云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

云计算安全责任共担白皮书

（2020 年）

云计算开源产业联盟

OpenSource Cloud Alliance for industry，OSCAR

2020年7月

版权声明

前　言

云计算作为新型基础设施建设的重要组成，关键作用日益凸显，市场规模呈现持续增长趋势。同时，云计算安全态势日益严峻，安全性成为影响云计算充分发挥其作用的核心要素。与传统 IT 系统架构不同，上云后安全迎来责任共担新时代，建立云计算安全责任共担模型，明确划分云计算相关方的责任成为关键。

白皮书首先介绍了云计算在市场发展、安全等方面的现状及趋势，分析安全责任承担在云计算安全发展中的必要性，以及安全责任共担模式的应用现状与痛点。重点围绕公有云场景，白皮书建立了更加精细落地、普遍适用的云计算安全责任共担模型，确定责任主体，识别安全责任，对责任主体应承担的责任进行划分，以提升云计算相关方责任共担意识与承担水平。最后，白皮书对云计算安全责任共担未来发展进行了展望，并分享了责任承担优秀案例。

参与编写单位

中国信息通信研究院、阿里云计算有限公司、腾讯云计算(北京)有限责任公司、华为技术有限公司、浪潮云信息技术股份公司

主要撰稿人

孔松、栗蔚、郭雪、王永霞、康雪婷、黄瑞瑞、王婷、胡甜、郑原斌、黄少青、王方、朱勇、贺进、周健

目 录

图 目 录

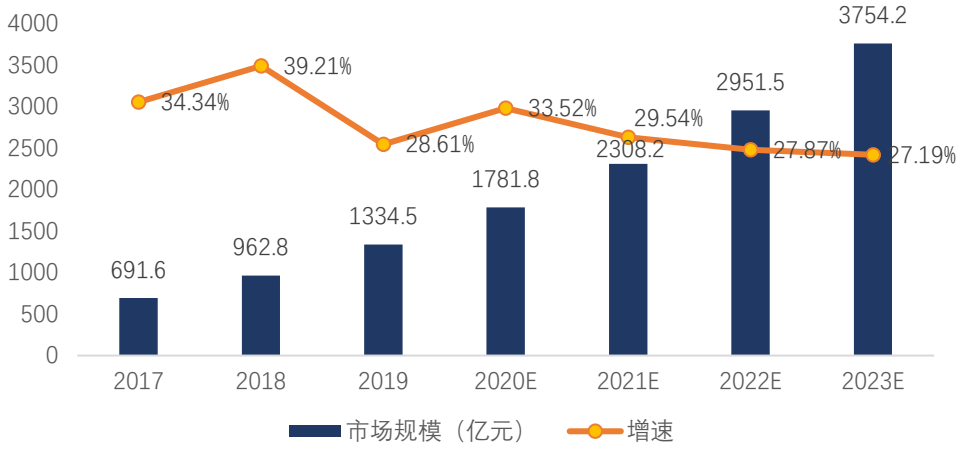
表 目 录

一、云计算安全责任共担成共识

（一）云计算作为新型基础设施，安全性成关键

随着互联网与实体经济深度融合，企业数字化转型成为必然趋势。云计算作为新型基础设施建设，是实现数字化转型的必然选择，安全性则是影响云计算充分发挥其关键作用的核心要素。

云计算“新基建”重要性凸显，市场规模将持续增长。2015 年国务院在《关于积极推进“互联网+”行动的指导意见》中第一次提出新型基础设施概念。2020 年 4 月，国家发改委首次就“新基建”概念作出正式解释，将其定义为以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系，具体包括信息基础设施、融合基础设施与创新基础设施三个方面。**云计算被纳入信息基础设施中的新技术基础设施**，在社会数字化转型中的重要性得到肯定，依托其高资源利用率、强业务承载能力等优势，成为企业信息化建设的首选。据 IDC 统计，2019 年全球云计算基础设施规模超过传统 IT 基础设施，占全球 IT 基础设施的 50%以上。在未来几年，**我国云计算市场仍将处于快速增长阶段，**据中国信息通信研究院统计，2019 年我国云计算市场（公有云、私有云）整体规模达 1334.5 亿元，增速 38.6%，2023 年预计达 3754.2 亿元，与 2019 年相比，市场规模约扩大 1.8 倍。

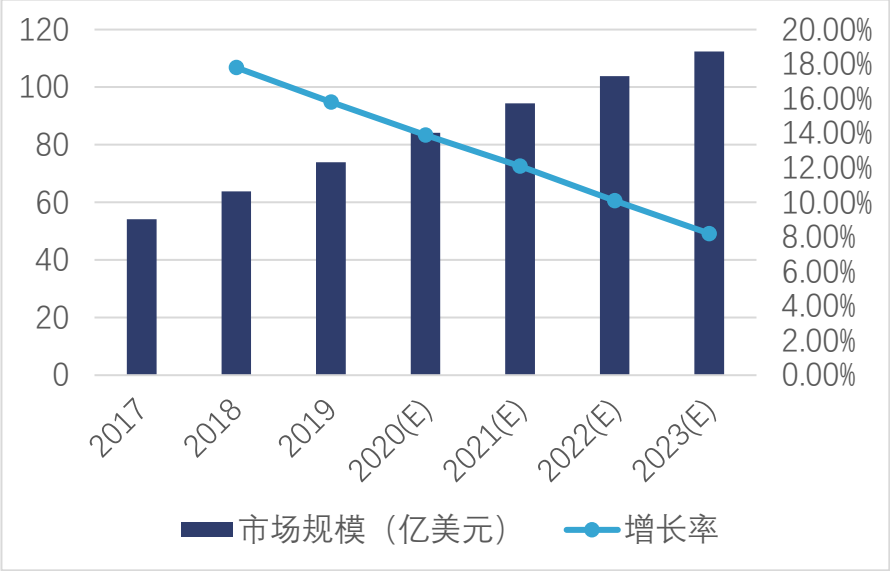


数据来源：中国信息通信研究院，2020 年 5 月

图 1 中国云计算市场规模及增速

云计算成攻击焦点，安全态势日益严峻。随着云计算的持续发展，云平台将承载越来越多的重要数据与用户关键业务，同时，云计算环境下多用户共享云基础架构，云平台一旦发生安全事件，将有海量用户受到影响，带来不可估量的经济损失，甚至影响社会的稳定生产。一方面，**云计算的重要性与价值导致其成为黑客攻击的重要目标。**黑客利用云计算提供商技术和管理上的漏洞，或利用云计算客户在云计算使用上的疏忽，对云平台进行破坏。据国家计算机网络应急技术处理协调中心统计，2019 年，我国云平台网络安全事件或威胁情况进一步加剧，DDoS 攻击次数占境内目标被攻击次数的 74.0%、被植入后门链接数量占境内全部被植入后门链接数量的 86.3%、被篡改网页数量占境内被篡改网页数量的 87.9%。另一方面，**云计算提供商或云计算客户造成的安全事件时有发生。**安全事件主要包括大规模服务中断、数据泄露和数据丢失。云计算客户对云服务的错误配置或使用，容易导致数据泄露或丢失的发生。2019 年，Attunity（以色列公司，为大

约 2000 名客户提供数据管理、仓储和复制服务，很多客户为《财富》100 强企业）因其将三个 AWS S3 桶的访问权限设置为公开，导致至少 1T 数据的泄露，其中包括电子邮件、系统密码、项目规格等重要数据。对于云计算提供商来说，内部人员误操作、恶意行为、软硬件故障、基础设施故障等都可能导致三类安全事件的发生。

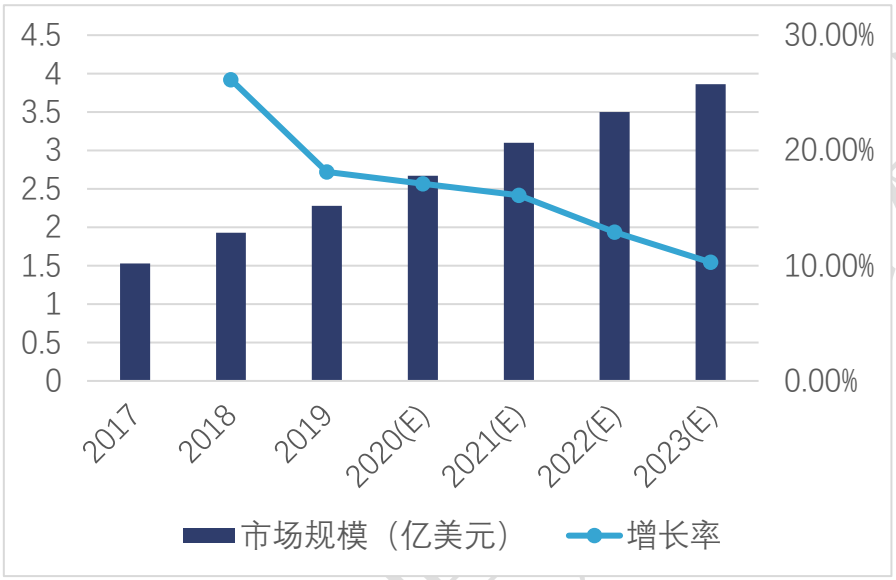


数据来源：Gartner

图 2 全球云服务安全市场规模

云计算安全受重视，云服务安全市场将持续发展。受云计算安全态势的影响，云计算客户对云上的安全需求越发迫切，关注点从“上云”逐步发展为“安全上云”，安全成为客户选择云计算的重要考量因素。据中国信通院《中国公有云发展调查报告（2020 年）》显示，42.4%的企业在选择云服务时会考虑服务安全性，安全性成为企业选择公有云服务商的第三大考量因素，较 2018 年提升一位。另一方面，云计算提供商增加安全投入，不断提升云平台安全性的同时，向客户提供丰富的安全产品，促进云计算客户云上数据与业务的安全防护水

平发展。据 Gartner 统计，2020 年全球云服务安全市场规模预计可达 84.18 亿美元，增速 13.9%。中国云服务安全市场规模预计可达 2.67 亿美元，增速 17.11%，2018-2023 年间，增长速率均高于全球水平，发展空间极大。



数据来源：Gartner

图 3 中国云服务安全市场规模

（二）安全责任共担，保障云计算全方位安全

1. 安全责任的承担与落实影响云计算整体安全

云平台作为一种持续运营、动态变化的基础设施，涉及的**关键点复杂**，既包括数据中心、计算、存储、网络、应用、数据、人员等实体要素，也包括研发、运维、运营、使用等关键环节。同时，云平台面临的**威胁多样**，威胁利用关键点的脆弱性对云平台进行破坏，环境灾害、黑客行为、技术故障等威胁都将带来不程度的损失和危害。

在实际运营中，云计算的**服务产业链纵深延长**，服务关系存在多

级嵌套的情况。云计算提供商向云计算用户交付云服务，云计算用户利用云服务，可以向其用户交付其它应用服务，而这些应用服务又可以形成下一级的“提供者-用户”关系。**威胁所带来的风险也将依附服务产业链不断渗透**，影响范围和危害程度不断扩大。如图 4 所示，不仅云计算提供者与用户风险依存，看似独立、毫无关系的用户之间也会产生影响，一个小的安全问题，可能导致云平台的大范围安全事故，牵一发而动全身。

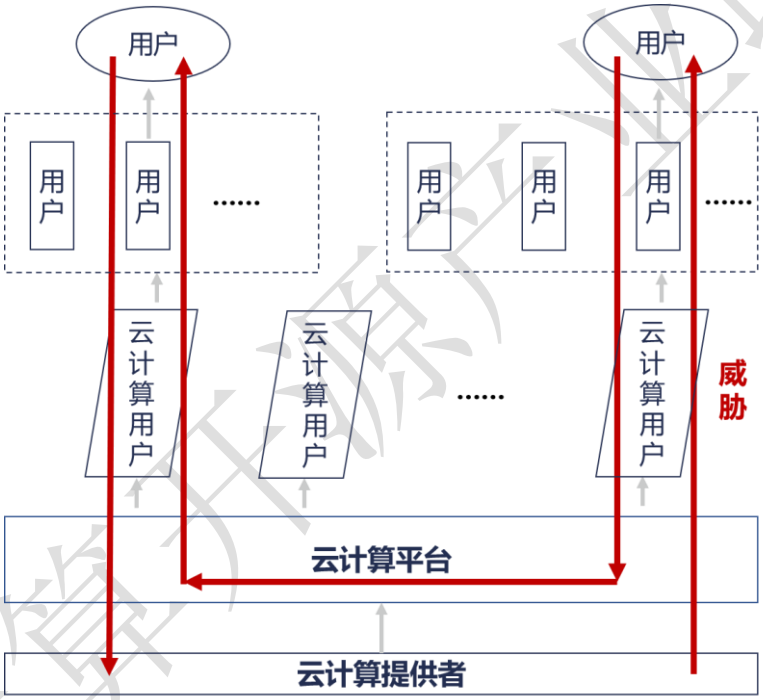


图 4 云计算威胁渗透示意图

为保证云平台安全稳定运行，必须**全面识别、切实承担云计算相关的所有安全责任**。在**事前**，深入落实云计算安全责任，可以最大可能的规避安全事件的发生；**事中**，根据安全事件属性，判断安全责任落实薄弱环节，可以迅速的响应和处置安全事件，尽可能阻断损失的扩大；**事后**，客观的事件定责，是通过法律、经济等手段降低安全事

件损失的前提和核心。事件定责的成熟，将促进云计算保险的发展，完善云保险赔偿机制，丰富云保险覆盖场景。云计算企业或云客户通过为云计算投保，可以有利推动事故发生后的赔偿力度和执行程度，保障云客户的事后权益，分担了云计算企业的赔偿损失。

2.责任共担已成共识，企业组织纷纷推出云计算安全责任共担模型

云计算安全体系复杂,所涉责任繁多,云计算提供商权利有限制,安全责任必然无法由提供商全部承担,云计算提供商与云计算客户进行责任分担的模式成为行业共识和最佳方案。

各大云服务商建立责任共担模型。亚马逊、微软、阿里、腾讯、华为等国内外知名云服务均推出了自己的云计算安全责任共担模型，各模型融合了云服务商业务场景和特色，均有差异，但大致可以分为以 AWS 和 Azure 为代表的两类模型。

1）**亚马逊 AWS 模型，在云服务商和云客户间划清责任分界线**。AWS 将其提供的云服务分为三大类，包括 EC2、EBS、VPC 在内的基础设施服务，RDS、EMR 为代表的容器服务，以及 S3、DynamoDB、SQS 等抽象服务。针对不同的云服务，AWS 分别建立了对应的责任共担模型（图 5-7 所示），识别不同云服务场景下云服务商和云客户应承担的责任，明确两者间的责任分界，分界线以下由云服商负责，以上由云客户负责。

图 5 AWS 基础设施服务责任共担模型

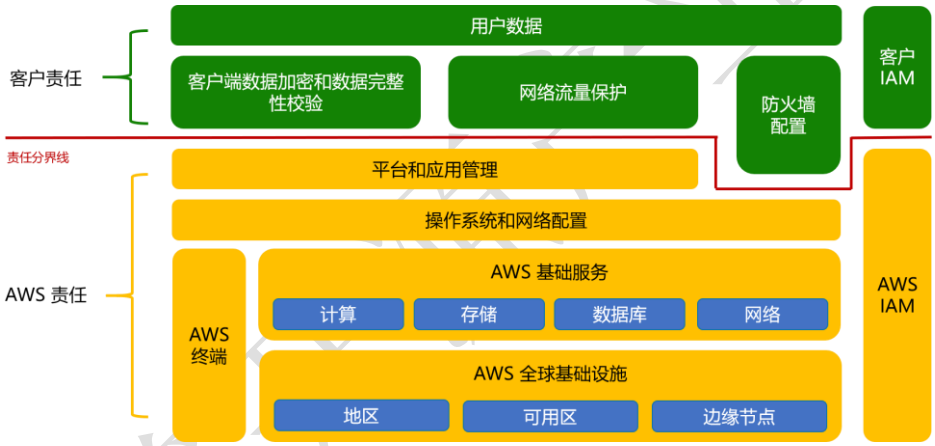


图 6 AWS 容器服务责任共担模型

图 7 AWS 抽象服务责任共担模型

2）**微软 Azure 模型，中间责任带由云服务商和云客户共同分担。**微软 Azure 将云计算安全责任从底层物理数据中心到上层数据分为十类，对 IaaS、PaaS 和 SaaS 三种场景下十大类的安全责任进行划分，底层安全责任一般由云服务商承担，上层安全责任则由云客户负责，除两者独立承担的责任外，中间部分安全责任由两者共同承担。

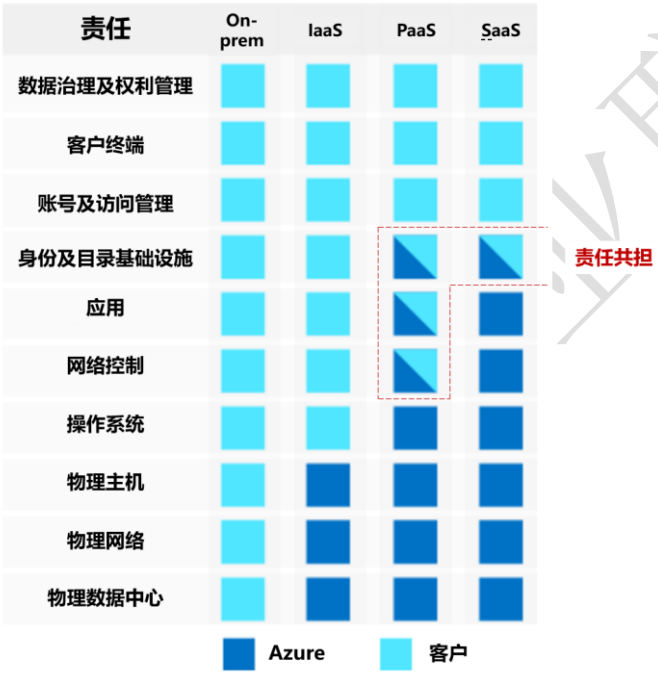


图 8 Azure 责任共担模型

相关标准与指南不断成熟。云计算安全责任共担受到越来越多的关注与重视，标准组织、联盟纷纷从行业角度出发，对云计算场景下的责任划分提出规范或建议。

1）**《GB/T 22239-2019 信息安全技术 网络等级保护基本要求》**中规范了不同云计算服务模式下云服务商和云服务客户的安全管理责任，如图 9 所示。在不同的服务模式中，**云服务商和云服务客户对计算资源拥有不同的控制范围，控制范围则决定了安全责任的边界。**

在基础设施即服务模式下，云计算平台/系统由设施、硬件、资源抽象控制层组成；在平台即服务模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在软件即服务模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件。

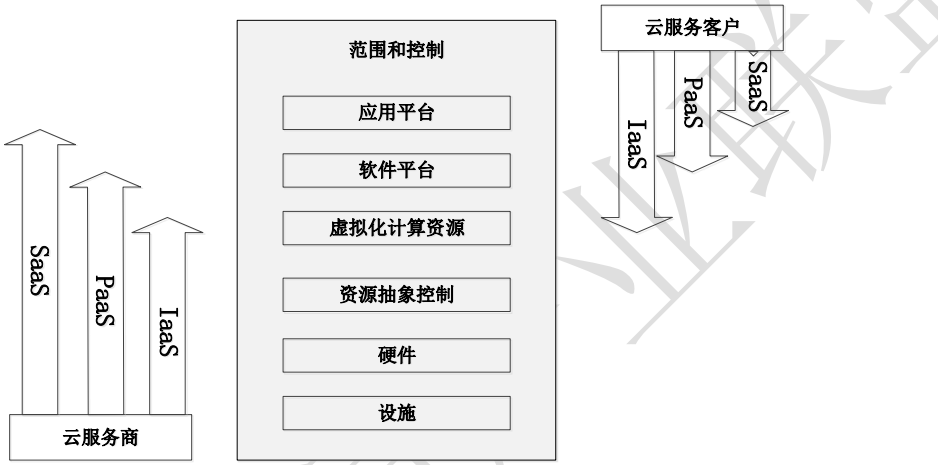


图 9　云计算服务模式与控制范围的关系

2）《GB/T 31167-2014 信息安全技术 云计算服务安全指南》规范了云服务商、客户和第三方评估机构三大云计算服务安全管理主要角色的责任。在该标准的新修订版本中，**进一步引入云服务安全提供商角色，同时给出了政务云中的责任划分实践与参考**，如图 10 所示。标准指出，如果部分安全措施需要由云服务安全提供商来实施，相关的责任也可以由云服务安全提供商承担。云服务商和客户需要保证各个角色承担责任的总和能够覆盖到系统的全部安全要素，避免责任无人承担或责任承担不明确的情况。

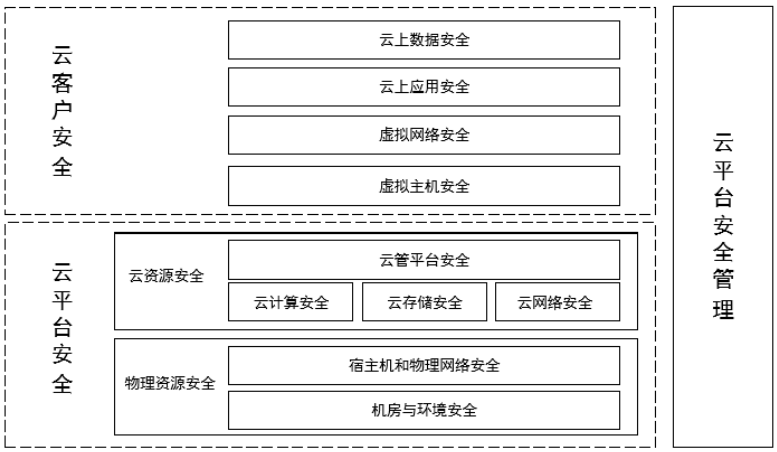


图 10　云服务商与云客户责任划分边界

3）**云安全联盟（CSA）《云计算关键领域安全指南》**中指出，安全责任与角色对架构堆栈的控制程度相对应，如图 11 所示。SaaS 中云服务提供商负责几乎所有的安全性，因为云消费者只能访问和管理其使用的应用程序，并且无法更改应用程序。PaaS 中云服务提供商负责平台的安全性，而消费者负责他们在平台上所部署的应用，包括所有安全配置，因此两者职责几乎是平均分配。IaaS 类似 PaaS，云服务提供商负责基本的安全，而云消费者负责他们建立在该基础设施上的其它安全，不同于 PaaS，IaaS 的消费者承担更多的责任。

图 11　CSA 安全责任与云服务模式关系

（三）云计算安全责任共担应用与发展有痛点

云计算安全责任共担已成行业共识，各大云服务商均推出了自己的共担模型，标准、指南也对责任划分提出了规范和建议，但在云服

务的实际运营与使用中，责任共担的应用与发展仍存在诸多痛点:

各云计算安全责任共担模型有差异，云客户应用存疑惑。一方面，各共担模型安全责任分类不尽相同，同一分类下覆盖的具体安全责任范围又可能有差异，不同模型对某一责任的解释和定义也存在不一致的情况。另一方面，不同云服务商业务模式不同，在责任划分时，云服务商与云客户间的责任界限也将不同，一些服务商承担的责任多些，一些服务商承担的责任少些。这些差异可能会影响云客户对责任共担模式的理解，甚至造成误解。

云客户责任共担意识薄弱，责任承担能力不足。部分云客户对上云后的安全责任问题认识不够清晰，认为上云后安全责任全部由服务商承担，根据中国信通院《中国私有云发展调查报告》调查显示，仅有 35.4%的企业表示安全责任应由私有云服务商和企业共同承担。同时，一些云客户对云上业务的安全管理体系建设不足，存在安全投入不够、运维人员安全意识不到位、安全防护水平低等问题，无法切实承担自己应承担的安全责任。

云客户消极承担责任或知法犯法，云服务商巡查存在技术挑战。部分云客户虽然能够意识到上云后应承担相应安全责任，但在承担责任时采取消极应对的态度，如不对云上业务进行有效的网络安全防护、使用虚假材料进行实名认证等。同时，云计算作为一种可靠的、可扩展的全球性基础设施，受到黑灰产的关注，恶意客户利用云资源，进行多种违法违规活动或云资源滥用行为，如经营涉黄涉毒涉赌等违法应用程序、对外发起 DDoS 等网络攻击、数字货币挖矿、暴力破解、

垃圾邮件和钓鱼活动、刷单、恶意 VPN 代理、云养号、恶意刷域名备案等。云服务商作为云平台的运营者，考虑监管要求以及自身业务安全稳定发展的需求，承担对上述行为巡查和处置的责任，即使大部分云服务商引入人工智能技术，结合人工措施，结果仍有缺失，全面审查依然是技术难题。

案件纠纷时有发生，实际场景复杂难定责。云服务的运营应满足国家法律法规的监管要求，包括《网络安全法》、《著作权法》、《电子商务法》等法律，《电信条例》、《计算机信息网络国际联网安全保护管理办法》等条例规章。部分法律法规通用性强，结合多种信息技术场景，提出的要求较为粗放。而云计算存在服务模式多样、服务关系多级嵌套等情况，在实际的案件纠纷中，责任的划分与确定面临诸多难题，如法律适用，履行责任的判定等。2019 年，国内首例云服务器侵权案二审改判，北京知识产权法院驳回一审原告的诉讼请求，判定阿里云不承担法律责任。该案争议焦点在于案件的法律适用、合格通知的判定标准、云服务商是否构成共同侵权及应否承担民事责任等问题，涉及云上用户数据与隐私安全，受到广泛关注。北京市知识产权法院认为，《信息网络传播权保护条例》不适用于本案，而应依据《侵权责任法》进行判决。

二、云计算安全责任共担模型框架

为建立更加精细可落地、普遍适用于云计算行业的安全责任共担模型，提升云服务客户责任共担意识与承担水平，自 2019 年起，中国信通院、云计算开源产业联盟牵头，联合数十家云服务商，开展了

云计算安全责任共担的相关研究，制定了《云计算安全责任共担模型》行业标准。基于以往研究成果，编写此白皮书，将云计算安全责任共担模型成果进行分享，以供行业相关企业、人员参考。

（一）模型应用场景

云计算分为公有云、私有云、社区云、混合云等部署模式。私有云、社区云和混合云模式具体应用情况与云服务客户需求较为相关，不同客户的云平台差异较大，公有云由云服务商统一交付，通用性强，不同公有云间运营模式差异不大。本白皮书将建立**公有云模式下安全责任共担模型**，白皮书中对云计算安全责任的分类和识别，也可供其它云计算部署模式参考。

根据服务模式的不同，本白皮书将按照以下三种服务模式进行责任划分：

基础设施即服务（IaaS）。云服务商为云服务客户提供计算、存储、网络等基础资源，云服务客户基于这些资源部署需要的中间件、应用软件等。典型的 IaaS 服务包括云服务器、云硬盘等。

平台即服务（PaaS）。云服务商为云服务客户提供封装后的 IT 能力，包括软件开发环境、运行平台等，云服务客户基于此来部署、管理和运营自己的应用。典型的 PaaS 服务包括消息中间件、机器学习平台等。

软件即服务（SaaS）。云服务商为云服务客户直接提供应用服务，云服务客户可通过网络访问和使用这些应用。典型的 SaaS 服务包括邮箱、在线会议、办公软件等。

（二）云计算安全责任主体

云服务在实际运营中存在服务关系多级嵌套的情况，如图 4 所示。本白皮书共担模型以云平台为核心，研究与云服务直接相关的**云服务提供者和云服务客户的责任划分**。云服务合作者[1]，以及云服务客户基于云服务对外提供应用而获得的用户，不在模型范围内。

云服务提供者。指提供云服务的参与方，本白皮书模型中为公有云云服务商，提供 IaaS、PaaS、SaaS 中的一种或多种云服务。对于仅提供 PaaS 或 SaaS 服务的云服务提供者，其基础资源可以是 IaaS/PaaS 云服务，也可以是物理机等非云服务资源，但后文将统一表述为 IaaS、PaaS。

云服务客户。指为使用云服务而处于一定业务关系中的参与方。业务关系不一定包含经济条款。包括企事业客户和个人客户。

（三）云计算安全责任分类

本白皮书将云计算安全责任分为七大类：1）**物理基础设施**，指运营云计算服务的数据中心安全和云计算平台基础架构安全。2）**资源抽象和管理**，指计算、存储、网络、数据库等资源的虚拟化安全，以及云主机、云存储、云网络和云数据库等云服务产品的安全管理。3）**操作系统**，指云主机的操作系统安全。4）**网络控制**，指云服务间的，或云服务与外部的网络通信的安全控制。5）**应用**，指云计算环

[1] GB/T 32400-2015 信息技术 云计算 概览与词汇
云服务合作者：支撑或协助云服务提供者和/或云服务客户活动的参与方。根据不同的服务合作者类型，以及他们与云服务提供者和云服务客户的关系，有不同的云服务合作者活动。云服务合作者包括云审计者、云服务代理等。

境下的应用系统的安全管理。在 IaaS、PaaS 模式中，应用是云服务客户自行部署在云环境上的软件或服务。在 SaaS 模式中，应用是云服务提供者为云服务客户提供的软件类云服务。6）**数据**，指云计算相关的云服务客户数据、云服务衍生数据、云服务提供者数据[2]和云服务客户个人隐私信息的安全管理。7）**身份识别和访问管理（IAM）**，指对云计算相关资源和数据的身份识别和访问管理，涉及云控制台、云服务和云服务提供者内部系统平台的身份识别和访问管理。内部系统平台指云服务提供者内部与云服务相关的平台系统，如代码托管系统、运维系统等。

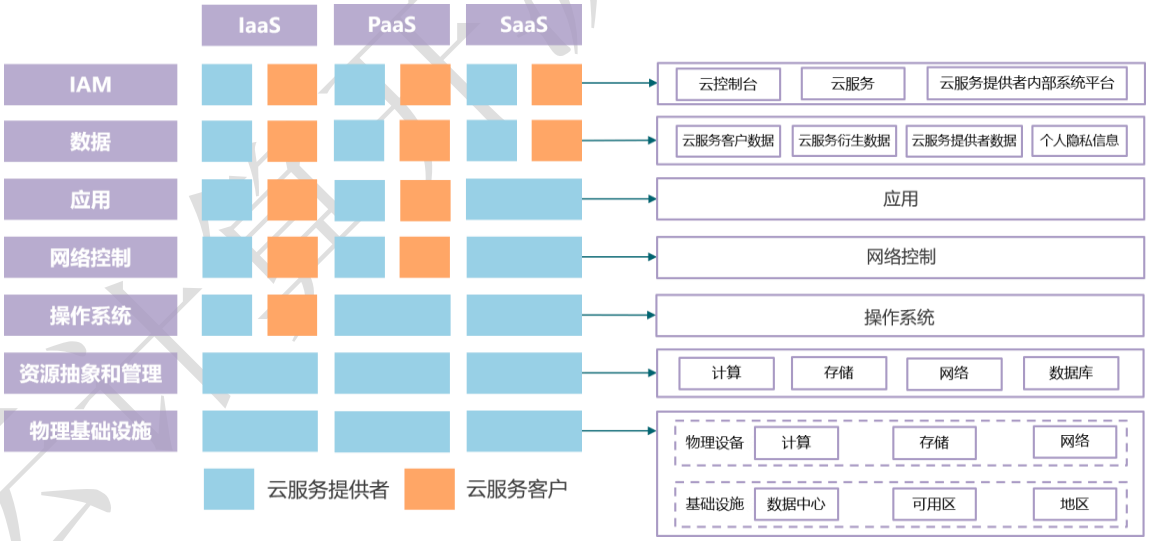


图 12　云计算安全责任共担模型

[2] GB/T 32400-2015 信息技术 云计算 概览与词汇

云服务客户数据：基于法律或其他方面的原因，由云服务客户所控制的一类数据对象。这些数据对象包括输入到云服务的数据，或云服务客户通过已发布的云服务接口执行云服务所产生的数据。

注1：法律原因包括版权等。

注 2：云服务可包含或操作非云服务客户数据。非云服务客户数据可包括云服务提供者可访问的数据，其他来源的数据，或公开可获取的数据。但是，按照一般的版权原则，云服务客户通过使用云服务在非云服务客户数据上所产生的数据可能是云服务客户数据，除非在云服务协议中有相反的条款规定。

云服务衍生数据：由云服务客户和云服务交互所产生的云服务提供者控制的一类数据对象。

注：云服务衍生数据包括日志数据，授权用户数以及授权用户的身份，配置数据和定制化数据。其中，日志数据记录了谁在什么时间使用了服务，使用了什么功能和数据等。配置数据和定制化数据用于云服务的配置和定制化。

云服务提供者数据：由云服务提供者控制，与云服务运营相关的一类数据对象。

注：云服务提供者数据包括但不限于资源的配置和使用信息、云服务特定的虚拟机信息、存储和网络资源配置信息、数据中心的整体配置和使用信息、物理和虚拟机资源的故障率和运营成本等。

三、云计算安全责任识别与划分

（一）云计算安全责任识别

1.物理基础设施安全责任识别

云计算场景下物理基础设施安全责任主要包括：1）**数据中心环境安全**，指选址、建筑结构、电力、消防、温湿度等数据中心环境的安全责任。2）**数据中心运营安全**，指访问控制与监控、安全审计与检查等数据中心运营的安全责任。3）**容灾**，指跨机房的、跨可用区的或跨地区的数据中心容灾责任。4）**物理设备生命周期安全**，指计算、存储、网络等云计算相关物理设备从采购、使用、维护到销毁全生命周期的安全责任。5）**基础架构安全**，指计算、存储、网络等云计算底层基础架构的安全责任。

2.资源抽象和管理安全责任识别

云计算场景下资源抽象和管理安全责任主要包括：1）**安全隔离**，指通过计算虚拟化、存储虚拟化、网络虚拟化等技术保障云计算环境下的多租户隔离以及虚拟资源与虚拟化平台之间的隔离。具体分为：**计算隔离**，指对管理系统与虚拟机/容器以及虚拟机/容器之间进行计算隔离，在未授权的情况下，无法通过虚拟机访问物理主机和其他虚拟机/容器的系统资源。**存储隔离**，指虚拟机只能访问分配给它的物理磁盘空间。**网络隔离**，指虚拟网络之间互相隔离，以及虚拟网络和物理网络间的隔离。**数据库隔离**，指不同云服务客户的数据库互相隔离。2）**虚拟化平台安全**，指虚拟化技术安全，以及确保虚拟化平台

免受外部攻击或内部滥用的责任。3）**云控制台安全**，指云控制台设计、开发、测试、部署和运维的全生命周期安全责任。4）**云服务API安全**，指云服务API设计、开发、测试、部署和运维的全生命周期安全责任。5）**云服务产品安全**，指云服务产品设计、开发、测试、部署和运维的全生命周期安全责任。

3.操作系统安全责任识别

云计算场景下操作系统安全责任主要包括：1）**镜像安全**。在IaaS模式中，镜像包括公共镜像（公共镜像是由云服务提供者制作并发布的镜像）、服务市场镜像（服务市场镜像由第三方服务提供者提供）和其它来源镜像（其它来源镜像由云服务客户自行制作，或云服务客户使用的其它来源共享的镜像），在PaaS/SaaS模式中，镜像指云服务提供者主机中所使用的镜像。安全责任具体包括：**镜像制作安全**，指镜像制作过程中的安全责任，镜像应由专业团队制作，已知的安全漏洞应在制作时被修复。**镜像版本管理**，指镜像版本计划，周期性的或在有重大安全漏洞被披露时对镜像进行更新或修复。**镜像校验与审核**，指镜像在发布或使用前应进行安全校验和内容审核，校验与审核通过后才可发布或使用。**镜像漏洞管理**，指镜像发布后或使用时的漏洞管理，包括漏洞信息的获取与告知，漏洞的修复等。2）**云主机安全监测**，指在云主机内部部署安全产品或工具，对云主机的入侵行为进行监测和处置，以避免云主机主动或被动向外部发起恶意攻击。3）**云主机备份**，指通过镜像、快照等方式对云主机进行备份。

4. 网络控制安全责任识别

云计算场景下网络控制安全责任主要包括：1）**设置安全组**，指为云服务设置合理的安全组，以控制云服务间的，或云服务与外部的网络通信。2）**网络类型选择**，指为云服务选择合适的网络类型，如专有网络等，以实现云服务的访问。3）**IP黑白名单配置**，指为云服务配置合理的IP黑名单、白名单，以限制或开放不同IP对云服务的访问。

5. 应用安全责任识别

云计算场景下应用安全责任主要包括：1）**应用生命周期安全**，指应用从设计、开发、测试到发布全生命周期安全责任。2）**应用安全管理**，指应用的漏洞管理和安全防护。应周期性对应用进行漏洞扫描和修复，部署面向应用的安全防护工具，对入侵行为进行监控、告警和处置。3）**应用内容安全**，指应用中运营的内容应符合相关法律法规规定，不应存在涉黄、涉毒等违规内容。4）**网站域名备案**，指网站的域名应按国家相关法律法规规定完成备案。

6. 数据安全责任识别

云计算场景下数据安全责任主要包括：1）**数据存储安全**，指数据存储的持久性、私密性、完整性和可用性。**数据持久性**指数据存储不丢失。**数据私密性**包括数据隔离安全性和数据存储保密性。数据存储保密性指采用加密技术或其他保护措施实现数据的存储保密性。数据隔离安全性仅适用于云服务客户数据，指同一资源池云服务客户数

据互不可见。**数据完整性**指数据完整性不被破坏的概率。**数据可用性**指对数据的各项操作（如上传、修改、删除、查找等）成功的概率。2）**数据传输安全**，指采用合理的技术和手段保障数据传输过程中的私密性和完整性。3）**数据访问安全**，指数据的访问和使用均在授权下，以及使用有效的数据保护手段，确保数据不被窃取。4）**数据迁移安全**，指数据在云平台的迁入迁出安全。5）**数据销毁安全**，指数据及其副本能够如期望的彻底销毁，以及使用有效的手段防止数据及其副本的误销毁。6）**数据安全管理**，指数据的分类分级管理机制。7）**数据安全合规**，指数据的收集、存储、使用、处理等满足相关法律法规的要求。8）**安全审查和取证**，指在配合政府监管部门开展安全审查或调查取证时，应采取一定的安全措施，具体包括：a）应建立相关的管理制度，对每一种数据披露场景建立内部审核机制。b）要求政府监管部门提供证件、法律函件等材料，以识别政府监管部门安全审查或调查取证的要求是否真实可信。c）在允许的条件下，将配合安全审查或调查取证行为告知数据相关方。

7.身份识别和访问管理安全责任识别

云计算场景下IAM安全责任主要包括：1)**密码安全策略**，指密码创建、修改时，有复杂度、更换周期等安全策略。2)**身份认证凭证管理**，指妥善保管身份认证凭证，包括登陆密码、访问密钥等，以避免身份认证凭证被盗用、冒用。3)**身份鉴别信息安全**，指身份鉴别信息以加密的方式传输和存储。4)**行为日志功能**，指对账号使用记录、操

作记录等内容进行记录、分析和审计。5)**用户管理和权限管理**，指对用户及其具备的权限进行管理。

对于云服务，除上述安全责任外，还应包括**实名备案**安全责任，既在购买和使用云服务时，应按国家法律法规规定，完成实名备案。

（二）云计算安全责任划分

在上一节识别的云计算安全责任中，一些安全责任必须由云服务提供者承担，一些安全责任必须由云服务客户承担，其余安全责任既可以由云服务提供者承担，也可以由云服务客户承担。在云服务的实际运营中，往往由两者协商后确定。在后续章节中，将对 IaaS、PaaS 和 SaaS 模式下必须由云服务提供者或云服务客户承担的责任进行划分，可协商的安全责任将给出多种划分示例以供参考，云服务提供者和云服务客户可以结合实际场景和需求进行调整和适配。

1. IaaS 模式

IaaS模式下，必须由云服务提供者或云服务客户承担的责任划分如表1所示，可协商安全责任的划分参考如表2所示。

表 1 IaaS 模式下云计算安全责任划分

安全责任		云服务提供者	云服务客户
物理基础设施安全	数据中心环境安全	✓ 数据中心可以是云服务提供者自建或向第三方租赁，无论是自建还是租赁，云服务提供者均应承担数据中心的环境安全责任	×

	数据中心运营安全		✓ 数据中心的运营可以由云服务提供者或第三方企业进行，安全运营责任均由云服务提供者承担	×
	容灾		✓ 为保障云服务和云服务客户数据的可用性，容灾可以作为基础服务或增值服务提供给云服务客户。但无论云服务客户是否使用容灾服务，云服务提供者都应保证云服务和云服务客户数据可用性达到SLA中的承诺值，因容灾不足而未达到SLA的，由云服务提供者承担相应责任	×
	物理设备生命周期安全		✓	×
	基础架构安全		✓	×
资源抽象和管理安全	安全隔离		✓	×
	虚拟化平台安全			
	云控制台安全			
	云服务API安全			
	云服务产品安全			
操作系统安全	公共镜像安全	镜像制作安全	✓	×
		镜像版本管理	✓ 除第（一）节中3. 1）b）提到的责任外，应确保云服务客户在购买云主机时获取的均是最新版公共镜像	×
		镜像校验与审核	✓	×
		镜像漏洞管理	参考表2	
	服务市场镜像安全	镜像制作安全	✓ 服务市场镜像由第三方服务提供者制作，但云服务提供者仍需承担如下责任： ——在云服务客户使用服务市场镜像前，告知云服务客户该镜像由第三方服务提供者制作，安全责任最终	×
		镜像版本管理		

			共担方为第三方服务提供者，应留意使用过程中面临的风险。 ——应对第三方服务提供者进行资质审查，确保发生安全事件后，云服务客户能够与第三方服务提供者取得联系。因云服务提供者审核不当导致云服务客户无法与第三方服务提供者取得联系的，安全责任由云服务提供者承担。	
		镜像校验与审核	✓ 云服务提供者应尽到注意义务，通过技术、管理等手段，对发布的服务市场镜像进行校验与审核，避免发布的镜像存在病毒等安全问题	×
		镜像漏洞管理	✓ 承担将重大安全漏洞信息告知已经使用该镜像的云服务客户的责任	✓ 使用服务市场镜像创建云主机后，应时刻关注云服务提供者和第三方企业机构发布的漏洞公告，及时对镜像存在的安全风险进行处置
	其它来源镜像安全	镜像制作安全 镜像版本管理 镜像校验与审核 镜像漏洞管理	×	✓
	云主机安全监测		参考表2	
	云主机备份		参考表2	
网络控制安全	设置安全组		✓ 承担为云服务客户提供安全组功能的责任	✓
	网络类型选择		✓ 承担为云服务客户提供多种网络类型的责任	✓
	IP黑白名单配置		✓	✓

			承担为云服务客户提供IP黑白名单配置的责任	
应用安全	应用生命周期安全		×	✓
	应用安全管理		×	✓
	应用内容安全		✓ 承担对云服务客户公开的应用进行内容安全审核的责任，应具备完备的审查流程、预警方案和配合机制。能够配合监管部门或核实用户举报，针对违法违规的应用，通知云服务客户整改，或将其封禁和下线。	✓
	网站域名备案		✓ 承担云服务客户网站进行域名备案审核的责任，针对未按规定备案的网站，有责任将其封禁和下线	✓
数据安全	云服务客户数据安全	数据存储安全	✓	×
		数据传输安全	✓ 承担为云服务客户提供保障数据传输安全的技术和手段的责任	✓
		数据访问安全	✓ 承担仅在云服务客户授权下才访问数据的责任	×
		数据迁移安全	参考表2	
		数据销毁安全	✓ 为避免云服务客户误删或未及时续订云服务，云服务提供者可以对云服务客户数据保留一定时间，时间到期后将云服务客户数据彻底删除，但该行为应提前告知云服务客户	×
		数据安全管理	×	✓
		安全审查和取证	✓	×
	云服务衍	数据存储安全		
		数据传输安全		

	生数据安全	数据访问安全	✓	×
		数据迁移安全		
		数据销毁安全		
		数据安全管理		
		安全审查和取证		
	云服务提供者数据安全	数据存储安全	✓	×
		数据传输安全		
		数据访问安全		
		数据迁移安全		
		数据销毁安全		
		数据安全管理		
		安全审查和取证		
	个人隐私信息安全	数据存储安全	✓ 除第（一）节中6.提到的责任外，个人隐私信息的收集、存储、处理等详细信息应通过隐私声明等方式披露给云服务客户	×
		数据传输安全		
		数据访问安全		
		数据迁移安全		
		数据销毁安全		
		数据安全管理		
		安全审查和取证		
IAM 安全	云控制台	密码安全策略	✓	×
		身份认证凭证管理	×	✓
		身份鉴别信息安全	✓	×
		行为日志功能	参考表2	
		用户管理和权限管理	✓ 承担为云服务客户提供用户管理和权限管理功能的责任	✓
	云服务	密码安全策略	参考表2	
		身份认证凭证管理	×	✓
		身份鉴别信息安全	✓	×
		行为日志功能	参考表2	
		用户管理和权限管理	✓ 承担为云服务客户提供用户管理和权限管理功能的责任	✓
		实名备案	✓	✓

			承担云服务客户实名备案审核的责任，在云服务客户备案前为其提供云服务的，安全责任由云服务提供者承担	承担完成实名备案的责任，因实名备案材料造假，云服务提供者依法停止对其提供云服务的，责任由云服务客户自行承担
	云服务提供者内部平台系统	密码安全策略	✓	×
		身份认证凭证管理		
		身份鉴别信息安全		
		行为日志功能		
		用户管理和权限管理		

表 2 IaaS 模式下云计算安全责任协商划分参考

序号	责任类别	责任划分参考模式		
		序号	云服务提供者	云服务客户
1	操作系统安全/公共镜像安全/镜像漏洞管理	a）	将安全漏洞信息告知已经使用该版本镜像的云服务客户	使用公共镜像创建云主机后，关注云服务提供者和第三方企业机构发布的漏洞公告，及时对镜像存在的安全风险进行处置
		b）	对云服务客户存在安全漏洞的镜像进行主动修复	——
2	操作系统安全/云主机安全监测	a）	——	在云主机内部署安全产品或工具，对云主机的入侵行为进行监测和处置
		b）	为云服务客户提供云主机安全产品	
		c）	在云服务客户购买云主机时，默认内置安全监测功能	——
3	操作系统安全/云主机备份	a）	提供云主机备份功能	合理使用云主机备份功能
		b）	在云服务客户购买云主机时，默认对云主机开启备份	——
4	数据安全/云服务客户数据安全/数据迁移安全	a）	——	自行进行数据迁移
		b）	提供数据迁移服务	——
5	IAM 安全/云控制台安全/行为日志功能	a）	提供行为日志功能	对行为日志进行分析和审计
		b）	提供行为日志功能、日志分析和审计服务	——

6	IAM 安全/云服务安全/密码安全策略	a）	——	设置合理的密码安全策略
		b）	配置合理的密码安全策略要求，如在云主机镜像制作时配置密码安全策略要求	——
7	IAM 安全/云服务安全/行为日志功能	a）	提供行为日志功能	对行为日志进行分析和审计
		b）	提供行为日志功能、日志分析和审计服务	——

2. PaaS 模式

PaaS 模式下，云服务提供者和云服务客户安全责任划分如表 3 所示。

表 3 PaaS 模式下云计算安全责任划分

安全责任			云服务提供者	云服务客户
物理基础设施安全	同IaaS模式			
资源抽象和管理安全	同IaaS模式			
操作系统安全	镜像安全	镜像制作安全	✓	×
		镜像版本管理	✓	×
		镜像校验与审核	✓	×
		镜像漏洞管理	✓	×
	云主机安全监测		✓	×
	云主机备份		✓	×
网络控制安全	同IaaS模式			
应用安全	同IaaS模式			
数据安全	同IaaS模式			
IAM安全	同IaaS模式			

3. SaaS 模式

SaaS模式下，必须由云服务提供者或云服务客户承担的责任划分如表4所示，可协商安全责任的划分参考如表5所示。

表 4 SaaS 模式下云计算安全责任划分

安全责任			云服务提供者	云服务客户
物理基础设施安全	同IaaS模式			
资源抽象和管理安全	同IaaS模式			
操作系统安全	同PaaS模式			
网络控制安全	设置安全组		✓	×
	网络类型选择		✓	×
	IP黑白名单配置		✓	×
应用安全	应用生命周期安全		✓	×
	应用安全管理		✓	×
	应用内容安全		✓	×
	网站域名备案		✓	×
数据安全	同IaaS模式			
IAM安全	云控制台/云服务	密码安全策略	✓	×
		身份认证凭证管理	×	✓
		身份鉴别信息安全	✓	×
		行为日志功能	参考表5	
		用户管理和权限管理	✓ 承担为云服务客户提供用户管理和权限管理功能的责任	✓
		实名备案	✓ 承担云服务客户实名备案审核的责任，在云服务客户备案前为其提供云服务的，安全责任由云服务提供者承担	✓ 承担完成实名备案的责任，因实名备案材料造假，云服务提供者依法停止对其提供云服务的，责任由云服务客户自行承担
	云服务提供者内部平台系统	同IaaS模式		

表 5 SaaS 模式下云计算安全责任协商划分参考

序号	责任类别	责任划分参考模式		
		序号	云服务提供者	云服务客户
1	IAM安全/云控制台安全/行为日志功能	a）	提供行为日志功能	对行为日志进行分析和审计
		b）	提供行为日志功能、日志分析和审计服务	——

四、云计算安全责任共担未来发展趋势展望

随着云计算作为新型基础设施建设的重要性不断凸显，云计算安全将更加关键，责任共担也将进入成熟发展与应用阶段，具体表现为：

行业发展成熟有序，责任主体共担意识得到提升。云服务商、云服务合作商、行业第三方组织等不断加强云计算责任共担模式的宣传，相关标准、研究成果日益丰富成熟，在此影响下，云服务客户的责任承担意识将不断提升。

监管政策日益健全，为事件追责提供依据。网络安全已经成为国家安全的重要组成部分，关系国家的稳定与发展。各政府相关部门积极推动网络安全相关法律法规的制定，不断完善面向云计算等新技术的法规政策，促进监管与时俱进，云平台责任的界定将更加清晰明确，有法有规可依。

技术水平持续发展，为云服务商全面巡查提供支持。目前，云服务商在合规巡查方面已经引入人工智能等新技术，但技术与实际场景的融合仍存在局限性，应用效果差强人意。随着技术的发展以及与应用场景的不断磨合，云服务商巡查能力将得到提高。

云计算安全生态不断丰富，云服务客户责任承担能力加强。近些年，我国云安全产品生态不断丰富。一方面，云计算厂商在强化自身

安全能力的同时，纷纷将自身安全能力产品化输出；另一方面，安全厂商积极布局云计算安全解决方案，将积累的丰富安全经验适配于云环境。安全产品的发展，极大程度的促进了云服务客户安全防护水平的提升，云服务客户能够更切实的承担相应安全责任。

附录 1：公有云安全责任承担优秀案例

注：排名不分先后，以首字母进行

（一）阿里云

1.物理基础设施安全责任承担

阿里云承担 IaaS、PaaS 和 SaaS 模式下物理基础设施的安全责任，具体包括:

数据中心环境安全。数据中心建设满足 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 T3+标准，在选址、抗震能力、耐火能力、防水能力、防静电能力、主机房负载、供电、灭火系统、报警系统、温湿度等方面均已通过“可信云云计算风险管理能力评估”。

数据中心运营安全。1）**访问控制**，仅向本数据中心运维人员授予长期访问权限，转岗或离职，立即清除权限。其他人员经各方主管审批后才能获取短期授权，每次出入需要出示证件并登记，且数据中心运维人员全程陪同。数据中心内各个区域拥有独立的门禁系统，重要区域采用指纹等双因素认证，特定区域采用铁笼进行物理隔离。2）**监控系统**，数据中心机房各区域和通道设有 7*24 小时视频监控系统。机房内具备完善的动力环境监控系统，能够对机房漏水、空调、配电等状况进行实时监控。3）**安全审计与检查**，监控和文档记录均会长期保存，且由专人定期复核。

容灾。在全球部署多数据中心，同地域支持多个可用区。不同云

服务具备不同的容灾能力，如云数据库支持同城容灾和异地容灾；对象存储默认采用多可用区机制，用户数据分散存放在同一地域的 3 个可用区，DDoS 防护、云防火墙等 SaaS 服务具备自动容灾能力。

物理设备生命周期安全。建立了数据中心物理设备从接收、保存、安置、维护、转移到重用或报备的全生命周期管理制度，在实际运营中严格按照相应制度开展工作。

基础架构安全。在计算架构、存储架构、网络架构方面均具备风险管理措施，已通过“可信云云计算风险管理能力评估”。

2. 资源抽象和管理安全责任承担

阿里云以飞天分布式云操作系统为核心，承担 IaaS、PaaS 和 SaaS 模式下资源抽象和管理的安全责任，具体包括:

安全隔离。1）**计算隔离**，关键隔离边界是管理系统与客户虚拟机以及客户虚拟机之间的隔离，由 Hypervisor 实现。阿里云平台使用的虚拟化环境，将用户实例作为独立虚拟机运行，并且通过使用物理处理器权限级别强制执行此隔离，确保用户虚拟机无法通过未授权的方式访问物理主机和其他用户虚拟机的系统资源。2）**存储隔离**，将基于虚拟机的计算与存储分离，使得计算和存储可以独立扩展，从而更容易提供多租户服务。在虚拟化层，Hypervisor 采用分离设备驱动模型实现 I/O 虚拟化。虚拟机所有 I/O 操作都会被 Hypervisor 截获处理，保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。3）**网络隔离**，一方面，把对外提供服务的云服务网络和支撑云服务的物理网络进行安全隔离，通过网络

ACL 确保云服务网络无法访问物理网络。另一方面，云服务网络中每个逻辑虚拟网络与所有其他虚拟网络隔离，确保部署中的网络流量数据不能被其它 ECS 虚拟机访问。

虚拟化平台安全。采用安全加固、逃逸检测、补丁热修复等安全技术保障阿里云虚拟化层安全。1）**安全加固**，使用轻量级和专门为云上场景开发的虚拟化管理程序，在设计之初即做到软硬件场景结合，专注于只支撑垂直的云上基础设施的硬件虚拟化，最大限度的从虚拟化管理程序中裁剪一些与云上设备无关的代码来降低攻击面，同时采用一系列可信计算技术来保障整个链路的安全，并对虚拟化管理程序和宿主机 OS/内核级别进行相应安全加固。2）**逃逸检测**，使用高级虚拟机布局算法以防止恶意用户的虚拟机运行在特定物理机上，且虚拟机无法主动探测自身所处的物理主机环境，同时在 Hypervisor 层面对虚拟机异常行为进行检测。3）**补丁热修复**，通过补丁热修复技术使得系统缺陷或者漏洞的修复过程不需要用户重启系统，从而不影响用户业务。

云控制台、云服务 API 和云服务产品安全。针对云计算制定了云产品安全生命周期（Secure Product Lifecycle，SPLC），目标是将安全融入到整个产品开发生命周期中。SPLC 在产品架构审核、开发、测试审核、应急响应的各个环节层层把关，每个节点都有完整的安全审核机制确保产品的安全性能够满足严苛的云上要求，从而有效地提高云产品的安全能力并降低安全风险。

3. 操作系统安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，阿里云对操作系统相关安全责任承担有所区别，具体包括：

公共镜像安全/（PaaS、SaaS）镜像安全。在 IaaS 模式下承担公共镜像安全，在 PaaS 和 SaaS 模式下承担底层主机所使用镜像的安全责任，具体表现为：支持 Linux 和 Windows 的多个发行版本，包括阿里云自研的 Aliyun Linux 2 版，能够保障镜像制作过程的安全，发布前对镜像进行校验与审核，对操作系统漏洞以及三方软件漏洞进行实时监测，以确保高危漏洞在第一时间得到修复。公共镜像集成了所有已知的高危漏洞补丁，防止云主机上线之后即处于高风险状态。在发现新的高危安全漏洞后，阿里云会迅速更新镜像并提供给客户。

服务市场镜像安全。在 IaaS 模式下承担部分服务市场镜像安全责任，具体表现为：通过三大方面保障云市场中镜像类产品的安全。1）**审核服务商资质**，确保提供镜像的服务商都有丰富的云服务器系统维护和环境配置经验，拥有专业的运维团队。2）**严格的制作流程**，要求所有镜像都基于包含云盾的操作系统制作，制作过程严格遵循《镜像产品安全审核标准》[3]进行，并通过专业的安全审核。3）**完善的保障机制**，镜像商须与每一个用户签订《镜像使用许可协议》，协议中规定了镜像商的义务与责任限制；镜像商都需要与阿里云签署《镜像内容承诺函》，保证镜像内容的安全性；镜像商入驻镜像市场都需要缴纳保证金，进一步约束镜像商，保护用户权益。

[3] 阿里云《镜像产品安全审核标准》
https://help.aliyun.com/document_detail/30500.html?spm=5176.10695662.1996646101.searchclickresult.24c7710fnNNSLf

主机安全监测。在 PaaS 和 SaaS 模式下，阿里云承担底层云主机的安全监测与处置。在 IaaS 模式下，阿里云公共基础镜像会默认添加云安全中心 Agent 软件以保障租户在实例启动时第一时间得到安全保障，用户在购买主机时可以主动选择不勾选该功能。阿里云容器支持提供镜像名称、标签、镜像大小、地域、最新发现时间及风险状态信息等安全状态相关信息，并提供 120,000+历史漏洞的识别能力和最新突发漏洞的检测能力。

云主机备份。在 PaaS 和 SaaS 模式下，阿里云负责底层云主机的备份。

4. 网络控制安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，阿里云对网络控制相关安全责任承担有所区别，具体包括:

安全组。在 IaaS、PaaS 模式下，阿里云向用户提供安全组功能，分为普通安全组和企业安全组。在 IaaS 模式下，用户可以基于安全组设置单台或多台云服务器的网络访问控制。在 PaaS 模式下，用户可以基于安全组对容器集群进行网络访问控制。在 SaaS 模式下，阿里云负责底层主机、容器资源的安全组设置。

网络类型选择。阿里云提供专有网络 VPC、NAT 网关等网络类型。在 IaaS、PaaS 模式下，多种云服务支持 VPC，如云服务器、云数据库、分析型数据库，用户可以通过合理使用 VPC 中路由器（VRouter）和交换机（VSwitch），通过网络访问控制列表 NACL 控制入站和出站流量，进而来实现云服务更安全的访问控制。在 SaaS

模式下，阿里云负责底层网络的选择和使用。

IP 黑白名单。在 IaaS、PaaS、SaaS 模式下，阿里云为多种云服务提供 IP 黑白名单功能以供用户使用，如云数据库、CDN、大数据计算服务、分析型数据库、负载均衡、对象存储，访问控制 RAM 等。

5. 应用安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，阿里云对应用安全相关安全责任承担有所区别，具体包括:

应用生命周期安全（SaaS）。详见云服务产品安全责任承担。

应用安全管理（SaaS）。通过安全监控及时发现平台自身应用被恶意攻击的安全事件，并在发现安全事件之后，触发云平台内部应急响应流程进行妥善处置，及时消除影响。应急响应是指阿里云对于内部监控发现的和外部上报的漏洞和安全事件做出应急处置。云平台侧通过日志收集和异常分析检测等手段发现可能的安全事件，并进行告警。外部上报的途径包括 ASRC 应急响应中心和阿里云先知漏洞平台、外部的开源三方组件对外通报的 CVE 漏洞信息和来自三方的威胁情报信息。

应用内容安全。基于深度学习技术及多年海量数据支撑，能够对应用内容风险进行实时自动化精准识别，同时建立了完善的违法违规内容处置与配合机制。在 IaaS、PaaS 模式下，应用为用户公开的应用，在 SaaS 模式下，应用为阿里云提供的 SaaS 服务。

网站域名备案。阿里云为用户提供免费的备案服务，自身积极履行 ICP 备案职责，同时对未履行备案职责的网站应用采取处置措施。

6. 数据安全责任承担

阿里云的云上数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期（数据采集、传输、处理、交换、存储、销毁）各环节进行数据安全管理管控，实现数据安全目标。在数据安全生命周期的每一个阶段，都有相应的安全管理需求以及安全技术保障。

利用云上数据安全体系，阿里云承担云服务衍生数据、云服务提供者数据和个人隐私信息的安全责任。对于个人隐私信息，阿里云保证客户对所有提供给阿里云的个人信息拥有所有权和控制权，积极响应国家监管部门对企业承担个人信息保护责任的号召，持续完善内部的个人信息管理和保护体系，设置专业的个人信息保护团队，在隐私权政策、用户权利保障等方面持续优化。

对于云服务客户数据，阿里云承担部分安全责任，具体包括:

1） 提供数据分类分级、传输加密、数据隔离、可控交换、存储加密等产品或能力（具体的使用和配置由用户负责）。

2） 在未获得用户授权的情况下不访问和使用用户数据。

3） 数据销毁安全。建立废弃介质上数据安全擦除流程;，云用户实例服务器释放后，其原有的磁盘和内存空间将会被可靠的进行数字清零以保障用户数据安全；云在终止为云服务客户提供服务时，会及时删除云服务客户数据资产或根据相关协议要求返还其数据资产。

7. 身份识别和访问管理安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，阿里云对身份识别和访问管理相关安全责任承担有所区别，具体包括:

云控制台IAM安全（IaaS/PaaS/SaaS）。1）密码安全策略。阿里云的账号密码规范、登录安全风控策略由阿里云统一管理。云账号下子用户（RAM 用户）的密码策略则可以由客户自己设定，如密码字符组合规范、重试登录次数、密码轮转周期等策略。2）身份鉴别信息。采用加密存储和加密传输的方式。3）ActionTrail 操作审计功能，以为用户提供统一的云资源操作日志管理。4）提供Resource Access Management（RAM）资源访问控制服务，以供用户进行身份管理与资源访问控制。5）多因素认证MFA。阿里云MFA是在用户名和密码（第一安全要素）基础之上，要求输入来自其MFA设备的可变验证码（第二安全要素），虚拟MFA设备是产生一个6位数字认证码的应用程序，它遵循基于时间的一次性密码 (TOTP) 标准(RFC 6238)。

云服务 IAM 安全（IaaS/PaaS）。1）密码安全策略。创建云主机等服务时，均有密码复杂度等要求。2）身份鉴别信息。采用加密存储和加密传输的方式。3）堡垒机。集中了运维身份鉴别、账号管控、系统操作审计等多种功能，专门针对云上 IT 运维人员、运维行为进行管理和控制。4）实名认证。对用户进行实名认证审核，完成实名认证的用户方提供云服务。5）SSH 密钥对。针对 ECS Linux 实例，阿里云通过 SSH 密钥对作为认证方，默认采用 RSA 2048 位的加密方式，相较于传统的用户名和密码认证方式，SSH 密钥对登录认证更为安全可靠。6）应用身份服务。阿里云应用身份服务 IDaaS（Alibaba

Cloud Identity as a Service，简称 IDaaS）是阿里云为企业用户提供的一套集中式身份、权限、应用管理服务，帮助用户整合部署在本地或云端的内部办公系统、业务系统及三方 SaaS 系统的所有身份，实现一个账号打通所有应用服务。

云服务提供者内部平台 IAM 安全（IaaS/PaaS/SaaS）。1）身份管理。阿里云针对正式员工、实习生、外包、合作伙伴等内部用户使用身份认证系统进行账号生命周期管理。所有用户按照“一人一账号”、“公私数据分离”原则进行账号分配和使用，账号一旦分配，不得共享账号并对账号做统一的登录管理、账号密码管理和访问控制。2）密码管理。所有用户集中下发密码策略，强制要求设置符合密码长度、复杂度要求的密码，并定期修改密码且不能与上一次密码相同。同时，阿里云支持账号密码登录、一次性口令登录、数字证书登录等多种认证登录方式。3）权限管理。阿里云根据业务需要合理分配权限，按照权限、角色、用户组、部门和用户进行权限统一管理，每个内部用户通过权限管理系统实行权限申请、使用和回收。阿里云为了加强内部系统权限使用管理，降低权限使用风险，根据风险将权限和角色设置为不同等级，并根据等级进行不同层级的申请审批机制，对于超过一定时间未使用的权限，系统则自动冻结权限；对于离职用户，系统自动冻结账号，回收权限；对于转岗用户，系统自动回收其权限。

（二）华为云

1. 物理基础设施安全责任承担

华为云承担 IaaS、PaaS 和 SaaS 模式下物理基础设施的安全责任，具体包括:

数据中心环境安全。制定了完善的物理和环境安全防护策略、规程和措施，满足机房建设要求及标准。 在选址、抗震能力、耐火能力、防水能力、防静电能力、主机房负载、供电、消防系统、报警系统、温湿度监控等方面均已通过“可信云云计算风险管理能力评估”。

数据中心运营安全。华为云数据中心业务实现全球统一规划管理: 1）**访问控制**，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。2）**监控系统**，对机房外围、出入口、走廊、电梯、机房等重要场所进行 7*24 小时闭路电视监控，并与红外感应、门禁等联动。电力、温湿度、消防等环境运行状态进行 7*24 小时监控，安全隐患能被及时发现并修复。3）**安全审计与检查**，保安人员对数据中心定时巡查。机房管理员开展例行安检，不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。

容灾。在全球的各地建立并部署了数十个区域（Region）。每个区域内部署了多个可用区（AZ），每个可用区内有多个物理数据中心（DC）。华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。各区域/可用区内部通过高速光纤进行数据中心互联（DCI）， 通过多副本冗余和多活技术，保障数据中心业务连续性。

物理设备生命周期安全。针对物理设备的使用、维护和销毁，制定了完善的安全防护规程和措施。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，且由专人负责保险箱的开关；数据中心的任何配件，都必须经过授权方能领取，且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。

基础架构安全。在计算架构、存储架构、网络架构方面均具备风险管理措施，已通过“可信云云计算风险管理能力评估”。

2.资源抽象和管理安全责任承担

华为云以统一虚拟化平台(UVP)为核心，承担 IaaS、PaaS 和 SaaS 模式下资源抽象和管理的安全责任，具体包括:

安全隔离。1）**计算隔离**，通过 CPU 隔离机制，UVP 可以控制虚拟机对物理设备以及虚拟化运行环境的访问权限，从而实现虚拟化平台与虚拟机之间以及不同虚拟机之间在信息和资源上的隔离。2）**存储隔离**，虚拟化平台管理虚拟机内存与真实物理内存之间的映射关系。保证虚拟机内存与物理内存之间形成一一映射关系。虚拟机对内存的访问都会经过虚拟化层的地址转换，保证每个虚拟机只能访问到分配给它的物理内存。3）**网络隔离**，由 虚拟交换机（vSwitch）通过设置 VLAN、VXLAN、ACL 等属性确保虚拟机在网络层的逻辑隔离。多台主机之间的网络依然使用传统的物理网络设备（路由器、交换机等）进行物理隔离。

虚拟化平台安全。对主机操作系统进行最小化裁剪并对服务做安全加固。同时，对接入主机操作系统的华为云管理员执行严格的权限

访问控制，对其所执行的各项运维运营操作实行全面的日志审计。华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。

云控制台、云服务 API 和云服务产品安全。1）**DevOps 和 DevSecOps 流程**。积极推行将安全嵌入快速迭代的 DevOps 流程，并逐步形成高度自动化的 DevSecOps 全新安全生命周期管理流程。2）**安全设计**。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，设计工程师设计对应的安全方案。3）**安全编码和测试**。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，经过多轮安全测试，测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。4）**第三方软件安全管理**。对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，并对引入环节实施严格的管控。5）**配置与变更管理**。通过专业的配置管理数据库工具对配置项、配置项的属性和配置项之间的关系进行管理。6）**上线安全审批**。云平台版本、重要云服务上线前，安全团队、法务团队和开发团队合作，共同分析、判断其相关版本或服务是否符合所服务区域的安全隐私合规要求。

3. 操作系统安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，华为云对操作系统相关安全责任承担有所区别，具体包括:

公共镜像安全/（PaaS、SaaS）镜像安全。在 IaaS 模式下承担公共镜像安全，在 PaaS 和 SaaS 模式下承担底层主机所使用镜像的安全

责任。公共镜像通过镜像服务持续提供给租户，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。同时还支持云主机镜像和容器镜像的滚动升级，以完成系统漏洞修复，不会对租户业务造成影响。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。

服务市场镜像安全。在 IaaS 模式下承担部分服务市场镜像安全责任，具体表现为： 1）在用户购买云主机时，需阅读和签定《镜像免责声明》[4]，声明中告知用户服务市场镜像由第三方提供，安全责任最终共担方为第三方服务提供者。2）对申请加入云市场的服务商，从资质和服务两方面进行要求和准入。

主机安全监测。在 PaaS 和 SaaS 模式下，华为云承担底层云主机的安全监测与处置。

云主机备份。在 PaaS 和 SaaS 模式下，华为云负责底层云主机的备份。

4. 网络控制安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，华为云对网络控制相关安全责任承担有所区别，具体包括:

安全组。在 IaaS、PaaS 模式下，华为云向用户提供安全组功能。在 IaaS 模式下,用户可以基于安全组设置多台云服务器的分组隔离，

[4] 华为云《镜像免责声明》
https://www.huaweicloud.com/declaration/tsa_ims.html?locale=zh-cn

建立内网负载均衡安全组以确保租户实例只接收来自负载均衡器的流量。在 PaaS 模式下，用户可以综合运用子网和安全组的配置，来完成关系型数据库、文档型数据库实例的隔离。在 SaaS 模式下，华为云负责底层主机、数据库资源的安全组设置。

网络类型选择。华为云提供专有网络 VPC、专线接入等网络类型。在 IaaS、PaaS 模式下，多种云服务支持 VPC，帮助用户实现云服务更安全的访问控制。在 SaaS 模式下，华为云负责底层网络的选择和使用。

IP 黑白名单。在 IaaS、PaaS、SaaS 模式下，华为云为多种云服务提供 IP 黑白名单服务以供用户使用。

5. 应用安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，华为云对应用安全相关安全责任承担有所区别，具体包括:

应用生命周期安全（SaaS）。详见云服务产品安全责任承担。

应用安全管理（SaaS）。1）**漏洞管理**。华为产品安全事件响应团队和云安全运维团队建立了成熟的漏洞感知、处置和对外披露的机制，并持续优化安全漏洞的管理流程和技术手段，确保漏洞可在 SLA 时间内完成响应和修复。2）**安全防护**。建立了稳固、完善的边界和多层立体的安全防护系统，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。

应用内容安全。建立了完善的违法违规内容处置与配合机制。在 IaaS、PaaS 模式下，应用为用户公开的应用，在 SaaS 模式下，应用

为华为云提供的 SaaS 服务。

网站域名备案。华为云为用户提供备案服务，自身积极履行 ICP 备案职责，同时对未履行备案职责的网站应用采取处置措施。

6. 数据安全责任承担

华为云的云上数据安全体系遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为用户提供最切实有效的数据保护能力。

利用云上数据安全体系，华为云承担云服务衍生数据、云服务提供者数据和个人隐私信息的安全责任。对于个人隐私信息，华为云秉承公司以网络安全和隐私保护为最高纲领，以国内外隐私保护的法律法规为基石，依托于华为公司的隐私保护体系，借鉴业界广泛认可的优秀实践，已形成适合华为云的隐私保护体系。致力研发各类隐私增强技术（PET），积累隐私保护工程技术能力，以满足客户不同需要实施隐私保护。

对于云服务客户数据，华为云承担部分安全责任，具体包括:

1） 提供传输加密、数据隔离、存储加密等产品或能力（具体的使用和配置由用户负责）。

2） 在未获得用户授权的情况下不访问和使用用户数据。

3） 数据销毁安全。致力于保护租户数据在删除过程中及删除后不至泄露。**内存删除**，在云操作系统将内存重新分配给用户之前，会对分配的内存进行清零操作，即写“零”处

理，从而保障在新启动的虚拟机中恶意内存检测软件无法检测到有用信息，防止通过物理内存恢复删除数据造成的数据泄露。**数据安全（软）删除**，提供对废弃数据的逻辑删除功能，租户可根据需要通过管理控制台对诸如 RDS 等存储服务中的数据实现灵活的一键删除。**磁盘数据删除**，对销户虚拟卷采用清零措施，确保数据不可恢复，有效防止被恶意租户使用数据恢复软件读出磁盘数据，杜绝信息泄漏风险。**物理磁盘报废**，对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保用户隐私和数据不受未授权访问

7.身份识别和访问管理安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，华为云对身份识别和访问管理相关安全责任承担有所区别，具体包括:

云控制台 IAM 安全（IaaS/PaaS/SaaS）。1）密码安全策略。支持租户的安全管理员根据需求，设置不同强度的密码策略、更改周期和登陆策略。2）身份鉴别信息。采用加密存储和加密传输的方式。3）云审计服务。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。4）权限管理。通过统一身份认证服务（IAM），提供用户管理权限和云资源权限。

云服务 IAM 安全（IaaS/PaaS）。1）密码安全策略。创建云主机等服务时，均有密码复杂度等要求。2）身份鉴别信息。采用加密存储和加密传输的方式。3）实名认证。对用户进行实名认证审核，完

成实名认证的用户方提供云服务。

云服务提供者内部平台 IAM 安全（IaaS/PaaS/SaaS）。1）账号认证。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。员工账号用于登录 VPN、跳板机，实现用户登录的深度审计。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。跳板机支持强日志审计，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。2）账号生命周期管理。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。运维帐号、所有设备及应用的帐号均由 LDAP 集中管理，并通过统一运维审计平台集中监控，并且进行自动审计。3）权限管理。根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。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，其他设备无权访问。

（三）腾讯云

1.物理基础设施安全责任承担

腾讯云承担 IaaS、PaaS 和 SaaS 模式下物理基础设施的安全责任，具体包括:

数据中心环境安全。腾讯云在全球的各数据中心均按照相关国际标准和当地安全要求进行选址、建设或租赁。各数据中心电力系统和空调系统均采用高稳定性全冗余系统，在任意单设备故障情况下，均

能确保数据中心的电力和供冷持续性；各数据中心均配备完整的消防系统，包括定点区域火灾侦测系统、自动气体灭火系统以及供紧急使用的手动灭火装置；各数据中心内部全部安装防静电地板，机柜、线槽等，且均安装接地线，用以防御静电给设备带来的损害，相关情况已通过“可信云云计算风险管理能力评估”。

数据中心运营安全。1）**访问控制**，腾讯云将数据中心不同区域划分为三类安全级别，一般安全区域、受限安全区和高度受限安全区。各数据中心根据不同级别的区域安全要求制订了严格的基础设施和环境访问控制。根据数据中心人员类别和访问权限，建立了完整的人员访问控制安全矩阵，实现对数据中心的各类人员的访问、操作等行为的有效管控。其中，门禁授权系统按照不同安全等级和不同功能的区域进行划分，各类来访或工作人员出入数据中心均需进行身份核对和随身物品检查，并登记携带物品。从环境控制角度，各数据中心对车辆进出也有严格的管理规定和控制措施，所有员工个人车辆、供应商货车等都需进行车辆信息登记，且仅允许获得授权的车辆进入数据中心周边环境。 2）**监控系统**，数据中心的监控管理方面覆盖各机房内部、工作交接区、园区出入口和园区内各建筑物的出入口，均配备了 7*24 小时无盲点的视频监控告警系统（所有监控记录均保存足够的时间并安全存储），并由保安室 7*24 小时值守。机房内具备完善的动力环境监控系统，能够对机房漏水、空调、配电等状况进行实时监控。3）**安全审计与检查**，各数据中心的安保人员每日均严格根据巡检清单和巡检计划对各机房和设备情况进行巡检，巡检频率不低于每

2 小时/次，并在每个检查点签名并记录检查时间，一旦发现安全违规事件，会立即启动数据中心机房管理紧急流程。建立了定期安全审计管理制度，每个季度对物理安全现场操作和管理进行审计，并输出内部审计报告，跟进和推动物理安全审计风险点的改进。

容灾。腾讯云计算节点覆盖华南、华东、香港、海外等多个地区，客户可根据业务发展需求和数据安全要求，自主灵活地将数据和系统部署于不同数据中心或不同区域，以保证业务的容灾性要求。为保证客户业务的持续可用，腾讯云为每一个云产品（包括计算与网络、存储与 CDN、云数据库以及安全类的云产品）制定了详细的容灾恢复预案，内容包括每一个产品的业务容灾特点、详细的应急响应流程、人员的详细职责和联系方式、恢复点目标 RPO 和恢复时间目标 RTO 等内容，并严格按照要求进行定期演练确保容灾恢复预案的及时性与可行性。

物理设备生命周期安全。建立了数据中心物理设备从采购、使用、维护和销毁的全生命周期管理制度，要求关键环节审批后再实施，并生成相应记录。

基础架构安全。在计算架构、存储架构、网络架构方面均具备风险管理措施，已通过“可信云云计算风险管理能力评估”。腾讯云基础网络采用 N*N 的冗余建设方式，配合路由层级的路径优先和路由可达性的流量工程调度，确保网络服务不会因为单点设备故障而中断。腾讯云的计算节点也是采用 N*N 的冗余建设方式，单一计算节点在故障发生时通过调度器实时自动剔除，有效保障用户业务的可用性。

2. 资源抽象和管理安全责任承担

腾讯云承担 IaaS、PaaS 和 SaaS 模式下资源抽象和管理的安全责任，具体包括:

安全隔离。在虚拟化控制层为云服务器等资源提供完整的租户间虚拟资源隔离能力，不同用户的网络、内存、磁盘等资源均通过底层逻辑控制杜绝了互通互访的可能性。对于云数据库，采用物理机，并在此基础上通过 VPC 网络和 Cgroup 技术，对网络与机器上的实例实现了严密隔离。

虚拟化平台安全。持续关注云自身的虚拟化安全问题。由于虚拟化架构的特殊性，当网络边界被模糊化时，一旦关键漏洞被恶意利用，极有可能会将风险贯穿至整个云计算系统导致出现重大的安全影响。腾讯云一直致力于虚拟化中漏洞挖掘和风险处置的研究，同时建设了成熟的网络安全架构，通过防火墙、分布式防护、入侵防御、态势感知等多重防护机制，应对云平台可能面临的各种威胁。

云控制台、云服务 API 和云服务产品安全。云着力将 ISO/IEC 20000 信息技术服务管理标准和 ISO/IEC 9001 质量管理体系标准融入到整个产品 SDL 安全开发流程中，关注需求、设计、研发、测试、交付、运维等不同环节，在产品开发各个阶段中消除信息安全和隐私问题，确保所有的云产品在其生命周期内均能获得足够的安全管控与评估。腾讯云严格按照安全开发生命周期方法开发云平台及云产品，目标是将信息安全融入到整个腾讯云的软件开发生命周期中。

3. 操作系统安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，腾讯云对操作系统相关安全责任承担有所区别，具体包括:

公共镜像安全/（PaaS、SaaS）镜像安全。在 IaaS 模式下承担公共镜像安全，在 PaaS 和 SaaS 模式下承担底层主机所使用镜像的安全责任，具体表现为：由内部专业安全运维团队制作并严格测试后发布。腾讯云凭借安全联合实验室提供的强有力的技术支持，构建了一套包涵漏洞多重挖掘、漏洞处置和漏洞库收集的完整深入的漏洞管理体系，形成有效的漏洞处置手段。同时 ，腾讯安全应急响应中心 TSRC 向所有公众开放一个漏洞提交平台，以借助大众的力量，协助腾讯一起完善漏洞的发现和处置。在发现新的高危安全漏洞后，腾讯云会迅速告知客户。

服务市场镜像安全。在 IaaS 模式下承担部分服务市场镜像安全责任，具体表现为：1）**制定云市场管理规范，**对入驻云市场的服务商进行严格的资质审核，要求其签定《腾讯云云市场服务商接入协议》，通过缴纳保证金、违规处罚等措施对服务商行为进行约束。2）**严格的制作流程**，腾讯云规范了镜像制作步骤和安全规范，服务商需按照步骤和规范进行服务市场镜像制作。3）**镜像安全审核**。腾讯云对服务商申请的镜像的安全、功能等进行扫描检查，以及对商品内容进行审核，达到《镜像安全审核标准》[5]后才可上架。

主机安全监测。在 PaaS 和 SaaS 模式下，腾讯云承担底层云主机的安全监测与处置。在 IaaS 模式下，腾讯云在用户购买云主机时默

[5] 腾讯云《镜像安全审核标准》
https://cloud.tencent.com/document/product/306/14191

认开启安全加固，为用户提供免费的 DDoS 防护和主机安全防护，用户可以主动选择不勾选该功能。

云主机备份。在 PaaS 和 SaaS 模式下，腾讯云负责底层云主机的备份。

4. 网络控制安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，腾讯云对网络控制相关安全责任承担有所区别，具体包括:

安全组。在 IaaS、PaaS 模式下，腾讯云向用户提供安全组功能。在 IaaS 模式下，用户可以基于安全组设置单台或多台云服务器的网络访问控制。在 PaaS 模式下，用户可以基于安全组对云数据库 Mysql 进行网络访问控制。在 SaaS 模式下，腾讯云负责底层主机、数据库等资源的安全组设置。

网络类型选择。腾讯云提供私有网络 VPC、专线接入等网络类型。在 IaaS、PaaS 模式下，多种云服务支持 VPC，如云服务器、云数据库，用户可以通过合理使用 VPC 来实现云服务更安全的访问控制。在 SaaS 模式下，腾讯云负责底层网络的选择和使用。

IP 黑白名单。在 IaaS、PaaS、SaaS 模式下，腾讯云为多种云服务提供 IP 黑白名单功能以供用户使用，如对象存储、CDN、企业邮箱等。

5. 应用安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，腾讯云对应用安全相关安全责任

承担有所区别，具体包括:

应用生命周期安全（SaaS）。详见云服务产品安全责任承担。

应用安全管理（SaaS）。云鼎实验室联合腾讯其他安全实验室进行全面的应用层安全漏洞挖掘和漏洞分享，将漏洞防护能力以虚拟补丁方式整合入腾讯云的 Web 应用防火墙系统中，提升应用安全性。

应用内容安全。以大数据与人工智能为核心构建业务安全防护体系，通过整合业务安全防护中不断积累的黑产对抗经验，将单一的安全数据单元关联形成立体的安全数据矩阵，持续完善腾讯云已有的黑产数据库，不断应用内容安全性。在 IaaS、PaaS 模式下，应用为用户公开的应用，在 SaaS 模式下，应用为腾讯云提供的 SaaS 服务。

网站域名备案。腾讯云为用户提供免费的备案服务，自身积极履行 ICP 备案职责，同时对未履行备案职责的网站应用采取处置措施。

6.数据安全责任承担

腾讯云的云上数据安全体系围绕事前防范、事中保护和事后追溯三个阶段，事前防范通过建立完善的数据分类分级标准，在人员、流程、技术上层层把关，从源头上确保数据的机密性、可用性和完整性；事中保护通过在云平台的各个层面部署全面的安全防护，并将事中保护能力转化为客户能够感知和应用的云安全产品，以及时发现潜在的数据安全事件；事后追溯通过腾讯安全应急响应中心以及强大的日志审计，对数据安全事件进行积极的补救和追溯，最大限度降低损失。

利用云上数据安全体系，腾讯云承担云服务衍生数据、云服务提供者数据和个人隐私信息的安全责任。对于个人隐私信息，腾讯云严

格按照《腾讯云隐私声明》和《腾讯隐私政策》进行收集、使用、存储和分享，不会尝试访问或披露客户内容，以确保客户对自己内容具有唯一的所有权和控制权。

对于云服务客户数据，腾讯云承担部分安全责任，具体包括:

1） 提供数据分类分级、敏感数据发现、传输加密、存储加密等产品或能力（具体的使用和配置由用户负责）。

2） 对于腾讯云内部的员工，除非客户所选取的服务需要处理客户的数据，腾讯云员工不会尝试访问任何客户数据。

3） 数据销毁安全。所有数据收集和处理的过程中产生的内存临时数据，均会不可撤销地将其自动清除。在进行资源再分配之前会遵循标准策略及合同要求及时进行严格的逻辑擦除或物理擦除。 当客户不再使用腾讯云服务时，根据腾讯云与客户达成的服务协议，腾讯云将在保留期限内为客户保留数据，客户需在保留期限届满前完成全部数据的迁移。保留期限届满后，服务系统将自动删除包括副本和备份在内的所有客户数据，删除后的所有数据无法复原。当用于提供腾讯云服务的介质出现故障需要更换或者到达使用期限需要报废时，腾讯云将及时清除剩余信息，并交由消磁中心按照行业标准做法对存储介质进行消磁，密封存放两年之后再进行彻底的物理销毁。

7.身份识别和访问管理安全责任承担

在 IaaS、PaaS 和 SaaS 模式下，腾讯云对身份识别和访问管理相

关安全责任承担有所区别，具体包括:

云控制台 IAM 安全（IaaS/PaaS/SaaS）。1）密码安全策略。控制台具备默认的密码安全策略要求,同时支持主账户配置安全策略。2）身份鉴别信息。采用加密存储和加密传输的方式。3）提供云审计服务,以为用户提供统一的云资源操作日志管理。4)提供访问管理 CAM 服务，以供用户进行身份管理与资源访问控制。

云服务 IAM 安全（IaaS/PaaS）。1）密码安全策略。创建云主机等服务时，均有密码复杂度等要求。2）身份鉴别信息。采用加密存储和加密传输的方式。3）实名认证。对用户进行实名认证审核，完成实名认证的用户方提供云服务。

云服务提供者内部平台 IAM 安全（IaaS/PaaS/SaaS）。在云产品的运营中，提供强制的、细粒度的权限管理能力。结合自动化的运维管理机制，建立了统一的运营管理门户，所有的生产环境操作均受到严格的权限控制和监控。腾讯云运营管理团队的人员变更均由统一运营管理门户实现自动化权限控制：入职时自动赋予基本的默认权限，调职时自动修改岗位权限，离职时自动禁用所有权限。员工可在统一运营门户中申请所需的临时或固定权限，在获得多级评审和批准后，系统将自动赋予其新的权限。临时权限在使用期限结束后自动回收。腾讯云不允许任何可能存在冲突的权限被同时获取,这依赖于腾讯云内部复杂的权限分离矩阵机制。腾讯云会定期组织内部权限审核工作，确保权限不会被滥用、误用。腾讯云生产环境已全面部署堡垒机，通过堡垒机将腾讯云后端系统组件的管理员账号权限进行集中管控。运

营管理团队人员仅能使用堡垒机新赋予的账号并通过二次身份校验（如动态验证口令）进行登录，自动获得适当的系统操作权限。所有后台运维操作记录均由日志平台集中加密存储，由腾讯云内部审计团队定期对记录信息进行审核。

附录 2：政务云安全责任共担优秀案例

（一）浪潮云

在政务云中，安全责任的识别和划分与云服务客户业务特性和需求相关。浪潮云通过与政务云客户沟通协商，确定该客户政务云场景下的安全责任及划分方式，并通过签定安全责任协议，约束双方对安全责任的承担与落实。

以下为浪潮云与某政务云客户的安全责任共担实践:

表 6 浪潮政务云安全责任划分案例

安全责任		云服务提供者	云服务客户
安全物理环境		✓	×
安全通信网络	网络架构	✓	✓
	通信传输	✓	×
	可信验证	✓	×
安全区域边界	边界保护	✓	✓
	访问控制	✓	✓
	入侵防范	✓	×
	恶意代码和垃圾邮件防范	✓	×
	安全审计	✓	✓
	可信验证	✓	×
安全计算环境	身份鉴别	✓	×
	访问控制	✓	✓
	安全审计	✓	×
	入侵防范	✓	✓
	恶意代码防范	✓	✓
	镜像和快照保护	✓	×
	可信验证	✓	×
	数据完整性和保密性	✓	✓
	数据备份恢复	✓	✓
	剩余信息保护	✓	×
	个人信息保护	×	✓
安全管理中心	系统管理	✓	×
	审计管理	✓	×
	安全管理	✓	×
	集中管控	✓	✓
安全管理制度		✓	✓

安全责任		云服务提供者	云服务客户
安全管理机构		✓	✓
安全管理人员	人员录用	✓	✓
	人员离岗	✓	✓
	安全意识教育和培训	✓	✓
	外部人员访问管理	✓	×
安全建设管理	定级和备案	×	✓
	安全方案设计	✓	✓
	产品采购和使用	✓	✓
	自行软件开发	✓	✓
	外包软件开发	✓	✓
	工程实施	✓	✓
	测试验收	✓	✓
	系统交付	✓	✓
	等级测评	✓	✓
	服务供应商选择	×	✓
	供应链管理	✓	×
安全运维管理	环境管理	✓	×
	资产管理	✓	×
	介质管理	✓	×
	设备维护管理	✓	×
	漏洞和风险管理	✓	✓
	网络和系统安全管理	✓	×
	恶意代码防范管理	✓	✓
	配置管理	✓	✓
	密码管理	✓	✓
	变更管理	✓	✓
	备份与恢复管理	✓	✓
	安全事件处置	✓	×
	应急预案管理	✓	✓
	外包运维管理	✓	×

1. 安全物理环境责任划分

安全物理环境责任由浪潮云承担，包括数据中心的物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、放水和防潮、防静电、温湿度控制、电力供应、电磁防护方面的安全责任。

2. 安全通信网络责任划分

安全通信网络责任划分如下:

浪潮云和客户共同分担的责任：网络架构。浪潮云负责网络架构冗余、网络区域划分、网络质量保障、虚拟网络隔离、云平台等级保护定级等安全责任，能够根据客户要求，提供边界防护、通信传输等网络安全机制。政务云客户负责云上业务系统的网络等级保护定级，同时应结合自身业务需求，明确政务云平台边界防护、入侵防范、通信传输等方面的网络安全机制的要求。

浪潮云承担的责任：1）通信传输，浪潮云采用合理的技术和手段保证通信过程中的数据安全性。**2）可信验证**，浪潮云基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，在检测到可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

3.安全区域边界责任划分

安全区域边界责任划分如下:

浪潮云和客户共同分担的责任：1）边界保护，浪潮云负责对跨边界的访问和数据流通进行控制，部署边界防护措施。政务云客户应结合自身业务需求，明确边界防护要求。**2）访问控制**，浪潮云根据政务云平台整体情况和客户的业务要求，制定访问控制策略，划分不同安全等级的网络区域，具备相应的安全防护能力。政务云客户应结合自身业务需求，明确访问控制策略、网络划分等要求。**3）安全审计**，

浪潮云负责对网络边界、重要网络节点的用户行为、安全事件进行记录和审计，对审计记录进行保护和留存，保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。政务云客户应结合自身业务需求，明确安全审计要求，确认相应权限。

浪潮云承担的责任：1）入侵防范，浪潮云负责对网络攻击行为、异常流量的检测、告警与防护，同时为客户提供互联网发布内容的安全监测。**2）恶意代码和垃圾邮件防范**。浪潮云负责对关键网络节点的恶意代码、垃圾邮件进行检测和清除。**3）可信验证**，同“安全通信网络-可信验证”部分。

4.安全计算环境责任划分

安全计算环境责任划分如下:

浪潮云和客户共同分担的责任：1）身份鉴别。浪潮云负责对用户登陆行为进行身份鉴别，制定身份鉴别信息安全策略，具备登陆失败处理功能，建立远程管理安全把控措施。政务云客户应核验、监督虚拟机等设备满足身份鉴别要求。**2）访问控制**。在资源交付前，及客户正式授权下，浪潮云负责对登陆用户和管理用户进行账户与权限分配，资源交付后权限归还于客户。政务云客户负责自身业务系统账号、口令及权限的控制。**3）入侵防范**。浪潮云负责对虚拟机异常情况、漏洞进行监测和告警，确保告警行为可及时通知客户，通过采取最小安装原则、关闭不必要端口和系统服务等措施提升虚拟机安全性。政务

云客户负责所属服务器操作系统及业务应用系统的更新和漏洞修复。**4）恶意代码防范**。浪潮云负责对恶意代码进行检测和处置。政务云客户负责配合浪潮云采取处置措施。**5）数据完整性和数据保密性**。浪潮云通过技术手段保证数据在传输和存储过程中的完整性和保密性。政务云客户对数据完整性、数据保护性功能提出要求。**6）数据备份恢复**。浪潮云提供数据本地备份与恢复、异地备份与恢复、数据迁移等功能。政务云客户应在本地保存其业务数据的备份。

浪潮云承担的责任：1）安全审计。浪潮云负责对用户行为、安全事件进行记录和审计，对审计记录进行保护和留存。保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。**2）镜像和快照保护**。浪潮云负责通过技术手段防止虚拟机镜像被篡改、敏感资源被非法访问，针对客户业务需求能够提供加固的镜像。**3）剩余信息保护**。浪潮云保证鉴别信息、敏感数据等存储空间被释放或重新分配前，以及虚拟机所使用的内存和存储空间回收时，均得到完全清除，确保云服务客户数据被删除时，所有副本都被删除。**4）可信验证**，同“安全通信网络-可信验证”部分。

政务云客户承担的责任：个人信息保护。客户应保证仅采集业务必须的个人信息，未授权不访问和使用个人信息。

5. 安全管理中心责任划分

安全管理中心责任划分如下:

浪潮云和客户共同分担的责任：集中管控。客户结合自身业务需求对服务商提出集中监测方面的要求，浪潮云对云平台底层各设备、链路进行集中监测，并提供虚拟机等云资源的集中监控功能。

浪潮云承担的责任：系统管理、审计管理、安全管理。浪潮云对系统管理员、审计管理员、安全管理员进行身份鉴别与操作审计，通过各管理员权限进行系统管理、审计分析和安全策略配置。

6.安全管理制度责任划分

安全管理制度责任由**浪潮云和客户共同分担，包括确定安全策略、形成管理制度体系、制定和发布、评审和修订**。浪潮云承担服务商侧上述责任，政务云客户承担客户侧上述责任。

7.安全管理机构责任划分

安全管理机构责任由**浪潮云和客户共同分担，包括岗位设置、人员配备、授权和审批、沟通和合作、审核和检查**。浪潮云承担服务商侧上述责任，政务云客户承担客户侧上述责任。

8.安全管理人员责任划分

安全管理人员责任划分如下:

浪潮云和客户共同分担的责任：人员录用、人员离岗、安全意识教育和培训。浪潮云承担服务商侧上述责任，政务云客户承担客户侧上述责任。

浪潮云承担的责任：外部人员访问管理。浪潮云确保外部人员的

访问在审批授权下进行。

9.安全建设管理责任划分

安全建设管理责任划分如下:

浪潮云和客户共同分担的责任:安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评。浪潮云承担服务商侧上述责任，政务云客户承担客户侧上述责任。

浪潮云承担的责任：供应链安全。浪潮云确保供应链安全事件及供应商重要变更及时传达到客户。

政务云客户承担的责任：定级和备案、服务供应商选择。客户需完成云上系统的定级和备案工作，通过签定协议规范服务商权限与责任。

10.安全运维管理责任划分

安全运维管理责任划分如下:

浪潮云和客户共同分担的责任：漏洞和风险管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、应急预案管理。对于漏洞和风险管理，浪潮云采用技术手段和专业服务及时发现云平台和上云系统的安全漏洞和隐患，做好云平台的修补；向云服务客户发出预警，并配合云服务客户完成上云系统的修复。云服务客户根据云服务漏洞和风险监测情况，在云服务商配合下组织修复。对

于其它安全责任，浪潮云负责服务商侧相关责任，政务云客户负责客户侧相关责任。

浪潮云承担的责任：环境管理、资产管理、介质管理、设备维护管理、网络和系统安全管理、安全事件处置、外包运维管理。浪潮云负责机房的安全管理，确保云平台运维地点位于中国境内、云服务衍生数据存储于中国境内；对资产进行分类与标识管理，保障介质安全，对设备的维护、处理、报备和重用进行安全管理；把控网络和系统的运维安全；具备安全事件报告和响应能力；对外包运维服务商进行安全管理。