份数据，以便在原始数据不可用或损坏时随时可以使用备份数据；<br>（6.4）保存服务器和重要网络硬件的日志，如保存和审查访问日志和活动日志，以监测和检查系统或数据的访问和使用；<br>（6.5）安全监控-必须有监控可能影响关键 IT 系统的可疑事件或威胁的流程或工具，例如安装监控和分析网络威胁的系统，以便金融机构能够及时发现、预防和处理可疑事件或威胁；<br>（6.6）根据风险水平管理系 | **1.容量和性能管理：**客户可通过华为云的云监控服务（CES）对弹性云服务器（ECS）、带宽等资源进行的立体化监控。云监控服务的监控对象是基础设施、平台及应用服务的资源使用数据，不监控或触碰租户数据。云监控服务目前可以监控多个云服务的相关指标，用户可以通过这些指标，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。<br>同时，华为云内部也制定了性能与容量管理流程，通过提前识别资源需求以及对平台资源容量和设备库存进行统筹管理，对资源使用率和资源可用性水平的不断优化，最终保证云资源满足用户的业务正常需求。<br>**2.主机安全管理：**客户可用通过使用华为云的企业主机安全服务（Host Security Service，简称 HSS）来保护主机安全。企业主机安全服务提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。<br>**3.备份管理：**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（Volume Backup Service，简称 VBS）、云服务器备份 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 统漏洞-以便发现漏洞，金融机构能够迅速采取进一步行动防止可能的威胁；关键 IT 系统的漏洞评估必须至少每年或在相关技术标准发生重大变化时进行一次；<br>（6.7）渗透测试，可由独立的内部或外部专家进行；测试必须覆盖面向互联网的系统，并且至少每年或在出现任何重大变化时进行一次，以便发现漏洞，并且金融机构能够迅速作出改进，以防止可能的威胁；<br>（6.8）变更管理-必须有一个安全和充分的过程来管理和控制变更，可以是系统部署、系统配置、补丁安装等形式，以确保变更正确和完全地达到规定的目标，并防止未经授权的变更；<br>（6.9）系统配置管理-生产系统的配置必须有一个控制过程，并且必须定期审查配置，以防止操作错误；<br>（6.10）补丁管理-必须有一个在生产系统上安装补丁的控制过程，以便及时安装重要的安全补丁。 | （Cloud Server Backup Service，简称 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，保证在灾难发生时数据不丢失。<br>**4.日志和监控管理：**华为云的云审计服务（CTS）为租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。CTS 会对各服务发送过来的日志数据进行检视，确保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，确保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，以确保支撑网络安全事件回溯和合规。<br>**5.漏洞和补丁管理：**华为产品安全事件响应团队（PSIRT – Product Security Incident Response Team）于 2010 年正式成为国际应急响应论坛 FIRST 成员之一，通过该组织可实现与 471 个成员交流业界最佳实践和安全信息；华为 PSIRT 已经建立成熟的漏洞响应机制， |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。同时，华为 PSIRT 和华为云安全运维团队已经建立了漏洞感知、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。此外，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 。<br>**6.渗透测试：**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。<br>**7.变更管理：**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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。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，确保变更达到预期目的。<br>**8.配置管理：**华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的配置管理。华为云设置配置经理对所有业务单元进行配置管理，包括提取配置模型(配置项类型、各类配置项属性、配置项间的关系等)、记录配置信息等，并通过专业的配置管理数据库工具（CMDB – Configuration Management Database）对配置项、配置项的属性和配置项之间的关系进行管理。 |
| 5.3.2(7) | 系统获取、开发和维护 | （7.1）系统采集：金融机构必须为选择系统和服务供应商制定明确和适当的标准，其中应包括系统或服务供应商的信誉、认证（根据国际标准或公认的 IT 标准）、系统安全、系统支持和维护，确保系统和服务供应商能够响应金融机构的业务需求。其他关键问题还包括服务供应商更换的灵活性、技术变化或金融机构未来业务战略的变化；<br>（7.2）系统开发：金融机构必须对系统进行设计、开发和测试，以确保系统准确、安全、可靠、随时可用，并具有足够的灵活性，以适应未来的任何变化。 | 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。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。<br>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。<br>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，确保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。 |
| 5.3.2(8) | IT 事件和问题管理 | 金融机构必须妥善、及时地管理信息技术事件和问题，对事件和问题必须及时记录、分析并报告董事会、指定委员会或高级管理层。此外，金融机构必须找出这些问题的根源，才能解决实际问题，防止异常事件再次发生。 | 华为云作为 CSP，负责其提供的基础设施和 IaaS、PaaS 和 SaaS 各类各项云服务的事件和变更管理。华为云制定了事件和管理流程并定期对其评审和更新。华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且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。 |
| 5.3.2(9) | 业务连续性计 | （9.1）金融机构必须成立一个工作组或指定一个特定单 | 客户应建立自身的业务连续性机制，并制定保证其关键业务 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | 划 | 位负责编制一份信息技术业务连续性计划，该计划必须是书面的，并符合规定的政策；<br>（9.3）信息技术业务连续性计划必须切实可行，因为它可以有效地用于减少损失，并且必须符合泰国央行的政策声明：业务连续性管理（BCM）和金融机构的业务连续性计划（BCP）。计划必须规定恢复时间目标（RTO）和恢复点目标（RPO），这将取决于系统的重要性，以及最长中断容忍期（MTPD），以确保金融机构业务运营的连续性，并确保该计划能够处理可能导致系统中断或损坏的事件，如网络威胁、自然灾害。该计划还将确保金融机构能够迅速恢复系统并恢复正常运作；<br>（9.5）IT 业务连续性计划必须至少每年或在发生任何重大变化时审查和测试一次；<br>（9.6）金融机构必须建立灾难恢复站点，以便在主站点遇到中断时随时可以运行。灾难恢复站点应远离主站点，以确保它们不会共享相同的中断或同时受到相同原因（如断电、自然灾害）的影响。 | 连续的 RTO、RPO 指标。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。<br>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 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。<br>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。为配合客户满足合规要求，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。<br>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，若测试结果表明业务连续性计划、恢复策略或应急预案等存 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 在不足之处，将对相关文件进行更新。<br>为配合客户满足合规要求，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。<br>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。<br>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。 |
| 5.3.2(10) | 第三方风险管理 | （10.1）明确并书面定义金融机构与第三方之间的角色和责任，并规定泰国央行有权检查第三方运行情况的条件；<br>（10.2）监控和管理在使用服务时连接第三方或从第三方获取信息而引起的风险；<br>（10.3）确保第三方信息安全符合金融机构的信息技术安全标准和公认的网络安全国际标准的网络安全；<br>（10.4）及时响应可能发生的事件，以及对金融机构有 | 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。华为云会安排专人积极配合客户发起的审计要求。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 重大影响的事件，以保证能够持续开展业务。 | 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。<br>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，确保云服务持续运行，保障客户的业务和数据安全。 |

# 7 华为云如何遵从 BoT《关于开展指定支付服务业务综合监管的规定》的要求

## 7.1 监管要求的一般规定

指定支付服务的业务提供者应当妥善管理与承接指定支付服务业务相关的风险，使其符合业务模式。风险管理过程必须能够识别、评估、监控、控制或缓解潜在风险，至少应符合以下规定：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 4.2.3(1) | 风险管理政策 | 以书面形式建立与业务模式、规模、交易量和业务复杂程度相适应的明确的支付服务风险管理政策，该政策必须经董事会或指定委员会批准。它应包括风险管理和评估的准则、惯例、授权人员，并在适当的时间内将结果报告给董事会或委员会或授权管理层。 | 客户应建立书面形式的风险管理政策，政策需要与业务模式、规模、交易量和业务复杂程度相适应。风险管理政策需要获得董事会或委员会批准，客户需要定期与董事会或管理层进行风险管理汇报。<br>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。 |
| 4.2.3(2) | 业务连续性管理 | 建立业务连续性管理（BCM）和业务连续性计划（BCP），以支持可能发生的任何问题或事件，并与业务的类型和复杂程度保持一致，以便将影响降到最低。 | 客户应建立业务连续性管理政策和对应的业务连续性计划、程序。<br>华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立信息安全管理体 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。 |
| 4.2.3(5) | 外包管理 | 指定支付服务的业务提供者在 IT 系统功能中，包括对业务有重大影响的功能，使用其他服务提供者或第三方（外包）提供的服务代为运营的情况下，指定支付服务的业务提供者在提供服务时，仍对服务使用者负责。以及任何潜在的损害，因为服务是由业务提供商自己提供的。指定支付服务的业务提供者应采取以下措施：<br>（5.1）建立适当的风险管理流程，包括对其他服务提供者或第三方提供的服务的选择、监测、评估和审查；定期评估外包活动产生的风险。<br>在这方面，风险评估应涵盖与保护机密性和数据隐私相关的风险，以及对指定支付服务提供商关键系统的影响。<br>（5.2）签订外包协议，约定内部审计师、外部审计师和 BOT 有权在与承担指定支付服务业务有关的部分对其他服务提供商或第三方的运营和内部控制进行审计。<br>（5.3）制定涵盖外包活动的业务连续性计划（BCP）或灾难恢复计划（DRP），包括定期测试和审查计划的实施情况，以确保计划能够实际实施。<br>（5.4）如果选择来自海外的其他服务提供商或第三方提供的服务，特别是数据存储、数据处理或任何其他与数据有关的操作，指定支付服务的业务提 | 涉及支付服务的 IT 系统功能外包时，客户需要建立外包第三方审查和评估流程，签订外包协议，制定涵盖外包活动的 BCP 和 DRP，并在使用服务跨境外包时评估跨境外包的风险与数据跨境的合规性。<br>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。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。<br>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。<br>华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。<br>华为云通过全球资源为客户 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 供商必须评估此类离岸外包活动可能产生的潜在风险，例如由于通信网络或国际通信系统（信息访问）的中断或阻塞而无法获取数据的风险风险)和与遵守外国法规相关的法律风险（跨境合规），并准备支持计划以管理潜在风险。 | 提供服务。因此，客户的账号数据可能会被转移到华为云的关联公司、华为云的合作伙伴所在的国家或地区，或受到这些国家或地区访问。在这种情况下，华为云将会确保此类转移符合适用的法律要求并经过内部严格评审，如签订能够为个人数据提供充分保护的数据转移协议，或向客户告知数据跨境转移的必要性以及潜在风险等，并获得客户的明确同意。 |

# 8 华为云如何遵从 BoT《维护信息系统安全的政策和措施》的要求

## 附录《支付系统相关 IT 系统安全指引》

BoT 发布的《维护信息系统安全的政策和措施》主要通过其附录《支付系统相关 IT 系统安全指引》为支付机构的 IT 系统提供安全建设指南。

### 8.1.1 访问控制

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 1.1 | 职责分离 | 服务提供商或业务提供商应向负责信息技术系统安全的员工或单位分配职责和责任，并为组织中的员 | 客户应：<br>（一）明确职责分工，明确信息技术系统安全各领域的职责分工，确保相互制衡，以防范可能发生的操作风险。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 工建立意识、提供知识和培训，包括在违反或违反安全规则和条例的情况下建立惩戒程序。 | （二）提供培训、教育和提高认识，包括定期与组织内的人员沟通，以使工作人员跟上技术和各种新威胁的发展。<br>（三）建立惩戒程序，对违反或违反信息技术系统安全相关政策或法规的人员进行处罚。<br>客户可通过华为云的统一身份认证服务（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。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。<br>为配合客户满足合规要求，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。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。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。 |
| 1.2 | 信息技术系统的访问控制 | 服务提供者或业务提供者应建立书面程序，根据需要控制和限制对与服务和信息有关的信息技术系统的访问权限，以防止来自组织内部和外部的未经授权的人员入侵或访问系统。 | 客户应建立正式的访问控制管理政策和程序，对组织提供服务的关键信息系统设置相应的访问权限控制。<br>客户可通过华为云的统一身份认证服务（IAM）对使用云资源的用户账号进行管理。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。<br>同时，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。 |
| 1.3 | 身份认 | 服务提供商或业务提 | 客户应使用密码、个人识别号码、令牌 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | 证与责任否认（抵赖）的防范 | 供商应使用与每种业务类型的风险等级相关的适当技术（例如，使用密码、个人识别号码、令牌或智能卡、生物特征或公共密钥基础设施）来识别、认证或验证用户身份，以防止在发生争议时拒绝赔偿责任。 | 或智能卡、生物特征或公共密钥基础设施）来识别、认证或验证用户身份，对每个帐户的行为进行记录，记录使用信息技术系统的详细信息，并留存，作为出现问题时审查的证据。<br>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 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。<br>同时，华为云的云审计服务（CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 |

## 8.1.2 信息机密性和系统完整性

服务提供者或者业务提供者应当建立信息保密和服务系统完整性的措施，如开发、控制、调整、改进用于信息处理的系统或者设备，管理与服务有关的网络系统，以确保系统的完整性，具体要求如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2.1 | 信息机密性 | 服务提供者或业务提供者应制定传输、处理和存储信息的适当步骤和程序，以保持信息的机密性和准确性。 | 客户应根据重要程度确定信息的密级，确定信息的访问权限，并根据重要程度，建立可靠、安全地传输、处理和存储机密信息的程序和存储、使用和销毁程序。<br>华为云基于数据的机密性、完整性、可用性和合规性评估数据的安全级别，从数据破坏、泄露等行为对华为云造成的影响严重至轻微对数据进行分类分级。<br>华为云在设计研发阶段会制定数据流转图，通过数据流转图展示业务中各种数据的生命周期以及华为所执行的操作，并明确操作的目的。华为云各领域对于涉及个人数据处理的业务，业务负责人定期梳理本业务涉及的个人数据清单，并每年定期审视并刷新。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 华为云内部建立了数据安全管理要求与流程办法，明确华为云数据与租户数据的数据负责人，负责数据安全定级和明确数据使用与安全及隐私保护要求。<br>华为云实施数据保护措施，对传输通道采取合理的加密技术手段、采用认可的安全协议、安全加密通道或对数据进行加密。 |
| 2.2 | 系统的开发、变更控制管理、信息技术系统或数据处理设备的改进 | 服务提供者或业务提供者应建立系统程序和内部控制，以开发和控制信息技术系统的变更或改进，以降低服务系统的失败或故障风险。 | 客户应按照变更管理和系统开发的指导方针实施 IT 系统的变更。同时，客户应始终更新操作程序、备份系统和业务连续性计划，以响应任何 IT 系统的变化。此外，此类更改应传达给相关人员进行确认，以便能够正确执行工作。<br>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，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。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，确保变更达到预期目的。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，确保变更达到预期的目的。 |
| 2.3 | 与业务相关的网络系 | 服务提供者或者业务提供者应当建立防范未经授权访问服务网 | 客户建立网络通信安全管理机制，确保网络中的信息及信息处理设施得到保护。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | 统的管理 | 络系统的措施。 | 华为云一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。<br>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。其中 VPC 可为租户构建出私有网络环境，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，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，满足租户更细粒度的网络隔离需求。 |

## 8.1.3 系统可用性

服务提供者或业务提供者应提供高效和高可用性的服务，以根据需要充分支持会员或服务用户的每笔交易，并在正常和高峰时段对交易作出快速响应，包括适当的信息备份，以确保在系统损坏时系统恢复。具体要求如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 3.1 | 业务系统的风险评估与管理 | 服务提供方或业务提供方应确保服务体系的适当风险评估方法，确定风险偏好和风险承受能力的标准，以及管理潜在风险的程序。在这方面，服务提供者或业务提供者应定期进行与技术开发和现状相关的风险审查。 | 客户应针对业务建立适当的风险管理体系，制定风险评估方法，并确认组织的风险偏好和风险承受标准以及消除/管理潜在风险的手段。<br>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。 |
| 3.2 | 监控和发现信 | 服务提供者或业务提供者应监测和检测异 | 客户应监测和发现异常交易和威胁，评估系统的脆弱性，制定解决或关闭系统 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | 息技术系统的异常或漏洞 | 常情况，并关注服务中使用的各种系统的脆弱性，以评估风险并确定风险缓解措施。 | 脆弱性的措施，可以对风险较高的系统，进行渗透测试，检验安全技术的有效性。<br>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，以确保支撑网络安全事件回溯和合规。<br>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，并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。<br>华为云会对渗透测试中发现的漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后进行验证，若验证发现存在问题，则要继续修订漏洞修复方案，若验证通过，则遵循华为云变更管理流程，根据漏洞 SLA 要求制定漏洞修复计划，完成漏洞修复或规避方案的实施并向管理层反馈修复结果。 |
| 3.3 | 解决、事件响应、记录和报告 | 服务提供商或业务提供商应通过规定的报告渠道尽快监控、记录和报告安全漏洞事件。此外，在预先准备必要的预防措施时，应考虑从过去经验中吸取的教训。 | 客户应建立完善的安全漏洞、事件管理机制，对安全漏洞、事件进行及时的发现、记录和报告。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。 |
| 3.4 | 信息备份 | 服务提供者或业务提供者必须有信息备份，并且必须定期对其进行验证，以保持服务的准确性、完整性和可用性。 | 客户应建立信息备份机制，通过多备份或异地备份等方式保障备份的可用性和准确性，并定期对信息系统的备份进行备份完整性校验。<br>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，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，保证在灾难发生时数据不丢失。<br>同时，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。 |
| 3.5 | 业务连续性计划或应急预案 | 服务提供商或业务提供商应根据情况制定高度重要的支付系统、指定支付系统或指定支付服务的服务业务连续性计划，并 | 客户应建立自身的业务连续性机制，并制定保证其关键业务连续的 RTO、RPO 指标。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。<br>为向客户提供持续、稳定的云服务，华 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 实施该计划，以确保在服务暂停事件发生后，服务能够在规定的时间内继续进行。 | 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。<br>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。为配合客户满足合规要求，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。 |

# 9 华为云如何遵从 BoT《关于使用金融机构业务伙伴提供的服务的规定》的要求

泰国央行于 2020 年 12 月 23 日发布了《关于使用金融机构业务伙伴提供的服务的规定》，该规定针对金融机构选择第三方或业务合作伙伴进行金融服务部分职能的外包提出监管要求，泰国央行特此发布金融机构业务伙伴服务使用条例，以使金融机构遵守。

金融机构在遵循《关于使用金融机构业务伙伴提供的服务的规定》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《关于使用金融机构业务伙伴提供的服务的规定》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 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 5.2.1 | 战略职能承担 | 金融机构可以使用商业伙伴（包括法人和自然人）提供的服务，这些合作伙伴在风 | 金融机构可以使用外包服务商提供的服务，但应承担自身组 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 险管理和客户保护方面有适当的指导方针。但是，战略职能必须由金融机构自身来承担。 | 织的战略方针职能<br>华为云应为金融机构客户提供风险管理和客户保护方面的指导方针。<br>华为云自身遵从成本效益原则设立风险管理目标，制定华为云风险评估、风险顶、风险处置相关的管理机制和操作细则，并每年对业务领域的风险进行全面评估，对发现的风险明确风险接口人或风险处置 Owner 并制定风险处置方案，不同级别的风险规定了不同期限的处置要求。<br>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，并遵守泰国《个人数据保护法》所述的数据保护原则。同时，在与金融行业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。<br>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。<br>作为金融机构的外包服务提供商，华为云将自身的对风险管理以及客户保护的优秀实践以白皮书或合规文档的形式对外展现，客户可以访问官网信任中心查看相关的优秀实践。 |
| 5.3.1 | 商业伙伴使用服务的 | （一）金融机构可在非战略性职能中使用业务合作伙伴的服务，以提高业务运营效 | 金融机构可以对自身非战略职能的业务使用外包服务，如果金融机构发现有必要使用同一 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | 一般范围和条件 | 率、企业风险管理、成本和业务效益为主要目的。<br>（二）金融机构必须自行履行战略性职能。如果金融机构发现有必要使用同一业务集团内业务伙伴的战略职能服务，金融机构应逐案向泰国银行申请批准。<br>（三）金融机构可以使用商业伙伴的服务，既可以是法人也可以是自然人，也可以是本地和海外的。<br>（四）财务公司和信贷机构不能指定银行代理，但可以使用国内的外包商提供的服务。<br>（五）在泰国注册的商业银行的海外分行应遵守该分行所在国监管机构发布的关于使用业务伙伴服务的范围和条件以及客户保护的规定。 | 业务集团内业务伙伴的战略职能服务，金融机构应向泰国银行申请批准。<br>金融机构可以使用本地或海外的外包服务，其中财务公司和信贷机构仅可以使用国内的外包商提供的服务。<br>在泰国注册的商业银行的海外分行应该遵守当地对外包服务的监管要求并保障客户的安全。<br>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，并遵守泰国《个人数据保护法》所述的数据保护原则。同时，在与金融行业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。<br>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。 |
| 5.3.3 | 风险管理 | 使用商业伙伴可能会给金融机构带来风险，如声誉风险、操作风险、与商业伙伴系统连接的信息技术风险以及商业伙伴服务中断时的业务连续性风险。金融机构必须有风险管理指南来管理业务伙伴的使用，如下所示。<br>（一）金融机构必须建立业务伙伴服务使用准则，至少涵盖业务伙伴服务的使用范围、重大风险程度或对客户 | 华为云使用 RPO、RTO、灾难恢复成功率等指标来评估灾备目标的达成情况，并定期进行业务影响分析和风险评估，以确定关键业务流程和恢复目标。它还制定了详细的业务连续性计划和灾难恢复策略，并定期进行演练测试以确保其有效性。同时，华为云也根据业界标准与先进要求制定了业务连续性管理规定和事件响应策略，对关键岗位进行培训，并 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 的影响，并应每年或在发生重大变化时进行审查。<br>（二）金融机构应确保业务伙伴向客户提供的服务与金融机构自身提供的服务一样，并遵循以下 3 项重要原则：1)适当保护客户的最低权利，特别是在数据安全、投诉和服务问题的处理方面。2)业务连续性和 3)使用业务伙伴服务的风险管理体系，该管理体系与重大风险和影响程度相适应，涵盖相关风险，尤其是声誉风险、运营风险和信息技术风险，其中业务伙伴选择流程和业务伙伴风险管理涵盖关键问题（详见附件 3-6）。<br>（三）金融机构必须确保为其提供服务的业务伙伴遵守相关法律法规，如数据隐私法、反洗钱法、外汇管制法和泰国央行关于市场行为的通知。<br>（四）金融机构必须确保业务伙伴的各级分包商也必须遵守 5.3.1-5.3.2 中要求的法规和条件。 | 定期更新灾难恢复计划。<br>华为云自身遵从成本效益原则设立风险管理目标，制定华为云风险评估、风险顶、风险处置相关的管理机制和操作细则，并每年对业务领域的风险进行全面评估，对发现的风险明确风险接口人或风险处置 Owner 并制定风险处置方案，不同级别的风险规定了不同期限的处置要求。<br>华为云法务部负责识别适用于华为云业务的网络安全、隐私保护、知识产权等领域的法律法规等要求及每年监管要求的更新。<br>同时，华为云每年对网络安全进行合规稽查，包括业务自查、技术评估和审计出现的严重问题，以及外部的要求，具体包括外部监管的合规要求、客户提出的安全隐私要求、监管要求落地执行的情况、业界的危机的稽查。稽查和整改结果向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。 |
| 5.5 | 泰国银行、外部审计师或其他监管机构的审计 | 金融机构必须确保泰国银行、外部审计师或其他官方组织能够审计代表金融机构提供服务的业务合作伙伴，或分包商（如果有），并且还拥有与用于审计的服务相关的准确和最新数据。 | 金融机构必须使用泰国银行、外部审计师或其他官方组织对其的业务外包服务商进行审计，并且还拥有与用于审计的服务相关的准确和最新数据。<br>华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT 服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。为配合客户满足合规要求，华为云根据内部管理体系的要求，每年定期对所有体系文件进行审核及做出 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 必要的更新。另外，华为云有专门的团队对云服务的产品说明和操作手册进行维护，在国际站上将至少提供英文版的文档。<br>同时，华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。<br>此外，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。 |
| 附件 3 | 商业伙伴选择指南 | 金融机构必须在签订合同或协议或审查延长合同或协议之前，制定有关选择适当业务伙伴的指导原则。金融机构必须根据风险水平和所使用的服务制定业务伙伴选择指南，涵盖以下关键问题。<br>（一）技术能力、专业知识、运营经验和提供服务的准备度<br>（二）金融稳定<br>（三）商业信誉、投诉历史或起诉历史<br>（四）适合金融机构的组织文化和服务提供政策<br>（五）适应新发展的能力<br>（六）该业务伙伴同时为许多其他金融机构或其他人提供服务的集中风险<br>（七）有关于考虑使用与董事和高级管理人员有关的业务伙伴提供的服务的指导原则（利益冲突） | 金融机构在签订合同、协议或审查延长合同、协议之前，需要制定选择适当业务伙伴的指导原则。这些指导原则应考虑以下关键问题：业务伙伴的技术能力、专业知识、运营经验和准备度；业务伙伴的金融稳定性；业务伙伴的商业信誉、投诉历史或起诉历史；业务伙伴是否适合金融机构的组织文化和服务提供政策；业务伙伴是否具备适应新发展的能力；业务伙伴是否存在同时为其他金融机构或其他人提供服务的集中风险；以及与考虑使用与董事和高级管理人员有关的业务伙伴提供的服务的指导原则（利益冲突）相关的问题。<br>华为云按照客户要求的网络安全与隐私要求对自身进行管控与监督。华为云会配合金融客户对自身提供云服务外包的资质进行评估。在提供金融外包云服务前，华为云会提供标准合同协议、服务协议级保密协 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 议，约定双方的责任与义务、服务水平等要求。在提供外包云服务后，华为云会配合金融机构客户对自身安全体系稽查检查并提供相应的证据或资质证明，稽查内容包括供应商安全组织、安全研发测试、漏洞管理等领域。 |
| 附件 4 | 商业伙伴合同或协议应包含的问题 | 金融机构必须与业务合作伙伴以书面形式签订合同或协议，此类合同或协议至少应涵盖以下关键问题。<br>（一）金融机构资产存放的业务种类、职责范围、风险管理、内部控制制度、安全制度等内容。<br>（二）服务水平协议，规定在正常和非正常情况下必须执行的最低服务标准。<br>（三）业务连续性计划，以在服务中断且无法持续提供时提供支持。<br>（四）监测、审计和评估运行效率的步骤。<br>（五）服务费（如有）必须合理，并参考成本或一般市场费率。它不得向商业集团内外的任何个人或法人提供不相称的利益。<br>（六）合同期限、终止合同的条款和条件，包括金融机构修改或延长合同的权利。这是为了在必要时灵活改进服务，也是为了防止金融机构未来经营的障碍。<br>（七）服务问题的责任范围，如服务延误或错误，以及解决问题的方向和发生的损失的补救。<br>（八）信息安全，维护客户和金融机构数据的机密性和隐私，包括数据的访问权限和所有权，如数据传输方 | 金融机构必须与业务合作伙伴以书面形式签订合同或协议，此类合同或协议至少应涵盖外包业务类型、外包服务商需要具有的风险管理、内部控制制度安全制度等，服务水平协议 SLA，业务连续性计划，审计和评估运行效率的步骤、服务费、合同期限或终止合同的条款等，信息安全维护客户和金融机构数据的机密性和隐私，包括数据的访问权限和所有权的要求，安全事件处理和补救机制等。<br>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。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 法、数据存储方法，以及客户和/或金融机构数据被泄露时的明确处罚。<br>（九）不得阻止或禁止向其他金融机构提供相同服务。<br>（十）遵守泰国银行规定的法规以及其他相关法律法规。<br>（十一）其他适当条件，如服务地点、保险、使用境外服务等。<br>（十二）允许代表金融机构提供服务的商业伙伴部分或整体分包的条件，其中此类分包人必须遵守本通知中规定的准则并与金融机构达成的协议。<br>（十三）授权泰国银行、金融机构、外部审计师或其他官方机构审计业务、内部控制系统以及向代表金融机构提供服务的业务伙伴或与提供的服务相关的分包商（如有）索取相关数据。如果进行审计需要获得代表金融机构提供服务的业务伙伴的监管机构的许可，金融机构或代表金融机构提供服务的业务伙伴必须采取行动，确保审计可以合法地进行。 | |

# 10 华为云如何遵从 OSEC《信息技术系统建设细则》和《信息技术系统建设指南》的要求

《信息技术系统建设细则 2023》是泰国证券交易委员会办公室（OSEC）为从事证券服务的经营者（以下简称“经营者”）提供在信息技术系统建设中应当遵循的企业 IT 治理和信息安全的管理要求。《信息技术系统建设指南 2023》是对《信息技术系统建设细则 2023》的管理要求的进一步解读， 提供满足管理要求的注意事项和最佳实践。

《信息技术系统建设细则 2023》通过附件《附件 2 信息技术治理》、《附件 3 信息技术安全》和《附件 4 信息技术审计》为经营者提供在信息技术系统建设所需要遵循的 IT 治理、IT 安全和 IT 系统审计的要求。

经营者在遵循上述法规要求时，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《信息技术系统建设细则 2023》及其相关附件和《信息技术系统建设指南 2023》中与云服务供应商相关的控制要求，并阐述华为云会作为云服务供应商，如何帮助中介机构满足这些控制要求。

## 10.1 信息技术系统建设细则-正文

《信息技术系统建设细则》第 4、5、6 条要求经营者应当根据附件 2、3、4 的内容进行信息技术系统的治理、安全管理与信息技术审计，并每年按照 OSEC 要求开展信息技术系统的风险等级评估，相关控制要求及华为云的应答如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 4 & 6 | 风险等级评估 RLA | 1. 为遵守本通知规定，业务经营者应根据风险等级评估表（RLA）评估信息技术系统对其业务经营的影响，并按照证监会办公室网站规定的格式和程序，于每年第四季度内向证监会办公室提交评估结果。<br>第 1 款规定的 RLA 的结果应由董事会或董事会指定的负责该事项的人员审议。<br>2. 在评估第 4 条规定的 2023 年与信息技术系统（RLA）相关的风险水平时，业务经营者应采取以下行动： | 金融机构需要按照本细则要求，每年基于证券交易委员会办公室 OSEC 官网发布的风险等级评估表 RLA 评估机构内信息系统对业务的风险影响，并在每年第四季度向 OSEC 提交 RLA 报告，提交前 RLA 需要机构的董事会或指定负责人进行审阅。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | （一）评估风险等级，并于 2023 年 7 月 31 日前将首次评估结果报送证监会办公室；<br>（二）评估风险等级，并于 2023 年 12 月 31 日前将第二次评估结果报送证监会办公室。 | 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。 |

# 10.2 信息技术系统建设细则-附件 2《信息技术治理》

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| Part 1 | 董事会的作用和职责 | 企业经营者应确保 IT 风险治理将由其董事会进行监督，以确保 IT 风险与风险偏好保持一致，同时考虑企业风险管理（如果有）。经营者应当至少说明下列事项：<br>1.1 建立 IT 治理框架并监督 IT 计划，确保 IT 计划符合业务计划，并充分适应未来 IT 变化和业务运营变化；<br>1.2 为业务运作配置适当、充足的 IT 资源和 IT 人员；<br>1.3 IT 风险监管相关的书面政策规定，至少应涵盖第二部分第 2.2 条规定的政策；<br>1.4 建立 IT 风险管理和 IT 安全的流程和程序，以符合第 1.3 条的政策，包括确保其适当实施；<br>1.5 持续和有效地培养主管和人员对 IT 风险的知识和意识；以及<br>1.6 每年至少一次监控、审查和向董事会报告第 1.3 条政策的符合情况。如果发生任何可能对这些政策的符合性产生重大影响的事件或变化，应立即通知董事会。 | 客户应明确信息安全组织，定义信息安全角色和职责，并建立信息安全职责分离或交叉检查的机制。<br>华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。在组织方面，华为云的最高管理层负责决策和批准公司总体网络安全战略。华为云安全管理部门负责制定和执行华为端到端网络安全保障体系。华为云安全管理部门直接向公司首席执行官汇报。华为云信息安全管理体系已建立职责分离机制，实现内部职责权限分离。华为云对于内部人员实行基于角色的访问控制权限管理，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使用网络分析和监控工具。 |
| Part 2 | 组织 IT | 2.1 企业经营者应建立 IT 治理框 | 客户应建立符合 3LoD 三 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | 风险治理 | 架，该框架至少应包含以下特征：<br>2.1.1 实现独立制衡；以及<br>2.1.2 符合三道防线（3LoD）概念，在此概念下，与 IT 相关的职责明确划分如下：<br>第一道防线：作战<br>第二道防线：风险管理和遵守适用的法律法规；以及<br>第三道防线：审计<br>2.2 经营者应以书面形式制定信息技术风险监管政策，并经董事会或董事会指定的委员会批准，具体如下：<br>2.2.1 IT 风险管理政策：<br>（一）IT 风险管理相关人员的角色和职责；<br>（二）建立 IT 风险管理流程，确保风险符合组织的风险偏好。<br>2.2.2 IT 安全策略：<br>（一）组织 IT 安全；<br>（二）人员及第三方管理；<br>（三）IT 资产管理；<br>（四）数据安全；<br>（五）访问控制；<br>（六）密码控制；<br>（7）物质和环境安全；<br>（八）IT 操作安全；<br>（九）通信系统安全；<br>（十）IT 项目管理、系统采购、开发和维护；<br>（十一）IT 事件管理；<br>（十二）资讯科技应变计划。<br>2.3 经营者应根据第 2.2 条的政策进行经营，具体如下：<br>2.3.1 将第 2.2 条规定的政策按照其角色、职责和数据访问权限以易于访问的方式传达给相关人员以确认，以使相关人员正确理解 | 道防线的 IT 治理框架并明确划分 IT 相关的人员职责。同时，客户应按细则的要求制定完善的信息技术风险监管政策和实施政策的相关程序与流程，并至少每年对政策、流程和程序进行审查与刷新。<br>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。<br>同时，华为云参照 ISO27001 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，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性等。全方位保护客户系统和数据的保密性、完整性和可用性。此外，华为云重点关注员工以及外包人员的安全意识培养，制定了可落地的安全意识培训计划并定期执行。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 和遵守政策；<br>2.3.2 根据第 2.2 条规定的政策建立运营流程和程序；<br>2.3.3 如果第 2.2 条规定的政策发生变更，应将此类变更通知所有相关人员，并应修订操作流程和程序以符合此类变更。<br>2.4 企业经营者应至少每年审查或修订第 2.2 条规定的政策一次，一旦发生任何可能对 IT 风险的治理和管理产生重大影响的事件，不得延误。 | |

# 10.3 信息技术系统建设细则-附件 3《信息技术安全》& 信息技术系统建设指南-附件《IT 系统建设指南》

信息技术系统建设细则的附件 3《信息技术安全》和信息技术系统建设指南的附件《IT 系统建设指南》为证券业务经营者从 12 个信息安全管理体系控制域，提供了构建安全的信息技术安全体系提供落地细则和指南。

## 10.3.1 信息安全组织

根据《信息技术安全》第 1 条和《IT 系统建设指南》第 2.1 条要求，经营者应当保证有至少具备下列特征的组织机构：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 1 & IT 系统建设指南 2.1 | 信息安全组织 | 1.1 建立 IT 运营的组织结构，以书面形式详细说明人员的职责和责任；以及<br>1.2 建立 IT 操作交叉检查机制，防范潜在风险； | 客户应明确信息安全组织，定义信息安全角色和职责，并建立信息安全职责分离或交叉检查的机制。<br>华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。在组织方面，华为云的最高管理层负责决策和批准公司总体网络安全战略。华为云安全管理部门负责制定和执行华为端到端网络安全保障体系。华为云安全管理部门直接向公司首席执行官汇报。华为云信息安全管理体系已建立职责分离机制，实现内部职责权限分离。华为云对于内部人员实行基于角色的访问控制权限管理，限定不同岗位不同职责的人员只 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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使用网络分析和监控工具。 |

## 10.3.2 人员及第三方管理

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 2 & IT 系统建设指南 2.2 | 人员管理 | 2.1 相关人员或使用 IT 系统开展工作的人员：<br>经营者应当按照 2.1 条的规定适当地进行人事管理，至少应当采取下列行为：<br>（一）具有下列人员遴选程序；<br>（1.1）考虑操作中的知识、能力和充分性；<br>（1.2）聘前对人员的背景进行充分审查，并与岗位职责和职责相符。<br>（二）要求工作人员对下列事项进行理解、确认并签字确认：<br>（2.1）该等人员在资讯科技保安方面的角色及职责；及<br>（2.2）保密协议<br>（三）提高组织内可以访问数据或应用系统的人员对 IT 风险的认识，使他们能够安全地使用应用系统；<br>（四）要求人员不得以会对资本市场造成损害或非法的方式使用 IT 系统，或违反业务经营者的要求或行为准则（如有）；<br>（5）制定纪律处分政策，以回应违反或未能 | 客户应建立云服务供应商的信息安全管理机制，明确在使用云服务时对云服务供应商的信息安全要求。<br>同时，客户在管理相关人员或使用 IT 系统开展工作的人员以及与第三方进行合作时，要采取一系列措施来确保 IT 安全和保护敏感数据。具体措施包括：对人员进行背景审查和签署保密协议，提高组织内人员对 IT 风险的认识，制定纪律处分政策，建立离职程序等；对第三方进行评估和管理，签订保密协议，监督和管理第三方的服务使用，维护 IT 安全，做好应对 IT 事故的准备等。<br>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。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。<br>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。<br>华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 遵守资讯科技保安政策及措施的人员；及<br>（6）建立在雇佣结束或职位变动时要采取的程序，以防止对 IT 资产的潜在破坏或损害。<br>2.2 经营者有下列行为之一的，对第三方进行管理：<br>2.2.1 使用第三方的 IT 服务；<br>2.2.2 IT 系统与第三方对接；或<br>2.2.3 允许第三方访问经营者的敏感数据或客户数据。<br>经营者对第 2.2.1、2.2.2 或 2.2.3 条规定的第三方的管理，应按下列方式进行：<br>（一）评估第三方（包括其分包商(如有）)使用服务、连接或访问数据的风险；<br>（二）确定选择第三方的程序和标准；<br>（三）以书面形式明确说明经营者和第三人的作用和责任；<br>（4）如果根据第 2.2 条第 1 款的风险评估结果，第三方是重要的 IT 服务提供商，则服务协议或合同应明确规定业务经营者、SEC 办公室以及业务经营者或 SEC 办公室指定的外部审计师对该第三方的运营和内部控制进行审计的权利。<br>如果有必要的理由阻止经营者在协议或者合同中约定上述第一款的审 | 响应及配合客户方发起的审计活动。<br>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（OMS）和主机迁移服务（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。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 计权，则经营者应当具有审慎、充分并与使用服务、连接或者数据访问的风险和重要性相适应的评估或者监控措施；<br>（五）与第三方或其分包商签订保密协议，如果这些人可以访问经营者的敏感数据或客户数据；<br>（六）监督、监控和管理来自第三方的服务的使用、连接或访问数据的风险，这些风险应与该第三方的风险水平和重要性水平相一致；<br>（7）从使用服务、连接或访问来自第三方的数据方面维护 IT 安全，以符合企业经营者的 IT 安全标准；以及<br>（八）做好准备，以应对任何可能造成重大影响的资讯科技事故，以确保服务或业务运作的连续性。 | |

## 10.3.3 IT 资产管理

《信息技术安全》第 3 条和《IT 系统建设指南》第 2.3 条规定，企业经营者应建立 IT 资产管理，以确保 IT 安全操作的适当、完整和最新，具体如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 3 & IT 系统建设指南 2.3 | 资产管理 | 3.1 编制硬件和软件的 IT 资产清单，包括其许可证；<br>3.2 指定一个人或单位负责每一项信息技术资产；以及<br>3.3 提供 IT 资产的定期维护。 | 企业经营者建立 IT 资产管理，以确保企业的 IT 操作安全、完整和最新。具体要求如下：<br>1.编制硬件和软件的 IT 资产清单，包括其许可证：企业应该对所有的硬件和软件进行清单管理，包括它们的许可证信息，以便对它们进行有效的管理和维护。<br>2.指定一个人或单位负责每一项信息技 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 术资产：企业应该指定一个人或单位负责每一项信息技术资产，以便对其进行有效的管理和维护。<br>3.提供 IT 资产的定期维护：企业应该对 IT 资产进行定期的维护，以确保它们的正常运行和安全性。<br>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。<br>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。 |

## 10.3.4 数据安全

《信息技术安全》第 4 条和《IT 系统建设指南》第 2.4 条规定，经营者应当妥善维护数据安全，确保其机密性、完整性和可用性，具体如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 4 & IT 系统建设指南 2.4 | 数据安全 | 4.1 指定个人或单位为数据所有者；<br>4.2 与数据分类相一致的数据分类和安全指南，包括以下数据：<br>4.2.1 终点数据<br>4.2.2 传输中的数据<br>4.2.3 静息数据<br>4.3 建立安全数据输入、数据处理和数据处理的指南；<br>4.4 编制一份完整和最新的数据清单。 | 经营者在处理数据时，应该采取一系列措施来确保数据的安全性、机密性、完整性和可用性。具体措施包括：<br>1.指定个人或单位为数据所有者，明确数据的归属和责任。<br>2.根据数据的不同分类，制定相应的数据分类和安全指南，包括终点数据、传输中的数据和静息数据等。<br>3.建立安全数据输入、数据处理和数据输出的指南，确保数据在整个处理过程中的安全性。<br>4.编制一份完整和最新的数据清单，记录所有数据的来源、用途、存储位置等信息，以便管理和监控数据的使用情况。<br>5.通过这些措施，经营者可以更好地保 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 护数据的安全性和机密性，避免数据泄露、损坏或丢失等问题。<br>华为云基于数据的机密性、完整性、可用性和合规性评估数据的安全级别，从数据破坏、泄露等行为对华为云造成的影响严重至轻微对数据进行分类分级。<br>华为云在设计研发阶段会制定数据流转图，通过数据流转图展示业务中各种数据的生命周期以及华为所执行的操作，并明确操作的目的。华为云各领域对于涉及个人数据处理的业务，业务负责人定期梳理本业务涉及的个人数据清单，并每年定期审视并刷新。<br>华为云内部建立了数据安全管理要求与流程办法，明确华为云数据与租户数据的数据负责人，负责数据安全定级和明确数据使用与安全及隐私保护要求。<br>华为云实施数据保护措施，对传输通道采取合理的加密技术手段、采用认可的安全协议、安全加密通道或对数据进行加密。 |

## 10.3.5 访问控制

《信息技术安全》第 5 条和《IT 系统建设指南》第 2.5 条规定，企业经营者应确保有有效的访问控制，以防止不符合资格或未经授权的人员访问和修改系统或数据，具体如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 5 & IT 系统建设指南 2.5 | 用户访问管理 | 5.1 制定用户帐户和访问权限管理指南，并根据职责和责任对权限进行适当和定期审查，包括在不再需要此类权限时制定删除权限的流程；<br>5.2 建立适合风险并防止抵赖的认证流程；<br>5.3 规定特权用户的控制、限制和监控措施（特权用户管 | 客户应建立用户访问管理机制，对访问系统的行为进行权限限制和监督。<br>客户可通过华为云的统一身份认证服务（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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 理），具体如下：<br>5.3.1 与关键 IT 系统相关的操作系统和数据库系统登录和修改密码时，需要 MFA；<br>5.3.2 如果经营者对 MFA 有限制，则可以使用其他等效方法代替，并在申请例外批准前进行风险评估并考虑充分的风险控制措施；<br>5.3.3 严格控制和监测特权用户帐户的使用。 | 未信任网络的恶意接入。<br>此外，华为云的云审计服务（CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。<br>为配合客户满足合规要求，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。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。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。<br>同时，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 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。 |

## 10.3.6 密码管理

《信息技术安全》第 6 条和《IT 系统建设指南》第 2.6 条规定，业务经营者应通过规定加密和密钥管理的安全方法，确保数据的保密性、完整性和真实性是适当和有效的，确保密码控制是可靠的和符合国际标准的，具体如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 6 & IT 系统建设指南 2.6 | 密码控制 | 6.1 规定安全的加密方法；<br>6.2 建立密码密钥管理，规定密码密钥的产生、安装、存储、备份、撤销和销毁的控制措施；<br>6.3 就第三者所提供 | 客户在使用加密措施保护数据时，应考虑采用业内认可以及符合国际标准的加密算法和密钥管理机制。<br>同时，客户需要建立密码密钥管理政策与程序，对密码密钥加以审查。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 的密码匙订定管制措施，并须加以审查，以确保所产生的密码匙不会与其他使用者共享；及<br>6.4 规定在密码钥匙泄漏时的事件应变程序。 | 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。<br>华为云为客户提供了数据加密服务（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，确保了客户云上数据的安全。DEW 提供专属加密、密钥管理、密钥对管理、凭据管理功能，支持对称与非对称加密，同时支持 AES 、RSA、EC、DES、ECDSA、ED25519 等多种加密算法。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，满足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。<br>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。 |

## 10.3.7 物理和环境安全

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 7 & IT 系统建设指南 2.7 | 物理和环境安全 | 业务经营者应建立 IT 资产的物理和环境安全，以及与 IT 相关的硬件和设施的保护系统和维护流程，以防止存储在主站点、备份站点和第三方托管数据中心的 IT 资产受到损害。 | 客户应当制定和实施物理和环境安全管理机制。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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。 |

## 10.3.8 运行安全

《信息技术系统建设细则 2023-附件 3 信息技术安全》和《信息技术系统建设指引 2023-附件 IT 系统建设指南》规定业务经营者应制定 IT 操作安全措施，以确保与数据处理相关的操作是正确的和安全的。这些措施至少应涉及以下事项的管理：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 8.1 & IT 系统建设指南 2.8.1 | 配置管理 | 系统配置管理，建立系统配置控制流程，定期审查系统配置，以确保其正确和安全； | 客户应对其系统开展配置管理，建立系统配置控制流程，定期审查系统配置，以确保其正确和安全。<br>华为云由内部安全工程团队负责系统和组件的安全配置规范的编制和刷新，对华为云生产环境的系统和组件及进行加固，并由华为云安全事件管理团队对生产环境中安全配置的遵从情况进行抽检。华为云安全事件管理团队负责按照已发布的安全配置规范和配套的自动化检查工具，例行抽检华为云生产环境中各系统/组件安全配置遵从情况。目前华为云也采取策略即代码 PolicyAsCode 的方式对安全配置基线进行自动化检查。<br>华为云构建了配置监控平台，实现对服务器操作系统、数据库管理系统及网络设备的配置项进行实时监控。配置监控平台会将实际的配置项同标准配置基线进行对比。当出现差异时，差异分析结果会通过邮件自动发送至巡检管理员进行后续跟进处理。<br>关于华为云开发活动的安全性，可参考《华为云安全配置基线指南》。 |
| 信息技术安全 8.2 & IT | 变更管理 | 充分和安全的变更管理，以确保变更将正确和完全地满 | 客户应建立文件化的变更管理政策，并考虑通过正式的程序来管理变更以控制可能影响安全性的 IT 基础设施、IT 系 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 系统建设指南 2.8.2 | | 足规定的目标，并防止未经授权的变更； | 统和运营程序的变更。<br>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，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。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，确保变更达到预期目的。 |
| 信息技术安全 8.3 & IT 系统建设指南 2.8.3 | 容量管理 | 对于容量管理，应制定管理容量、监控系统效率和预测 IT 资源使用的措施和流程，以确保当前业务运营得到支持，并为未来使用有效分配资源。 | 客户应考虑建立正式的容量管理标准和程序，以评估和监控其 IT 基础设施的适当性，包括计算机系统、数据库系统、通信网络系统和 IT 相关设施，并对其云资源进行监控，确保云资源能够满足业务增长的需要。<br>客户可通过华为云的云监控服务（CES）对弹性云服务器（ECS）、带宽等资源进行的立体化监控。云监控服务的监控对象是基础设施、平台及应用服务的资源使用数据。云监控服务目前可以监控下列云服务的相关指标：弹性云服务器、云硬盘服务（EVS）、虚拟私有云服务（VPC）、关系型数据库服务（RDS）、分布式缓存服务（DCS）、分布式消息服务（DMS）、弹性负载均衡（ELB）、弹性伸缩服务（AS）、网站应用防火墙（WAF）、主机漏洞检测服务（HVD）、云桌面服务（Workspace）、机器学习服务（MLS）、网页防篡改服务（WTP）、数据仓库服务（DWS）、人工智能服务（AIS）等。用户可以通过这些指标，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。<br>同时，华为云内部也制定了性能与容量管理流程，通过提前识别资源需求以及对平台资源容量和设备库存进行统筹管理，对资源使用率和资源可用性水平的 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 不断优化，最终保证云资源满足用户的业务正常需求。 |
| 信息技术安全 8.4 & IT 系统建设指南 2.8.4 | 端点安全 | 服务器和端点安全旨在保护此类设备不被用作数据泄露或未经授权访问 IT 系统的渠道； | 客户在部署开发环境、测试环境和生产环境时，应保证环境间物理和逻辑层面都实现隔离，并严格管理对环境的访问。<br>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。 |
| 信息技术安全 8.5 & IT 系统建设指南 2.8.5 | 远程办公、移动设备接入和自带设备管理 | 制定远程工作、移动设备和自带设备（BYOD）的安全策略和措施，考虑相关风险并采取适当的控制措施。 | 客户应制定针对远程访问、移动设备管理以及自带设备接入 IT 系统的管理程序和流程，应建立谨慎、充分且适合 IT 系统和被访问数据的安全措施，为所访问的 IT 系统和数据建立足够的安全措施，同时考虑 BYOD 接入的相关风险并制定相应的风险控制措施。<br>**远程访问控制：**<br>华为云员工在内部办公网络中使用唯一身份标识。当需要从外部网络接入华为内部办公网络时，需通过 VPN 接入。针对运维场景，华为云通过在数据中心部署的 VPN 和堡垒机实现运维管理平台的统一运维管理和审计。数据中心外网运维人员和内网运维人员对网络、服务器等设备的本地及远程操作全部集中管理，实现用户对设备资源操作管理的统一接入、统一认证、统一授权、统一审计。<br>为实现对华为云的远程管理，不论是从互联网还是办公网接入，都要首先访问资源池堡垒机，再从堡垒机访问相关资源。<br>**移动设备管理：**<br>华为云允许员工通过移动终端进行办公，对于移动终端，华为云内部制定了移动办公终端安全管理规定，规定了移动设备的一般使用要求以及设备遗失时的删除机制，要求进行办公的移动终端需进行资产注册，并于用户账号进行绑定，确保在终端遗失后，可通过远程删除机制删除终端数据，并与账号进行解绑。<br>移动设备可通过工作所需的华为云内部 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 应用访问华为云企业办公环境，但华为云不支持如 IOS 或安卓系统的手机、平板等移动设备对生产环境，尤其是客户内容数据的访问。<br>华为云统一管理终端设备，可实现软件、数据和策略的远程停用、删除和锁定。<br>**BYOD 管理：**<br>华为云不允许员工通过自带的设备进行办公，如需通过自带设备接入华为云企业办公环境，需要进行申请与审批，并在设备上安装华为云的统一终端设备管理工具。 |
| 信息技术安全 8.6 & IT 系统建设指南 2.8.6 | 备份 | 敏感数据的备份应采用适当的方法和频率，以确保数据的可用性与恢复 IT 系统和主数据被中断或损坏的 IT 系统的目标一致。数据备份副本和数据恢复过程应至少每年测试一次； | 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。<br>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，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，保证在灾难发生时数据不丢失。<br>同时，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。 |
| 信息技术安全 8.7 & IT 系统建设指南 2.8.7 | IT 系统日志和监控 | IT 系统日志应完整、充分地制作和存储，以作为电子交易的证据。它们还可用于根据法律的要求监控和审查对数据和 IT 系统的 | 客户应建立日志管理机制，对关键信息系统的日志进行完整、充分地存储和记录，以及监测和分析。<br>华为云的云审计服务（CTS）为租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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 访问和使用。 | 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，确保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，确保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。<br>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，以确保支撑网络安全事件回溯和合规。该日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间超过 180 天，90 天内可以实时查询。华为云设置独立的内审部门，定期对运维流程各项活动进行审计，以及时发现、纠正违规行为。 |
| 信息技术安全 8.8 & IT 系统建设指南 2.8.8 | 安全监控 | 安全监控涉及使用流程或工具来预防和检测可能影响关键 IT 系统安全的 IT 事件、恶意软件或网络威胁。 | 客户应实施一种流程或工具，及时发现可能危及其关键 IT 系统安全的异常事件，如用于审查日志的流程或工具，以便了解事件或威胁，并采取适当的预防或响应行动。同时，客户应建立接收网络威胁情报的流程或工具，以便监控和分析潜在的网络威胁，并适当地预防或处理这些威胁。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 作。<br>为了保证华为云平台以及网络的安全、稳定运行，华为云采取了一系列管理措施，包括：漏洞分析和处理，日志监控和事件响应、云产品默认安全配置优化、安全补丁部署、防病毒软件部署以及定期备份系统和设备配置文件并测试其有效性。<br>华为云内部针对华为云的所有的系统、应用、网络可能面临的威胁都设置了相应的检测工具、威胁特征和攻击指标，并每周更新检测工具、威胁特征和攻击指标。 |
| 信息技术安全 8.9 & IT 系统建设指南 2.8.9 | 技术漏洞管理 | 按照风险等级对 IT 系统进行技术漏洞评估，识别漏洞并及时修复，防止潜在的网络威胁。关键 IT 系统和所有面向互联网的 IT 系统的技术脆弱性评估应至少每年进行一次，并在此类系统发生重大变化时进行，例如 IT 基础设施的变化或关键功能的增加。 | 客户建立有效的漏洞管理机制、漏洞评估计划并按照计划的目标、范围和要求执行漏洞评估，识别系统中可能存在的漏洞。<br>华为产品安全事件响应团队（PSIRT – Product Security Incident Response Team）于 2010 年正式成为国际应急响应论坛 FIRST 成员之一，通过该组织可实现与 471 个成员交流业界最佳实践和安全信息；华为 PSIRT 已经建立成熟的漏洞响应机制，针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。同时，华为 PSIRT 和华为云安全运维团队已经建立了漏洞感知、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。<br>更多信息请参见《华为云安全白皮书》8.2 漏洞管理。 |
| 信息技术安全 8.10 & IT 系统建设指 | 渗透测试管理 | 8.10.1 经营者应进行渗透测试，具体如下：<br>（一）应用系统和面 | 客户对其应用系统和面向互联网的网络系统每年至少进行一次渗透测试，并在系统发生重大变化时进行测试。对于除此之外的系统，应评估通过内部网络的入侵风险，并进行适当的渗透测试。测 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 南 2.8.10 | | 向互联网的网络系统<br>（1.1）每年至少一次；<br>（1.2）每当此类系统发生重大变化时。<br>(2)除（1）以外的系统<br>应评估通过内部网络的入侵风险，以指定范围和认为适当的渗透测试。<br>8.10.2 上述渗透测试应由独立于系统所有者的内部或外部专家进行；<br>8.10.3 一旦发现任何漏洞，业务经营者应当采取措施进行修复，并及时预防潜在的网络威胁，消除该漏洞带来的任何风险；<br>8.10.4 根据第 8.10 条的规定，业务经营者应自产生之日起至少保留两年的经营报告，其方式应使此类文件在 SEC 办公室要求时随时可供查阅；<br>8.10.5 业务经营者应在证券交易委员会办公室通知后，立即提交渗透测试结果报告。 | 试应由独立于系统所有者的内部或外部专家进行，一旦发现漏洞，应采取措施修复并预防潜在的网络威胁。经营者还应保留至少两年的经营报告，并在证券交易委员会办公室通知后立即提交渗透测试结果报告。<br>华为云的年度业务计划里包括渗透测试计划，渗透测试人员需获批准和授权后，并遵照华为云云安全渗透测试相关规定执行渗透测试。在华为云制定的渗透测试管理办法政策中，定义了漏洞扫描与渗透测试所涉及的角色以及每个角色的具体工作流程，每次渗透测试前都需要和华为云的首席安全官与区域安全官进行报备并获取审批。<br>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，并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。<br>华为云会对渗透测试中发现的漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后进行验证，若验证发现存在问题，则要继续修订漏洞修复方案，若验证通过，则遵循华为云变更管理流程，根据漏洞 SLA 要求制定漏洞修复计划，完成漏洞修复或规避方案的实施并向管理层反馈修复结果。 |
| 信息技术安全 8.11 & IT 系统建设指南 | 补丁管理 | 应通过建立一个控制在系统和设备上安装补丁程序的流程来实现补丁程序管理，以降低潜在攻击的风险。 | 客户应通过建立一个建立补丁管理的标准和规范来实现补丁程序管理，以降低潜在攻击的风险。<br>华为云建立了安全漏洞管理流程，设置了漏洞管理员及相关安全角色为漏洞的评估负责，并对定期安装关键安全补 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2.8.11 | | | 丁，降低漏洞风险，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。 |

## 10.3.9 通信安全

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 9 & IT 系统建设指南 2.9 | 网络安全管理 | 业务经营者应当具有适当的通信系统安全，以确保通信系统和通过通信系统传输的数据是安全可靠的，能够防止潜在的网络入侵或威胁，并能够提供持续的服务。 | 客户建立网络通信安全管理机制，确保网络中的信息及信息处理设施得到保护。<br>为配合客户行使对云服务供应商的监管，华为云线上的《华为云用户协议》对客户和华为的安全职责进行划分，《华为云服务等级协议》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。<br>华为云一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。所以华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。<br>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。其中 VPC 可为租户构建出私有网络环境，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，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，满足租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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 力，实现更高水平的应用程序容错性能。另外，华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，进一步排除单点故障的风险。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。<br>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。 |

## 10.3.10 项目管理与系统获取、开发和维护

根据《信息技术安全》第 10 条与《IT 系统建设指南》第 2.10 条，经营者应具备 IT 项目管理和 IT 系统的采购、开发和维护能力，确保其 IT 系统在整个生命周期内的安全性，具体如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 10 & IT 系统建设指南 2.10.1 | 项目管理 | 建立项目管理框架，以确保对重大 IT 项目进行有效管理，确保按计划准确、完整地交付项目，并实现既定目标。 | 客户以书面形式建立项目管理框架、项目管理细则。<br>华为云在公司战略的指导下制定中长期的发展规划，支撑华为云业务的持续发展，并制定年度业务计划及实施路径图，其中包含网络安全相关活动、适用的法律法规的合规要求、开展和建立各类网络安全项目、支撑的人员及资源等，确保网络安全战略的有效落实。<br>华为云至少每年审查一次网络安全管理策略和网络安全计划，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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 和建议。 |
| 信息技术安全 10 & IT 系统建设指南 2.10.2 | 系统采购 | 应建立 IT 系统和服务提供商的采购标准，以确保所采购的系统满足业务需求和 IT 安全要求。标准应考虑到服务商变更、技术变化以及与业务运营有重大关联的变化的灵活性。 | 客户应制定 IT 系统和服务提供商的选择标准，以确保所采购的系统能够满足业务需求和信息安全要求。<br>华为云按照自身的网络安全与隐私要求对供应商提出要求和监督。华为云在采购前将会对供应商资质进行评估，仅经过资质认证的供应商才能进入华为云的采购范围。在供应商引入前，需签署合同、服务协议级保密协议，约定双方的责任与义务、服务水平等要求。在供应商引入后，华为云通过供应商安全体系稽查检查供应商安全协议执行、能力状况和问题闭环管理，稽查内容包括供应商安全组织、安全研发测试、漏洞管理等领域。 |
| 信息技术安全 10 & IT 系统建设指南 2.10.3 | 开发和支持过程的安全 | 经营者应建立与 IT 系统开发相关的控制措施，包括设计、开发、系统测试和部署系统，以确保系统准确、安全、可靠、随时可用、充分灵活地适应使用并符合业务计划，至少应采取以下行动：<br>（1）制定系统的详细要求和所开发系统的技术规范，具体如下：<br>（1.1）安全；<br>（1.2）可用性；以及<br>（1.3）容量。"<br>（2）划分参与系统开发的人员的角色和责任，以确保系统在投入生产前会被审查；<br>（3）将用于开发和测试的应用系统的环境与生产环境隔离；<br>（4）建立确保源代码 | 客户应建立安全开发管理机制。<br>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。<br>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。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 开发安全的程序或工具；<br>（5）对已开发或变更的 IT 系统进行测试，确保该系统能够准确、全面地处理数据，满足用户的需要；<br>（6）有保证数据转换完整性的措施；<br>（7）有维护测试中使用的敏感数据的安全和隐私的措施；<br>（8）在电子渠道服务或电子交易相关系统有重大发展或变更时，进行性能测试，以确保该等系统能够支持符合业务需要的并发用户数和并发交易量；<br>（9）在指定第三方开发或变更 IT 系统的情况下，业务经营者应当监督并确保其操作符合协议；<br>（10）在系统部署前，有一个向管理层或业务经营者指定的委员会申请批准的程序。 | 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。<br>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，确保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。 |
| 信息技术安全 10 & IT 系统建设指南 2.10.4 | 系统变更 | （1）进行影响评估和确定变革的优先次序；<br>（2）建立一个请求变更批准的流程，该流程必须由系统所有者单位书面批准，以确保已适当考虑变更的必要性；<br>（3）在配置变更或将变更部署到生产之前进行测试，以降低潜 | 客户应按照变更管理和系统开发的指导方针实施 IT 系统的变更。同时，客户应始终更新操作程序、备份系统和业务连续性计划，以响应任何 IT 系统的变化。此外，此类更改应传达给相关人员进行确认，以便能够正确执行工作。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 在风险或影响；<br>（4）有批准经营管理部门或经营者指派的委员会批准生产变更的程序；<br>（5）实现控制源代码版本更改并支持回退的过程或工具；<br>（6）更新已变更的应用系统的支持性文件。 | 判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。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，确保变更达到预期目的。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，确保变更达到预期的目的。 |

## 10.3.11 信息安全事件管理

根据《信息技术安全》第 11 条与《IT 系统建设指南》第 2.11 条，业务运营者应及时、合理地管理 IT 事件，具体如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 11 & IT 系统建设指南 2.11 | 信息安全事件管理 | 企业经营者应及时、适当地管理 IT 事件，具体如下：<br>11.1 提供由人员、客户和相关方报告 IT 事故的联络点；<br>11.2 建立 IT 事故管理计划或流程；<br>11.3 发现对客户资产造成损害的 IT 事件、个人数据泄露和 IT 系统安全事件，立 | 客户应当建立信息安全事件管理机制。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 即向相关责任人和 SEC 办公室报告；<br>11.4 对任何 IT 事件进行根本原因分析，以制定解决方案和预防此类事件未来再次发生的指导原则；<br>11.5 记录与 IT 事件管理相关的数据，并从此类事件发生之日起至少将此类数据保存两年，以便在 SEC 办公室要求检查时随时获取此类数据；以及<br>11.6 至少每年测试和审查一次 IT 事件管理流程或计划。测试内容应涵盖网络安全演练的管理。这些测试和审查的结果应当向董事会或董事会指定的委员会报告。 | 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。<br>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。 |

## 10.3.12 信息技术应急预案

根据《信息技术安全》第 12 条与《IT 系统建设指南》第 2.12 条，业务经营者应建立 IT 应急计划，以应对妨碍正常服务或持续业务运营的 IT 事件。经营者应当有能力在合理的时间范围内将系统恢复到正常状态，具体如下：

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 信息技术安全 12 & IT 系统建设指南 2.12 | 业务连续性的信息安全管理方面 | 12.1 任命应急小组或负责编制 IT 应急计划的单位；<br>12.2 建立 IT 应急计划的编制程序，该计划应包括以下行为：<br>12.2.1 进行风险评估，识别可能中断 IT 流程和系统，从而导致业务经营者无法提供正常服务或持续经营业务的风险情景；<br>12.2.2 对 12.2.1 中的风险情景进行业务影响分析，以规定适当的恢复时间目标（RTO）、恢复点目标（RPO）和最大可容忍停机时间（MTD）；以及<br>12.2.3 编制经董事会或董事会指定的委员会批准的书面 IT 应急计划；<br>12.3 提供备份 IT 系统和必要的资源，使系统按照既定的恢复时间目标恢复；<br>12.4 将 IT 应急计划传达给相关人员，确保他们理解并能够适当地遵守 IT 应急计划；<br>12.5 每年至少审查和测试一次 IT 应急计划，并在出现任何必要的审查和测试理由时。并将检测、复核结果报告董事会或董事会指派的委员会；<br>12.6 规定处理 IT 资源过度使用或超过指定指标容量的事件的 | 客户应建立自身的业务连续性机制，并制定保证其关键业务连续的 RTO、RPO 指标。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。<br>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 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。<br>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。为配合客户满足合规要求，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。<br>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 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 流程，例如限制通过某些渠道提供的服务或断开与服务提供商或第三方的连接，从而影响 IT 系统；以及<br>12.7 提供以下联系信息，以便有效协调 IT 事件报告或请求相关外部机构的协助，此类信息应定期更新：<br>12.7.1 提供服务或与经营者 IT 系统连接的监管机构和第三方的名单；<br>12.7.2 第 12.7.1 条规定的监管机构或第三方的联系渠道和相关人员名单。 | |

# 10.4 信息技术系统建设细则-附件 4《信息技术审计》

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2 | 审核计划和审核范围定义 | 审核计划和审核范围应至少每年审核一次，并在必要的情况下进行审核，以确保范围与 IT 风险和第 38/2565 号通知一致。 | 审核计划和审核范围应至少每年审核一次，并在必要的情况下进行审核。<br>华为云已建立审计管理流程，并按该流程执行审计。审计管理流程中包括审计支持计划、风险分析、安全控制评估和总结、整改计划、报告、审阅以往报告及相关证据方面的管理要求。<br>华为云定期评审的标准例如 ISO27001、CSA STAR 认证、PCI DSS 认证、SOC 报告等，也会对华为云的安全实施进行评审。 |
| 3 | 既定计划和范围下的 IT 审计 | 3.1 信息技术审计和报告信息技术审计结果应按以下方式进行：<br>3.1.1 对于小规模企业经营者，每年至少应进行一次 IT 审计。在任何情况下，应至少每两年完成一次涵盖适用于小规模企业经营者的所有规则的 IT 审计。<br>3.1.2 对于低风险业务经营者，每年至少进行一次 IT 审计。在任何情况下，应至少每两年完成一次涵盖所有适用规则的全面审计；<br>3.1.3 对于中风险或高风险业务经营者，至少每年进行一次涵盖所有规则的全范围 IT 审计；<br>3.2 审计信息应形成文件并记录，如工作文件和审计证据，自 | 信息技术审计和报告信息技术审计结果应按以下方式进行：<br>3.1.1 对于小规模企业经营者，每年至少应进行一次 IT 审计。在任何情况下，应至少每两年完成一次涵盖适用于小规模企业经营者的所有规则的 IT 审计。<br>3.1.2 对于低风险业务经营者，每年至少进行一次 IT 审计。在任何情况下，应至少每两年完成一次涵盖所有适用规则的全面审计；<br>3.1.3 对于中风险或高风险业务经营者，至少每年进行一次涵盖所有规则的全范围 IT 审计；<br>3.2 审计信息应形成文件并记录，如工作文件和审计证据，自创建之日起至少两年。这些文件的储存方式应确保在证券交易委员会办公室提出要求时可随时查阅。<br>华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。华为内部审计团队直接向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 创建之日起至少两年。这些文件的储存方式应确保在证券交易委员会办公室提出要求时可随时查阅。 | 符合性和有效性，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。 |
| 4 | 为 IT 审计和进度监控中识别的纠正措施提供计划 | 在上述第 3 条规定的 IT 审计中确定的纠正措施的计划应与调查结果的风险水平相适应，并应监控该计划的实施进度。 | 金融机构应制定完善的审计政策，在进行 IT 审计时，如果发现了问题，就需要制定相应的纠正措施计划。这个计划需要根据调查结果的风险水平来制定，也就是说，风险越高，需要采取的纠正措施就越严格。同时，还需要监控这个计划的实施进度，确保纠正措施能够按照计划顺利实施，从而降低风险。<br>华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。华为内部审计团队直接向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。<br>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，管理层进行审阅并对整改情况进行跟进。 |
| 5 | 审核结果的编制和报告 | 5.1 上文第 3 条规定的审计结果和纠正行动计划应立即提交经营者董事会或经营者审计委员会。<br>5.2 经营者应在下列期限内，以先到期者为准，将经营者董事会或经营者审计委员会审议后的审计结果和纠正措施计划，以证券交易委员会网站上规定的形式和程序向证券交易委员会办公室报告：*<br>5.2.1 自向董事会或审计委员会提交审计报告和纠正措施计划之 | 审计结果和纠正行动计划应立即提交经营者董事会或经营者审计委员会。<br>经营者应在下列期限内，以先到期者为准，将经营者董事会或经营者审计委员会审议后的审计结果和纠正措施计划，以证券交易委员会网站上规定的形式和程序向证券交易委员会办公室报告：<br>自向董事会或审计委员会提交审计报告和纠正措施计划之日起 30 日内；<br>自完成上述第 3 条规定的报告结束日期起的 90 天内；或<br>在上述第 3 条规定的审计开始年度的日历年结束后 3 个月，如果审计结果报告不能在审计开始年度内完成。<br>审计结果报告和纠正措施计划应自生成之日起至少保存两年，以备 OSEC |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 日起 30 日内；<br>5.2.2 自完成上述第 3 条规定的报告结束日期起的 90 天内；或<br>5.2.3 在上述第 3 条规定的审计开始年度的日历年结束后 3 个月，如果审计结果报告不能在审计开始年度内完成。<br>（*注：对于 2023 年审计结果的报告，经营者应在 2023 年日历年度结束后的三个月内提交此类报告。）<br>5.3 审计结果报告和纠正措施计划应自生成之日起至少保存两年，以备 SEC 办公室要求时随时查阅。 | 办公室要求时随时查阅。<br>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。 |

# 11 华为云如何遵从 OSEC《云计算实施指南》的要求

泰国证券交易委员会办公室于 2019 年 11 月发布了《云计算实施指南》，该指南为金融机构提供了关于使用云计算服务的治理和云服务供应商管理要考虑的做法，其中对于云服务供应商管理包括：评估和选择服务供应商、服务协议、使用云计算、服务跟踪和评估、取消或终止服务使用。

金融机构在遵循《云计算实施指南》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《云计算实施指南》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。

# 11.1 评估和选择服务供应商

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2.2.1 | 服务供应商的选择 | 金融机构应明确选择云服务供应商的流程和标准，并检查服务供应商的准备情况和适用性。通过考虑重要因素，例如知识，经验，财务能力等。 | 客户应建立制定服务供应商的选择标准。<br>**（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。<br>**（2）财务状况：**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%。<br>**（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。在海外市场，华为云香港、俄罗斯、泰国、南非、新加坡大区相继开服。<br>**（4）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、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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 云结合行业需求特点和华为丰富的云服务，发布了金融行业解决方案，为银行、保险等客户提供端到端的云解决方案。 |
| 2.2.1 | 评估信息技术安全标准 | 评估信息技术安全标准，包括数据保密性、信息系统的完整性、服务的可用性，例如国际公认的安全标准评估结果，如 ISO27001、ISO27017，PCI-DSS 等。 | 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。 |
| 2.2.1 | 独立审计 | 由独立审核员提供评估检查报告，并提供技术安全标准领域报告，例如系统和组织控制（SOC）报告，报告中应包含审计范围、审计区间、审核结果中的关键问题。 | 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。 |
| 2.2.1 | 评估持续服务能力 | 评估云服务供应商的连续性实践和对将在云计算系统上使用的系统的业务影响分析的一致性，包括最大可容忍停机时间（MTD）、可接受的恢复时间目标（RTO） 和恢复点目标（RPO）。 | 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。 |

# 11.2 服务协议

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2.2.2 | 服务协议 | 金融机构在与供应商签订的服务协议中， | 客户应建立云服务供应商的信息安全管理机制，明确在使用云服务时对云 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 应考虑以下重要的条件：<br>A.服务供应商与服务用户之间的协议至少具有以下详细信息：<br>1.服务供应商的职责，以及在服务商未能遵守本协议的情况下对中介机构的责任；<br>2. 符合国际公认的信息安全标准的操作程序；<br>3. 信息技术安全、访问控制和信息披露措施；<br>4. 由独立审计师对云服务供应商的运营进行审计；<br>5. 云服务供应商转包给其他服务供应商的条件，以及其他服务供应商的运营可能造成的损害赔偿责任条款。<br>B. 分包云服务供应商在信息安全方面的资质与云服务供应商相当或符合国际标准；<br>C. 监测、评估和审查云服务供应商的服务性能；<br>D. 在替换云提供程序时迁移到新云提供程序的过程。 | 服务供应商的信息安全要求。<br>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。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。<br>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。<br>华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。<br>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（OMS）和主机迁移服务（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。 |

# 11.3 使用云计算

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2.2.3 | 组织架构（内部组织） | 金融机构应有多种渠道可以联系服务供应商应对使用问题和信息安全事件。 | 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。 |
| 2.2.3 | 访问控制 | 金融机构应：<br>（1）制定适当的身份验证方法，如在访问管理员页面时的多因素身份验证；<br>（2）密码的分配应通过正式的管理过程加以控制；<br>（3）基于职责分配访问权限，并根据定义的访问权限控制用户对信息和应用系统功能的访问；<br>（4）监控和检查用户的访问权限。 | 客户可通过华为云的统一身份认证服务（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。<br>此外，华为云的云审计服务（CTS），可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 |
| 2.2.3 | 密码管理 | 在管理由服务供应商提供的加密时，金融机构应收集以下信息：<br>• 加密算法的类型；<br>• 密钥的创建、编辑、存储、访问、撤消和销毁不应向服务供应商授予访问、存储和管理密钥的权限。 | 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。<br>华为云为客户提供了数据加密服务（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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 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，满足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。 |
| 2.2.3 | 物理和环境安全 | 金融机构应审查销毁程序，以重复使用服务供应商的设备或信息存储资源。 | 针对存储金融行业客户内容数据的存储介质，华为云制定了介质管理流程，确保存储在介质中的数据的安全。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循适用的法律法规，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。实现方式如下：当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。 |
| 2.2.3 | 运营安全 | 若就备份活动由服务供应商负责，金融机构与服务供应商达成协议，金融机构应按照协议要求对服务供应商执行备份程序进行审查。<br>金融机构应确定记录与云计算服务相关的事件的要求，并对事件日志进行监控和存储。<br>金融机构应检查和评估服务供应商漏洞管理准则并安装服务供 | 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，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，保证在灾难发生时数据不丢失。<br>华为云的云审计服务（CTS）为租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。CTS 会对各服务发送过来 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 应商的补丁。 | 的日志数据进行检视，确保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，确保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。<br>华为云建立了漏洞感知、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。 |
| 2.2.3 | 通信安全 | 金融机构应评估并确定在云环境中进行网络分段和租户隔离的需求，并根据服务协议检查服务供应商的行为。 | 为配合客户行使对云服务供应商的监管，华为云线上的《华为云用户协议》对客户和华为的安全职责进行划分，《华为云服务等级协议》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。<br>华为云在最初的从网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。客户可以使用华为云提供的虚拟私有云（VPC）服务，实现不同区域之间网络隔离。VPC 可为租户构建出私有网络环境，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，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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 控，满足租户更细粒度的网络隔离需求。 |
| 2.2.3 | 系统获取、开发和维护 | 金融机构应对云计算应用程序进行信息安全评估，并将其作为尽职调查活动的一部分来评估和检查云服务供应商的能力。<br>在使用 SaaS 的情况下，金融机构应评估和检查服务供应商以建立安全的开发程序。 | 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。 |
| 2.2.3 | 信息安全事件管理 | 金融机构应在事件管理规定中明确以下内容：<br>• 将报告给云计算用户的事件类型；<br>• 详细信息和事件响应；<br>• 向用户通知事件的时间范围和过程；<br>• 联系渠道和联系人的详细信息；<br>• 解决问题的方法。 | 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。 |

## 11.4 服务跟踪和评估

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2.2.4 | 服务跟踪和评估 | 金融机构应明确负责跟进、评估和审查服务的角色和职责，以确保服务合同和服务质量履行以及识别使用服务的潜在风险。<br>金融机构应根据其与服务供应商之间的协议条款（以下简称“云服务协议”）进行监控、评估和审查服务供应商的服务。 | 华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。<br>同时，华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。<br>此外，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。 |

## 11.5 取消或终止服务使用

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 2.2.5 | 取消或终止服务使用 | 在取消和终止云服务的使用时，金融机构应全面制定策略和计划以适当选择退出服务，以防止或消除可能产生的不良影响的风险。例如：服务中断的风险、信息安全和存储风险等。 | 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（OMS）和主机迁移服务（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。<br>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，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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 方式进行数据清除，确保其上的数据无法恢复。 |

# 12 华为云如何遵从 OIC B.E. 2563 (2020) （非人寿/人寿）保险公司信息技术风险（IT 风险）治理和管理的标准

保险委员会办公室于 2020 年 9 月发布了《B.E. 2563 信息技术风险（IT 风险）治理和管理的标准》，该标准为泰国的（非人寿/人寿）保险公司提供了治理和管理组织信息技术风险要考虑的做法，其中对于云服务供应商管理包括：评估和选择服务供应商、服务协议、信息安全事件报告等。

金融机构在遵循《B.E. 2563 信息技术风险（IT 风险）治理和管理的标准》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 B.E. 2563 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。

## 12.1 信息技术安全

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 第 23 条 | 第三方服务提供商或业务合作伙伴管理 | 如果公司聘请第三方管理服务提供商或拥有业务合作伙伴，其系统连接到其信息技术系统，或可访问其重要信息或其客户的重要信息，则公司必须安排确定评估和选择此类第三方管理服务提供商的程序和标准，以及根据服务协议与他们合作。 要求他们遵守公司的安全策略、服务水平协议 （SLA） 的条 | （寿险/非寿险）保险公司客户与第三方管理服务提供商或业务合作伙伴有系统连接或可以访问重要信息，公司需要制定评估和选择第三方管理服务提供商的程序和标准，并根据服务协议雇用他们。公司要求第三方遵守安全策略、服务级别协议（SLA）的条款，并对他们的服务进行定期检查和监控。对于信息技术外包，公司可以考虑采用符合保险委员会办公室关于管理信息技术外包标准的实用指引的运作方式。<br>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》， |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 款，以及对其服务的定期检查和监控。关于信息技术外包，公司可以考虑采用符合保险委员会办公室关于管理信息技术外包标准的实用指南的操作方案。 | 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。<br>为配合客户行使对云服务供应商的监管，华为云线上的《华为云用户协议》对客户和华为的安全职责进行划分，《华为云服务等级协议》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。 |

# 12.2 网络威胁或信息技术威胁报告

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| 第 43 条 | 网络威胁或信息技术威胁报告 | 公司必须以以下方式报告网络威胁或信息技术威胁：<br>（1）发生或确认任何与信息技术应用有关的重大问题或事故，影响提供服务、系统、被保险人的信息或公司声誉，包括对公司重要信息技术的任何攻击，或任何网络威胁攻击，及时向保险委员会办公室报告。以及公司必须向其最高层主管报告的问题或事件，包括此类事件的详细描述和原因，以及预期的影响、解决问题所采取的行动、结果、问题解决的周期和防止未来事件发生的过程；<br>（2）如果任何网络威 | （寿险/非寿险）保险公司客户需要按照以下方式报告网络威胁或信息技术威胁：首先，对于任何与信息技术应用有关的重大问题或事故，包括对公司重要信息技术的攻击或任何网络威胁攻击，公司必须及时向保险委员会办公室报告，并向最高层主管报告问题或事件的详细描述、原因、预期影响、解决行动、结果、问题解决周期和防止未来事件发生的过程。其次，如果任何网络威胁攻击导致公司提供的涉及主要信息基础设施服务的问题或事件属于低严重性、高严重性或严重严重性的网络威胁，公司必须在 72 小时内立即通知保险委员会办公室或法律要求的代理机构，并向政府机构或根据网络安全法建立的任何组织提供相关信息或与之协调，以应对和处理网络威胁。<br>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 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | 胁攻击导致公司提供的涉及其主要信息基础设施服务的问题或事件属于低严重性、高严重性或严重严重性的网络威胁，公司必须在 72 小时内毫不拖延地通知保险委员会办公室或法律要求的代理机构。并向政府机构或根据网络安全法建立的任何组织提供此类信息或与之协调，以应对和处理网络威胁。 | 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。 |

# 13 结语

本文描述了华为云如何为客户提供遵从泰国金融行业监管要求的云服务，并表明华为云遵守泰国央行（BoT）、证券交易委员会办公室（OSEC）以及保险委员会办公室（OIC）发布的重点监管要求，有助于客户详细了解华为云对于泰国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、构建和部署遵从泰国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泰国金融行业监管要求的遵从性。

# 14 版本历史

| 日期 | 版本 | 描述 |
| --- | --- | --- |
| 2024 年 12 月 | 2.0 | 监管要求刷新 |
| 2024 年 8 月 | 1.2 | 例行刷新 |
| 2022 年 4 月 | 1.1 | 例行刷新 |
| 2020 年 7 月 | 1.0 | 首次发布 |