ICS 35.030
CCS L 80

T/CCIA

中国网络安全产业联盟技术规范

T/CCIA XXX—2024

云计算服务安全责任划分规则及实施指南

Implementation guidelines for security responsibility division and control of cloud computing services

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国网络安全产业联盟　　发　布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国网络安全产业联盟提出并归口。

本文件起草单位： 阿里云计算有限公司、国家信息技术安全研究中心、北京赛西科技发展有限责任公司、中国电子技术标准化研究院、中国信息通信研究院、中国信息安全测评中心、中国软件测评中心

本文件主要起草人：方强、陈迪思、王睿超、卢夏、惠景丽、张英、何延哲、刘文治、马庆栋、石然、王惠莅、刘佳良、胡华明、韩雪峰、付嵘、李安伦、任恒、张祺

信息安全技术 云计算服务安全责任划分规则及实施指南

1 范围

本文件规定了客户、云服务提供者、硬件提供者、软件提供者、运维服务提供者、安全服务提供者等角色的安全责任划分的参考规则及实施方法。

本文件适用于上述云服务参与方进行云计算服务的规划、建设、运营等过程。第三方测评机构在开展云计算服务安全评估测试时可参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 42250-2022 信息安全技术 网络安全专用产品安全技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 31167-2023 信息安全技术 云计算服务安全指南

GB/T 31168-2023 信息安全技术 云计算服务安全能力要求

GB/T 32400-2015 信息技术 云计算 概览与词汇

GB/T 32399-2015 信息技术 云计算 参考架构

GB/T 35279-2017 信息安全技术 云计算安全参考架构

3 术语和定义

GB/T 31167-2023界定的以及下列术语和定义适用于本文件。

3.1

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自助服务的方式供应和管理的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[来源:GB/T 32400-2015，3.2.5]

3.2

云服务 cloud computing service

通过云计算已定义的接口提供一种或多种能力。

[来源:GB/T 32400-2015，3.2.8]

3.3

云服务提供者 cloud service provider

面向云服务客户，使用电信资源提供云服务，对云平台的搭建或运维、底层硬件及云平台安全能力有决策和控制权的参与方。

[来源:GB/T 32399-2015，3.2.15，有修改]

3.4

云服务客户 cloud service customer

为使用云服务而处于一定业务关系中的参与方。

注:业务关系不一定包含经济条款。

本文件中云服务客户简称客户。

[来源:GB/T 32400-2015， 3.2.11]

3.5

云服务合作者 cloud service partner

支撑或协助云服务提供者对云平台行使决策和控制权的活动参与方。包括软件提供者、硬件提供者、运维服务提供者、安全服务提供者。

3.6

软件提供者 software provider

为云服务能力的形成提供软件产品的参与方。

注：本文件中的软件是指提供物理设备的虚拟化、物理和虚拟化资源的调度、管控、产品化能力的云平台软件。

3.7

硬件提供者 hardware provider

为云服务能力的形成提供物理基础设施的参与方。

注：物理基础设施包括机房、服务器、网络设备、存储设备等。

3.8

运维服务提供者 operation and maintenance service provider

为软件、物理基础设施等提供运行维护服务的参与方。

注：运行维护服务包括软件、物理基础设施的使用支持、变更支持、巡检、问题发现和推动解决等。

3.9

安全服务提供者 cloud service security provider

支撑或协助云服务提供者安全管理、安全技术和安全运维活动的参与方。

注：安全管理、安全技术和安全运维活动是指为实现云服务提供者或客户的安全目标提供安全规划方案、安全工具或产品、安全运维人员支持等。

4 云计算服务安全责任角色划分

当云服务提供者与云服务合作者联合向云服务客户提供云计算服务时，除GB/T 31167 5.2.1规定的角色和职责外，云计算服务安全管理的责任方还会包括软件提供者、硬件提供者、运维服务提供者、安全服务提供者。6个安全责任角色之间的关系如图1 云计算服务安全责任参与方角色示意图所示。

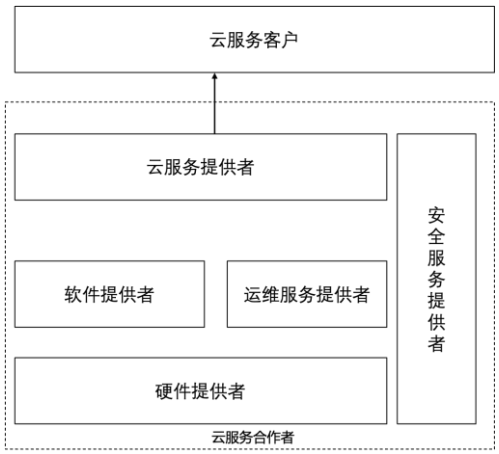

图 1 云计算服务安全责任参与方角色示意图

云服务提供者需以合同或其他方式，与软件提供者、硬件提供者、运维服务提供者、与服务安全提供商等相应的安全责任进行规定并予以落实。云服务提供者是客户或主管部门开展云计算服务安全管理的直接对象。

5 云计算服务安全责任共担模型

云计算服务安全责任的划分参考图2。

图 2 云计算服务安全责任划分模型

本文件是对GB/T 31167-2023及GB/T 31168-2023中未明确的多方责任的控制点提出安全责任划分及实施细化和补充。

云计算服务安全责任划分模型分为通用实施方法、基础设施层实施方法、平台层实施方法、应用层实施方法四个层级。各层级中根据开发与建设、运行、迁移与终止三个阶段分别由不同角色承担相应的控制点实施工作。

本文件给出的责任模型为参考模型，是从强化云服务安全责任管理方面提出的建议。由于在实践中，并非所有云计算服务采取一致的责任划分及实施方法，也可能因云服务实际情况以及不同角色之间合同协议等方式发生安全责任实施工作情况。因此，关于责任模型在实践中的应用，需关注以下方面：

a） 原则上，控制点实施工作可以转移，责任不能转移，包括：
云服务提供者责任原则上不应以任何方式转移至客户；
云服务提供者责任原则上不能将所有责任转移至云服务合作方，如因云计算服务安全运营需要转移安全责任实施工作的，则需确保合同协议中有明确的责任划分条款；

b） 云服务提供者安全责任实施工作转移原则上不应超过2次；

c） 客户将安全安全责任实施工作委托云服务提供者或其他第三方角色的，需确保合同协议中有明确的责任划分条款且合同协议不得中断，合同协议中断的，则客户承担责任；

d） 云计算参与方发现其他方未能履行安全责任的，有及时提醒的义务。

5.1 经营合规

客户与云服务提供者、软件提供者、硬件提供者、运维提供者、安全服务提供者之间的经营合规责任划分如下：

a） 客户：根据自身经营所需要遵循的法律法规、国家强制性标准的要求，选择符合网络安全和数据处理安全条件的云服务（如网络安全等级、加密、备份等）。

b） 云服务提供者：遵守云服务作为电信业务所需要符合的法律法规、国家强制性标准的要求，包括根据《电信业务经营许可管理办法》获得相关电信业务经营许可证（如需），采购和备案电信资源、完成机房节点的测评等。

c） 软件、硬件提供者：遵守相关国家标准的强制性要求，网络安全专用产品符合GB/T 42250-2022等标准要求。

d） 运维服务、安全服务提供者：遵守相关国家标准的强制性要求，具备相关技术人员及行业资质。

5.2 业务定级

客户与云服务提供者、软件、硬件提供者、运维服务提供者、安全服务提供者之间的业务定级责任划分如下：

a） 客户：

1） 根据GB/T 31167-2023规定并结合自身数据和业务类型，确定云计算服务的部署类型及安全能力要求级别。根据云计算服务的特点进行需求分析，确定选择的云服务类别，形成决策报告。

2） 选择合适的云服务提供者，并应告知云服务提供者具体的安全要求，约定安全要求的具体指标。

b） 云服务提供者：按照自身的业务类型以及与客户的约定，明确自身应当满足的安全能力要求，制定安全规划，完成安全评估报告。

c） 云服务合作者：如实描述所提供产品、服务的功能、性能、参数、适用场景，供云服务提供者评估、选择、管理、使用。

5.3 安全组织和人员

云服务各参与方应参考GB/T 31168-2023履行安全责任，还宜负责：

a） 客户负责：确保安全组织和人员具备使用云服务所需的安全知识，足以支持客户选择和管理符合条件的云服务。客户业务系统被认定为关键信息基础设施的，设置安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查。

b） 云服务提供者负责：确保安全组织和人员具备建设和运营云服务所需的安全知识，足以支持云服务提供者选择和管理符合条件的云服务参与方。对云服务合作者的服务人员提出管理要求及考核。

c） 云服务合作者负责：确保安全组织和人员具备研发和运营软件、硬件，提供运维和安全服务所需的安全知识，具备能力提供协议约定的网络产品和服务。

5.4 风险评估与业务连续性

云服务各参与方所负责如下：

a） 客户负责：按照上云后“安全管理责任不变，数据归属关系不变，安全管理标准不变”的原则，对自身业务系统进行风险评估与持续监控，根据GB/T 31167-2023 6.14要求保证业务的连续性，并据此与云服务提供者约定风险的评估指标和监控指标。

b） 云服务提供者负责：

1） 定义有关云服务业务连续性的信息，并将这些信息通过产品文档、服务等级协议等形式提供给客户，供客户在实现业务系统的连续性计划时参考。

2） 对所提供的云服务进行风险评估与持续监控，并根据GB/T 31168-2023要求保证云服务的业务连续性的要求，与云服务合作者约定风险的评估指标和监控指标。

3） 云服务合作者负责：在提供相关软件、硬件、服务时，应当定义有关软件、硬件、服务的业务连续性的信息，并将这些信息通过产品文档、服务等级协议等形式提供给云服务提供者、客户。支撑云服务业务连续性计划应满足与云服务提供者签署协议的要求。

5.5 协议约定

云服务各参与方所负责如下：

a） 客户负责：与云服务提供者通过签署合作协议的方式，根据合作方及合作情况约定各自应承担的安全责任内容和履约标准，且满足GB/T 31167-2023 7.3.2要求。

b） 云服务提供商负责：与云服务参与方通过签署合作协议的方式，明确各参与方针对漏洞修复、处置安全事件、配合监管等安全责任的落地。

c） 软件提供者负责：通过与云服务提供者签署合作协议的方式，明确产品功能、产品漏洞的通知方式和响应标准，提供软件安全云服务的周期和服务内容等。

d） 硬件提供者：通过与云服务提供者签署合作协议的方式，明确硬件产品的功能和质量保障。

e） 运维服务提供者：通过与云服务提供者签署合作协议的方式，明确提供运维服务的内容，以及提供运维服务的人员、服务流程、服务制度的标准，包括并不限于对运维服务提供者的授权范围、对运维变更决策的交互方式等。

f） 安全服务提供者：通过与云服务提供者签署合作协议的方式，明确安全服务提供的目的，涉及的安全产品、安全服务内容及提供标准等。

5.6 供应链安全

客户与云服务提供者、云服务合作者的供应链安全责任划分如下。

a） 客户负责：

1） 对云上业务系统提供保护，根据安全要求选择云服务提供者、云服务合作者，并对云服务提供者是否符合约定要求进行监督和管理。

2） 在合作协议中明确安全控制要求。

3） 基于法律法规和国家强制性标准对供应链有额外要求的，应当明确告知云服务提供者、云服务合作者。

b） 云服务提供者负责：

1） 在开发、建设云计算平台时应对软件提供者提出整体安全要求，确保软件提供者能够满足云服务提供者对云平台提出的安全需求。

2) 应在选购产品前，按需对采购的关键设备进行选型测试，针对云平台关键组件制定组件替换方案。
3) 当云服务提供商采购软件、硬件、运维服务、安全服务时，宜向供应商明确信息安全目标，要求每个供应商进行风险管理，通过协议等方式确保供应商具备软件供应链风险信息共享的安全措施。
4) 为客户提供安全措施的文档和信息，配合客户完成对云计算平台和业务系统的管理。

c) 云服务合作者负责：
1) 在合作开展前，确定客户、云服务提供者对供应链安全管理的要求，确保自身能够满足。
2) 根据与客户、云服务提供者签署的合作协议，履行供应链安全相关义务，配合运行监管。
3) 发现自身产品、服务存在漏洞、安全缺陷的，应当及时告知受影响的客户、云服务提供者，并采取必要措施，防范风险。
4) 云服务合作方可在合作协议中说明以下信息及不当使用时造成的风险：
- 提供的产品；
- 服务的研发；
- 提供目的及功能；
- 内容。

6 基础设施层安全责任划分与实施

6.1 开发与建设阶段

6.1.1 机房选址与建设安全

客户与云服务提供者、硬件提供者的机房选址和建设安全责任划分如下。

a) 客户负责：根据对业务系统的定级，确保选择符合自身安全要求的云服务节点，包括节点对安全管理的要求、数据存储的地理位置要求、数量要求、备份要求的满足情况等。

b) 云服务提供者负责：
1) 向客户明确云服务节点的基本情况。
2) 根据对云服务业务的定级，参考GB/T 31168-2023 16.1及16.2明确机房的技术要求和安全管理要求，如云平台软件由第三方提供的，应与软件提供者确定云平台软件正常运行所需要的机房要求，据此选择负责提供机房的硬件提供者并进行验收、管理。

c) 硬件提供者负责：
1) 确保机房的选址、设计、供电、消防、温湿度控制等符合相关标准和云服务提供者的要求，并支持机房通过云服务提供者的验收。
3) 确保机房具备物理安全隔离管控能力，包括以保护硬件资产及其运维正常运行为目的，为机房、库房、办公等区域配有安防门禁和监控设施，限制各类人员与运行中的设备进行物理接触，并按照云服务提供者提出的交付要求进行交付。

6.1.2 物理设备安全

客户与云服务提供者、硬件提供者的物理设备安全责任划分如下。

a) 客户负责：
1) 根据对业务系统的定级，确定云上系统所需要的性能型号，并据此选择云服务。
2) 对于物理设备的部署有特殊安全要求的（如需与服务其他客户的平台和系统区分开进行物理部署隔离的），客户应明确向云服务提供商提出要求。

b） 云服务提供者负责：

5） 在选购物理设备前，对关键设备进行选型测试，针对云平台关键组件制定组件替换方案。如云平台软件由第三方提供的，应与软件提供者确定设备的技术要求。

4） 采购的物理设备符合GB/T 31167-2023 6.3要求。基于法律法规和国家强制性标准对供应链有额外要求的，应当明确告知硬件提供者、运维服务合作者，并选择合适的安全服务提供者。

6） 云服务系统被认定为关键基础设施的，物理设备的采购应满足网络安全审查相关的要求，包括要求硬件提供者签署保密协议，采取供应链风险信息共享的安全措施。

c） 硬件提供者负责：

1） 按照与云服务提供者的协议约定提供物理设备，并宜在协议中对物理设备的功能、适用场景及使用不当时造成的风险进行说明。

2） 不得设置恶意程序，发现自身供应的硬件存在漏洞、安全缺陷的，应当及时告知受影响的云服务提供者。

6.1.3 网络搭建安全

该阶段客户与云服务提供者的物理网络搭建安全责任划分如下。

a） 客户通过搭建物理网络以部署云上系统的，客户向具备国内通信设施服务业务许可的运营商采买，并配合云服务提供者、硬件提供者完成专线部署进物理机房的手续。

b） 云服务提供者负责：

1） 自行或委托云服务合作者搭建物理网络，并负责采用结构化设计等方法在物理边界上进行监视、控制和网络通信防护，有效保护物理网络的安全性。

2） 在网络搭建时，应考虑足够支撑平台层的安全要求，包括云平台不同用户之间、业务网与管理网之间采取有效的网络安全隔离措施，为每个用户分配独立的虚拟私有网络的隔离要求。

6.2 运行阶段

客户与云服务提供者、运维服务提供者的物理环境访问控制安全责任划分如下。

a） 当客户自行负责机房管理时，客户与云服务提供者、云服务合作者明确机房物理环境的访问控制要求，宜确保机房的访问控制同时满足云服务运行和自身安全管控的要求。

b） 云服务提供者自行或委托运维服务提供者负责对机房物理环境进行访问控制，访问控制应满足GB/T 31168 16.4要求。

c） 硬件提供者：在规定或者与云服务提供者约定的期限内，不得终止提供安全维护。

d） 当运维服务提供者负责机房管理、云服务提供者负责设备管理时，云服务提供者需与运维服务提供者就物理设备的管理边界进行具体约定，包括：

1） 机房管理权限与物理设备管理权限的管理系统、审批权限归属，审批流程设置。

2） 云服务提供者对运维指令、运维标准的下发渠道和运维服务提供者的响应方式、时限。

3） 物理设备上下架的流程及保障。

6.3 迁移与退出阶段

云服务提供者与硬件提供者的迁移和推出责任划分如下：

云服务提供者应当与硬件提供者约定物理设备数据的清除责任方及数据擦除的标准，确保实例服务器释放后，其原有的存储介质将会被执行数据擦除操作，保障用户数据的安全。

7 平台层安全责任划分与实施

7.1 开发与建设阶段

7.1.1 云平台研发与规划安全

云服务提供者与软件提供者的云平台研发和规划安全责任划分如下。

a) 云服务提供者负责自行或通过采购符合要求的云平台软件、硬件，实现：
   1) 计算隔离：管理系统与客户虚拟机，以及客户虚拟机之间互相隔离。
   2) 网络隔离：每个虚拟网络与其他网络之间互相隔离。
   3) 存储隔离：计算与存储分离，虚拟机只能访问分配好的物理磁盘空间。
   4) 确保云平台软件的功能满足使用和管理需求。
   5) 确保云平台软件许可期间覆盖云服务业务经营期间，以保障软件/系统的稳定性和业务的连续性。
   6) 了解云平台软件的软件运维周期和当前状态，及时做好业务规划。如软件提供者约定的运维周期终止，并提供了替代方案（包括但不限于将软件更新到指定版本、更换替代软件），云服务提供者应当在软件的运维周期终止前明确替代方案或相关的风险应对方案。

b) 软件提供者负责：
   1) 制定安全开发管理制度以及软件的文档说明，提供配置管理、访问控制、运行维护等的工具或功能，配合客户对本项目平台和业务系统的管理。
   2) 确保软件功能提供云上账号的管理能力和云服务的访问服务，包括但不限于云平台主、子账号管理、登录的多因素认证机制、细粒度的访问授权能力，以及通过安全方式访问云平台的服务等。
   3) 在云平台的软件生命周期内，按照约定的云平台SLA确保功能的稳定运行。
   4) 明确说明云平台软件的软件运维周期，或者提供获取软件生命周期的渠道或方式，并在软件运维期间即将结束时，宜通过合理方式告知云服务提供者。
   5) 宜围绕产品能力、服务内容为云服务提供者提供必要、合理的培训。

7.1.2 云平台配置安全

云服务提供者与软件提供者的云平台配置安全责任划分如下。

a) 云服务提供者负责安全责任包括：
   1) 准确理解、使用云平台软件以搭建云计算平台，为云平台软件提供符合使用说明的运行环境，对云平台软件进行配置管理，在系统生命周期内建立和维护云平台 (包括硬件、软件、文档等)的基线配置和详细清单，并设置和实现云平台中各类产品的安全配置参数。
   2) 身份识别和访问管理安全。包括在允许人员、进程、设备访问本项目的设备、网络、系统、应用之前，应对其进行身份标识及鉴别，并以最小特权为原则，限制其可执行的操作和使用的功能。

b) 软件提供者负责:通过产品文档、合作协议等方式，向云服务提供者说明云平台软件的功能、服务等级和出厂基础配置，并说明为达到云平台软件服务等级所需要的硬件、物理环境、网络环境等基础条件。

7.1.3 虚拟网络系统通信安全

云服务提供者与软件提供者、硬件提供者的虚拟网络系统通信安全责任划分如下。

a) 云服务提供者负责：

1） 保障云平台不同租户之间、同一租户的不同业务系统之间、业务网与管理网之间采取有效的网络安全隔离措施，为每个租户或业务系统分配独立的虚拟私有网络。

2） 确保云平台软件具备容灾恢复能力， 建立必要的备份与恢复设施和机制，支撑客户业务的连续性计划。

b） 软件提供者负责：

1） 对云平台软件所提供的虚拟网络系统通信组建功能在技术允许范围内进行准确描述，并按照合作协议约定提供服务。

2） 宜围绕产品能力、服务内容为云服务提供者提供必要、合理的培训。

c） 硬件提供者负责：

1） 确保硬件符合合作协议的约定及国家强制性标准的要求。

2） 宜围绕产品能力、服务内容为云服务提供者提供必要、合理的培训。

7.2 运行阶段

7.2.1 云平台访问控制

客户和云服务提供者的云平台访问控制安全责任划分如下。

a） 客户负责：

1） 自身登录云平台账户的账密、口令等身份认证信息的安全配置；

2） 使用适当的身份验证技术提升特权账号的管理（例如多因素身份验证），加强对自身云服务管理人员的权限认证。

b） 云服务提供者负责：

1） 对云计算平台进行配置管理，在系统生命周期内建立和维护云平台（包括硬件、软件、文档等)的基线配置和详细清单，并设置和实现云平台中各类产品的安全配置参数。

2） 对云平台设置身份识别和访问管理的能力。包括在允许人员、进程、设备访问本项目的设备、网络、系统、应用之前，需要对其进行身份标识及鉴别，并以最小特权为原则，限制其可执行的操作和使用的功能。

3） 根据客户的请求对云资源本身进行开通、分配和关闭。

c） 软件提供者提供的云平台软件，需从产品功能上确保云平台能够按照客户设置的的访问控制规则的生效，为云平台访问控制功能的使用提供答疑等服务。

d） 运维服务提供者负责基于运维服务实现的目的，管控自身员工掌控的云平台访问控制权限，对于获得云平台访问、控制等权限的账户按照最小必要的原则进行申请，并需要获得云服务提供者的审批、授权。

e） 安全服务提供者，围绕客户/云服务提供者的需求提供访问控制的安全加固软件、硬件、服务，并确保其按照合作协议的说明发挥作用。

7.2.2 云平台运维安全责任

云服务提供者与软件提供者、运维服务提供者、安全服务提供者的云平台运维安全责任划分如下。

a） 云服务提供者负责：

1） 关注软件提供者或其他第三方共享的风险威胁信息，根据云平台软件出现的问题进行软件功能升级、漏洞修复或版本迭代，并落实解决措施。

2） 云服务提供者需要基于自身的应用场景和安全管理策略的需求，设立安全基线、完善安全计划和投入安全资源、建设安全措施以确保云平台软件的正常运行。

3） 聘请运维服务提供者、安全服务提供者提供运维服务的，宜明确不同服务提供者的服务定义、服务目标、服务内容说明、服务形式、服务等级，并制定服务过程中的风控制措施。

b) 软件提供者负责：

1) 在法定或约定的运维期间内提供约定的软件技术服务，为云服务提供者使用云平台提供必要的技术支持。

2) 根据合作协议约定提供软件的更新、迭代服务，对风险威胁提供解决方案或替代方案的建议。

c) 运维服务提供者、安全服务提供者负责

1) 按照合作协议约定的服务定义、服务目标、服务内容说明、服务形式、服务等级提供服务；

2) 为提供服务而获得的授权，不得超出提供服务范围进行使用，并通过制度和内部权限管理流程，确保内部人员以最小必要为原则使用云服务提供者赋予的授权；

7.2.3 应急响应

该阶段客户和云服务提供者、运维服务提供者、安全服务提供者的应急响应安全责任划分如下。

a) 客户负责：

1) 要求云服务提供商提供有关可能影响所提供的云服务的技术漏洞管理的信息。

2) 负责识别云上业务系统的漏洞，并及时进行修复。

3) 收集云服务提供者、云服务合作方及其他第三方共享的安全威胁信息，并评估风险和影响，采取必要措施进行应对。

b) 云服务提供者负责

1) 收集云服务合作方及其他第三方共享的安全威胁信息，并评估风险和影响，采取必要措施进行应对。

2) 对云服务可能面临的安全威胁类型、认定标准、处置措施采取的一版规则进行明确，并在发现、知悉安全威胁后按照法律法规的要求告知受影响的云客户，报送监管，履行网络运营者的职责。

3) 自行或委托安全服务提供者制定应急响应的规划，协调资源组织应急响应演练，确保应急响应方案的落地。

c) 运维服务提供者负责与云服务提供者就故障、漏洞类型及其相应标准进行明确约定。

d) 安全服务提供者负责根据客户提出的安全要求，制定应急响应的规划，支持客户调度资源进行应急响应。

7.2.4 数据安全

客户和云服务提供者、运维服务提供者、安全服务提供者的数据安全责任划分如下。

a) 客户对使用云服务生成、加工、存储、上传、下载、分发以及通过其他方式处理的数据负责，承担数据处理者的安全责任，包括：

1) 负责数据分类分级；

2) 负责数据全生命流程安全治理：明确数据在收集、存储、处理、披露和公开各环节的安全治理目标，并采取相应的数据安全管理措施。例如，如果客户使用云服务提供商、软件服务提供商提供的备份功能，应仔细阅读文档说明，明确并验证备份功能的规格是否符合客户自身的备份要求。如不符合要求时，客户应负责自行实施备份功能。

3) 负责数据安全风险的检测、评估、应急处置；

4) 负责识别和遵从行业领域的数据安全标准；

5) 在委托云服务提供者、云服务合作者处理数据时，宜通过签署数据处理委托协议的方式明确具体需要云服务提供者、云服务合作者采取的数据管理动作和数据安全措施。

b） 云服务提供者对云平台本身在建设、运行过程中产生、收集的，并能以自身意志决定其处理方式和目的的数据负责，同时基于与客户签署的数据处理委托协议对客户负责的数据采取数据安全管理或数据安全措施。

c） 软件提供者、运维服务提供者、安全运维服务提供者对于提供服务过程中所接触到的数据，需要按照与客户/云服务提供者签署的数据处理委托协议对客户负责的数据采取数据安全管理或数据安全措施。未经客户/云服务提供者同意的，不得将所接触到的数据用于提供服务以外的目的。

7.2.5 运维审计

客户和云服务提供者的运维审计责任划分如下。

a） 客户应当负责自身云上业务系统的运维审计，监控自身的云服务运行安全性、稳定性，包括：

1） 定义其事件日志记录的要求，并验证云服务是否满足这些要求；

2） 实施日志记录功能，监控和检测其购买的云服务是否被用作攻击他人的平台；

b） 云服务提供商提供功能，使客户能够监控与其自身相关的云服务运营信息，包括：

1） 提供事件日志记录的功能数据是否从云服务中泄露。

2） 适当的访问控制功能。这些功能应仅能够访问云服务客户自己的云服务实例信息。

7.3 迁移与退出阶段

该阶段客户和云服务提供者、软件提供者的迁移与退出责任划分如下。

a） 客户负责及时维护资源的有效性。

b） 云服务提供者负责遵循合作协议中约定的的服务到期、欠费、提前终止情况下下双方对数据处理要求的约定，包括返还及删除数据，迁出数据的措施等。

c） 云服务提供者负责云上客户数据的销毁。与硬件提供者约定物理设备数据的清除责任方及数据擦除的标准，确保实例服务器释放后，其原有的存储介质将会被可靠地执行数据擦除操作以保障用户数据的安全。

d） 软件提供者负责明确软件的生命周期，并在软件生命周期结束后负责提供软件的升级方案，供云服务提供者、客户进行选用。

8 服务层安全责任划分与实施

8.1 开发与建设阶段

该阶段客户和云服务提供者、软件提供者的应用研发和规划安全责任划分如下。

a） 客户负责：

1） 负责自身应用的研发、第三方应用的选用、部署。

2） 负责自身部署在云上的应用，及基于云服务提供者的产品搭建的应用系统的研发与规划安全。

3） 了解所购买产品的使用说明、安全配置，理解并遵守相关的使用限制，并根据业务的安全需求进行应用、应用系统的研发与规划。

b） 云服务提供者负责所提供云产品的研发与规划安全:

1） 对于IaaS层云产品，云服务提供商负责提供云上账号的管理能力和云服务的访问服务，并负责提供各类权限管理工具帮助客户加强对业务的管理，包括但不局限于提供云平台主子账号管理、登录的多因素认证机制、细粒度的访问授权能力，以及通过安全方式访问云平台的服务等。

2) 对于PaaS层云产品，云服务提供者宜对操作系统管控面的组件配置和镜像进行安全加固，保障PaaS层组件安全漏洞的识别、告知，以及修复、替代方案的提供。
3) 对于SaaS层云产品，云服务提供者应负责SaaS产品安全合规使用，应对该层面脆弱性或安全漏洞被恶意人员利用攻击平台的情况等负责。
4) 对于客户自行选用的第三方软件，云服务商宜提供第三方与云平台适配的咨询，但不负责第三方软件的配置指导以及故障排查，以及安装、补丁更新、测试、故障诊断、优化等日常运维服务。

8.2 运行阶段

客户和云服务提供者、软件提供者的运行阶段责任划分如下。

a) 客户负责
1) 应用的安全防护、安全巡检，云产品内的安全策略配置和更新，指云产品账号管理、访问授权、权限配置等安全策略配置。
2) 密码安全策略的制定和执行，指密码创建、修改时，有复杂度、更换周期等安全策略。
3) 行为日志功能的配置和使用，指对账号使用记录、操作记录等内容进行记录、分析和审计。
4) 基于云服务提供者的公告和提供的补丁或版本升级方式及时进行云产品、组件等漏洞的修复和版本更新。

b) 云服务提供者主要负责云产品在运行过程中按照合作协议约定的标准提供服务，并可根据云上应用生命周期中安全防护的典型场景为云客户提供最佳实践指导。

8.3 迁移与退出阶段

该阶段客户和云服务提供者、软件提供者的迁移与退出阶段的安全责任划分如下。

a) 客户负责：对使用云服务生成、加工、存储、上传、下载、分发以及通过其他方式处理的数据，负责决定其存储、销毁、删除计划，并据此安排匹配相关的云资源。

b) 云服务提供者：在合同约定服务期间和数据保留的过渡期结束后，云服务提供者应负责确保客户存储在云上的数据会被安全地销毁或删除。

附 录 A
（资料性）
责任角色认定案例

D

在云计算服务过程中，云服务提供者有可能是单一的主体，也可能与其他主体合作为客户提供云计算服务。本文件将典型案例分为单一云服务提供者场景、社区云模式下的联合云服务提供者场景、公共云模式下的联合云服务提供者场景来介绍各责任角色的认定。

A.1 单一云服务提供者情况下的责任角色认定案例

单一云服务提供者情况下，云服务各参与方之间的合作关系如图3 单一云服务提供者情况下的云服务参与方合作关系图所示：

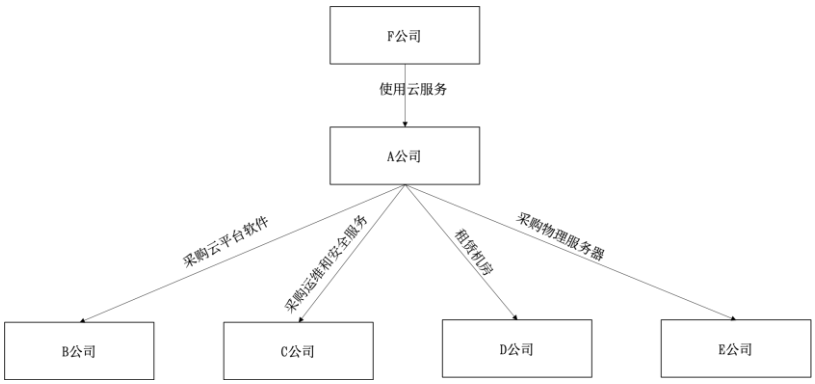

图3 单一云服务提供者情况下的云服务参与方合作关系图

A公司拟建设云系统，向B公司采购云平台软件、向C公司采购运维和安全服务，向D公司租赁机房，向E公司采购物理服务器。责任角色认定参考表1 单一云服务提供者情况下的责任认定案例。

表 1 单一云服务提供者情况下的责任认定案例

主体	行为	责任角色
A 公司	● 提供云服务：使用电信资源，确认实际云资源使用请求。 ● 选择云平台软件：决定选用 B 公司的云平台软件。 ● 管理云平台运维：与 C 公司签署运维服务协议，审批 C 公司的运维变更需求。 ● 控制底层硬件：决定向 D、E 公司采购底层硬件并拥有使用权。 ● 决定云服务安全能力：决定安全策略，决定选择 C 公司作为安全服务提供商。	云服务提供者
B 公司	● 提供云平台软件：决定云平台软件产品的代码、能力支持、代码发布、软件补丁。确定产品的安全维护期限，基于软件功能提供维护支持。	软件提供者
C 公司	● 提供运维服务：根据授权按照标准执行运维动作，向云服务提供者提交运维变更申请。	运维服务提供者

	● 提供安全服务：提供安全方案、安全软硬件、安全服务人员。	安全服务提供商
D 公司	● 提供物理机房。	硬件提供者
E 公司	● 提供物理服务器。	硬件提供者
F 公司	● 使用云服务	客户

A.2 联合云服务提供者（社区云模式）情况下的责任认定案例

联合云服务提供者（社区云模式）情况下，云服务各参与方之间的合作关系如图4 联合云服务提供者（社区云模式）情况下的云服务参与方合作关系图所示：

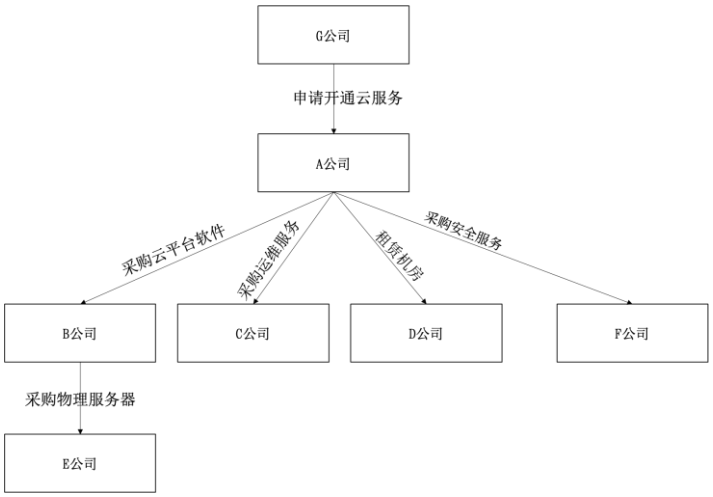

图4 联合云服务提供者（社区云模式）情况下的云服务参与方合作关系图

A公司是集团公司，旗下有若干个独立运营的子公司（统称为“G公司”），A公司拟建设集团共同使用的云系统供G公司使用。

- A公司提供电信资源并决定使用B公司的云平台软件。A公司决定由C公司提供运维服务。A公司决定向D租赁机房，决定F公司提供安全服务。
- B公司向E公司采购物理服务器，并拥有物理服务器资产的归属权和使用权（对于已经搭载云平台软件的物理服务器，未经B公司许可A公司不得访问），并在物理服务器上部署A公司选择的云平台软件。
- G公司向A公司申请开通云服务，A公司提供云服务实例。

云服务合作者责任角色认定参考表2 联合云服务提供者（社区云模式）情况下的责任认定案例。

表 2 联合云服务提供者（社区云模式）情况下的责任认定案例

主体	行为	责任角色
A 公司	● 提供云服务：使用电信资源，确认实际云资源使用请求。 ● 选择云平台软件：决定选用 B 公司的云平台软件。 ● 管理云平台运维：与 C 公司签署运维服务协议，审批 C 公司的运维变更需求。	云服务提供者(联合)

	● 决定云服务安全能力：决定选择 F 公司作为安全服务提供商，并决定安全策略。	
B 公司	● 控制底层硬件：拥有底层硬件的归属权和使用权。	云服务提供者（联合）
	● 提供云平台软件：决定云平台软件产品的代码、能力支持、代码发布、软件补丁。确定产品的安全维护期限，基于软件功能提供维护支持。	软件提供者
C 公司	● 提供运维服务：根据授权按照标准执行运维动作，向 A 公司提交运维变更申请。	运维服务提供者
D 公司	● 提供物理机房。	硬件提供者
E 公司	● 提供物理服务器。	硬件提供者
F 公司	● 提供安全服务：提供安全方案、安全软硬件、安全服务人员。	安全服务提供商
G 公司	● 使用云服务。	客户

A.3 联合云服务提供者（公有云模式）情况下的责任认定案例

联合云服务提供者（公有云模式）情况下，云服务各参与方之间的合作关系如图5 联合云服务提供者（公有云模式）情况下的云服务参与方合作关系图所示：

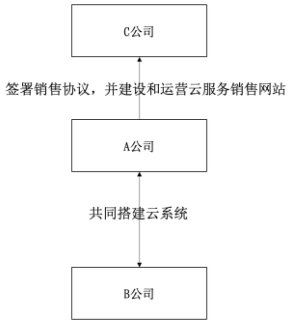

图5 联合云服务提供者（公有云模式）情况下的云服务参与方合作关系

A公司拥有电信资源、物理机房，B公司拥有云平台软件。

A公司与B公司共同搭建云系统，由A公司面向C公司签署销售协议，并建设和运营云服务的销售网站，A公司提供物理机房，拥有物理服务器资产所有权。

B公司提供云平台软件和运营云平台，并对底层物理服务器有使用权（即未经B公司许可A公司不得访问）。B公司通过接口向A公司提供可调用的云服务。

表 3 联合云服务提供者（公共云模式）情况下的责任认定案例

主体	行为	责任角色
A 公司	● 提供云服务：使用电信资源，面向 G 公司签署销售协议。 ● 选择云平台软件：决定选用 B 公司的云平台软件。 ● 管理云平台运维：负责云服务销售网站对 B 公司云服务接口调用的运维。 ● 控制底层硬件：对物理机房有控制权，B 公司增加减少物理服务器需经 A	云服务提供者（联合）

	公司同意。 ● 决定云服务安全能力：决定选择 B 公司作为安全服务提供商，并决定云服务销售网站的安全策略。	
	● 提供运维服务：根据授权按照标准执行云销售网站的运维动作，向 A 公司提交运维变更申请。	运维服务提供者
	● 提供物理机房和物理服务器。	硬件提供者
B 公司	● 管理云平台运维：决定云平台软件的运维变更需求。 ● 控制底层硬件：拥有底层硬件的使用权。 ● 决定云服务的安全能力：决定云平台软件侧的安全方案。	云服务提供者（联合）
	● 提供云平台软件：决定云平台软件产品的代码、能力支持、代码发布、软件补丁。确定产品的安全维护期限，基于软件功能提供维护支持。	软件提供者
	● 提供运维服务：根据授权按照标准执行云平台软件的运维动作，向 A 公司提交运维变更申请。	运维服务提供者
	● 提供安全服务：提供安全方案、安全软硬件、安全服务人员。	安全服务提供者
C 公司	● 使用云服务	云服务客户

附 录 B
（资料性）
典型的安全责任划分案例

云计算服务典型的安全责任事件及责任划分可参考表4云计算服务典型安全责任事件及责任划分表。

表 4 云计算服务典型安全责任事件及责任划分表

序号	分类	典型事件	客户	云服务提供者	软件提供者	硬件提供者	运维服务提供者	安全服务提供者
1.	通用 -安全组织及人员	未设置符合要求的安全组织和人员，导致云服务的选择和使用不符合经营合规要求。	✓					
2.		未设置符合要求的安全组织和人员，导致对软件、硬件、运维服务、安全服务的选择和使用不符合经营合规要求。		✓				
3.		未设置符合要求的安全组织和人员，导致对软件、硬件、运维服务、安全服务的提供不符合与云服务提供者协议的约定。			✓	✓	✓	✓
4.	基础设施层 -机房选址及建设安全	云服务节点选择不当或节点采购无法满足数据备份要求。	✓					
5.		未按照 GB/T 31168-2023 16.1 及 16.2 明确的技术要求和安全管理要求选择、验收、管理硬件提供者。		✓				
6.		未按照云服务提供者验收后的标准持续交付机房。				✓		

7.	基础设施层 -物理设备安全	未按业务系统定级选择、验收、使用云服务，或未向云服务提供者明确特殊安全要求导致的安全问题。	✓					
8.		未向硬件提供者明确云平台正常运行所需的技术要求，或未按硬件提供的功能、适用场景使用物理设备而导致的安全问题。		✓				
9.		因物理设备存在恶意程序，或硬件提供者未及时告知已识别漏洞或安全缺陷而导致的问题。				✓		
10.	平台层 -云平台研发与规划	云平台研发与规划过程中，未选择符合 GB/T 31168-2023 要求的云平台软件、硬件，而导致云平台发生安全事件的。		✓				
11.		云平台研发与规划中，对产品软件功能进行虚假描述，或产品软件功能不满足 GB/T 31168-2023 技术要求而导致云平台发生安全事件的。			✓			
12.	平台层 -云平台配置	云平台配置过程中，未设置具备安全能力的人员/组织对云平台软件进行配置管理，导致云平台软件操作不当、配置不当而引发安全风险的。		✓				
13.		云平台运行过程中，对已发现云平台软件漏洞未及时通报云服务提供者，而引发安全风险的。			✓			

14.	服务层	因客户维护不当或加密不当致使口令、密码等丢失或泄漏所引起的损失和后果。	✓					
15.		未及时响应及处置云服务提供者或其他第三方通报的网络安全风险。	✓					
16.		应用层的行为日志功能的配置和使用不足，导致安全风险爆发后无法溯源的。	✓					

参 考 文 献

[1] ISO 27017:2015 Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services