云计算服务中的安全风险如何管理？
《信息安全技术-云计算服务安全指南》（征求意见稿）内容简介

2020 年 1 月 20 日，全国信息安全标准化技术委员会（“全国信安标委”）发布了《信息安全技术 云计算服务安全指南》征求意见稿（“《安全指南》”）。《安全指南》聚焦于云计算服务采购和使用中的安全问题，提出了党政机关及关键信息基础设施运营者采用云计算服务的安全管理基本要求，明确了采用云计算服务的生命周期各阶段的安全管理和技术措施。

《安全指南》下的标准属于推荐性国家标准，不具有强制性效力，适用对象面向党政机关及关键信息基础设施运营者（在《安全指南》中被称为“客户”，为了便于介绍，本文将沿用这一概念）。但对于其他已经使用或打算使用云计算服务的企业而言，《安全指南》对于如何建立有关云计算服务采购和使用中的安全管理标准、要求、措施和制度，也有较大参考价值。本文将对《安全指南》的关键内容进行简要介绍，供读者参考。

云计算服务面临的安全风险有哪些？

要解决云计算服务采购和使用中的安全问题，首先需要明确云计算面临的主要安全风险。《安全指南》首先在第 5.2 条从客户的角度列举和说明了云计算服务可能面临的七处安全风险：

(1) 客户对数据和业务系统的控制能力减弱;

(2) 客户与云服务商之间的责任难以界定；

(3) 因数据存储位置导致可能产生的司法管辖权问题；

(4) 数据所有权保障面临风险；

(5) 数据保护更加困难；

(6) 客户退出后的数据残留；

(7) 客户容易产生对云服务商的过度依赖。

云计算服务安全管理中有哪些主要角色？

《安全指南》第 5.3 条明确了云计算服务安全管理的四类主要角色及其责任。这四类主要角色包括：云服务商、客户、云服务安全提供商和第三方评估机构。其中，云服务商、

客户和云服务安全提供商主要负责云计算服务实际开展过程中的安全管理责任；第三方评估机构对云服务商及其提供的云计算服务开展独立的安全评估。此外，《安全指南》还提出，客户需承担部署或迁移到云计算平台上的数据和业务的最终安全责任。

云服务商和客户的安全责任如何划分？

就云服务商和客户在安全方面的具体责任划分，《安全指南》从原则到细则，规定了一套划分标准和责任边界。

在《安全指南》第 5.4 条概括性地规定了责任划分原则。《安全指南》提出，由于云服务商和客户的控制范围有所不同，因此云服务商和客户需要共同判断哪个角色在实施安全措施方面具有相对有利地位，由处于有利地位的角色承担相应安全责任；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。此外，《安全指南》强调，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。

在明确责任划分原则之后，《安全指南》又通过多份附录图表的示例，细化了客户和云服务商之间安全责任划分的具体边界。首先，《安全指南》的附录 A 通过图例和表格明确了云服务商与客户的责任划分边界。

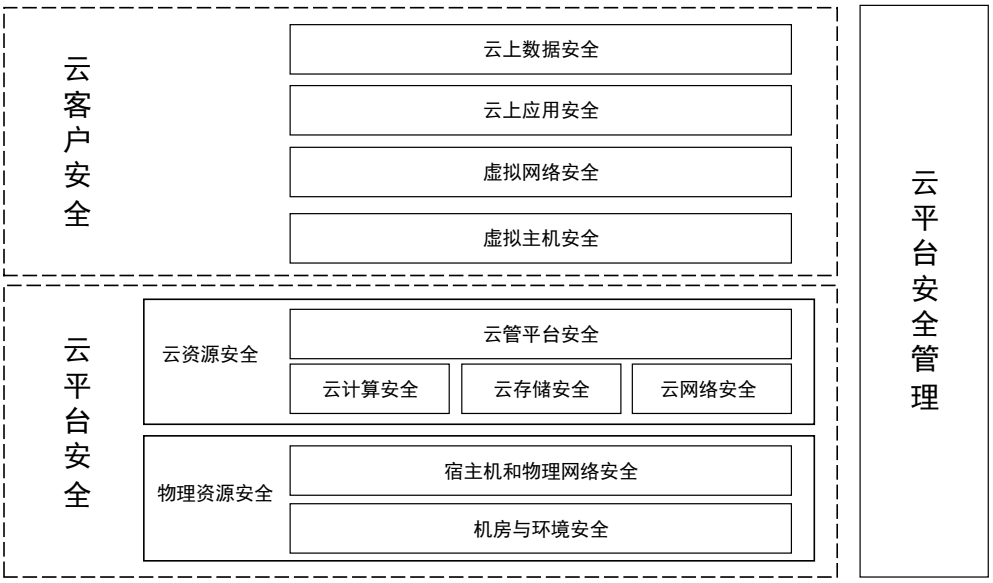

图 A2 云服务商与云客户责任划分边界[i]

单位	责任边界	说明
云服务商	设施层安全； 负责硬件层、资源抽象层、虚拟化技术资源层的安全。	包括机房采暖、通风、空调、电力和通信等机房基础设施的安全保障； 云服务商自身云平台组成的服务器、网络设备和安全设备等硬件层安全，及其云管理平台安全；

单位	责任边界	说明
		政务云平台网络边界的安全防护。
云上客户	负责自身部署系统的软件平台层、应用软件层安全和系统数据安全，实施对这些资源操作、更新、配置的安全可靠管理。	业务系统相关的安全责任，包括主机、应用和数据安全，如操作系统、数据库、中间件和应用系统的安全配置检查和加固，应用系统的升级维护和日常代码审计、渗透测试等，以及业务数据的加密和备份等。

表 A1 云服务商与云客户责任划分边界说明[ii]

其次，《安全指南》又进一步将应用能力类型、基础设施能力类型和平台能力类型[iii]三种不同的云能力类型下，云服务商与云客户的具体责任划分边界，以表格的方式进行了详细地说明。

《安全指南》中提供的责任划分原则和具体责任划分边界体系，对于各类云服务采购者和云服务提供商如何在其服务合同中明确双方的安全责任，提供了非常有意义的参考和指导。

云计算服务安全管理的基本要求有哪些？

针对云计算服务安全风险，《安全指南》第 5.5 条明确了云服务期间，客户和云服务安全管理应遵循的五项基本要求，包括：

(1) 安全管理责任不变，客户始终是信息安全的最终责任人。

(2) 资源的所有权不变。客户提供给云服务商的数据、设备等资源，以及云计算平台上客户业务系统运行过程中收集、产生、存储的数据和文档等都应属客户所有，客户对这些资源的访问、利用、支配等权利不受限制。

(3) 司法管辖关系不变。除非中国法律法规有明确规定，云服务商不得依据其他国家的法律和司法要求将客户数据及相关信息提供给他国政府及组织。

(4) 安全管理水平不变。云计算平台和提供云计算服务的云服务商应当遵守政府信息系统安全管理要求、政策及标准。

(5) 坚持先评后用原则，云服务商应当通过安全评估。

如何确定数据的安全保护要求？

《安全指南》强调，在采购云计算服务之前，应做好规划。规划阶段的重要工作之一，是根据客户部署在云计算平台的信息类型和其自身承载业务的重要程度，确定安全保护的要求，进而根据安全保护要求再选择合适的云计算服务和部署模式。

信息类型及安全保护要求

《安全指南》根据是否涉密将信息划分为涉密信息和非涉密政府信息。涉密信息的处理、保存、传输、利用按国家保密法规执行。就非涉密政府信息而言，《安全指南》根据信息的重要程度进一步划分为敏感类信息（如个人信息和重要数据）和公开类信息（如行政法规）。值得注意的是，《安全指南》根据云服务业务可能涉及的信息内容，广泛地列举了敏感类信息的范围，除了个人信息和重要数据外，还包括企业商业秘密和知识产权中不宜公开的信息等；这与目前数据保护的立法体系一致。根据《安全指南》，不同信息类型对应的安全保护要求如下表所示：

信息类型		安全保护要求
涉密信息		按国家保密法执行。
非涉密信息	敏感类信息	防止未经授权披露、丢失、滥用、篡改和销毁。
	公开类信息	防止篡改和丢失。

业务类型及安全保护要求

在确定了信息类型后，还需要对承载相关信息的业务进行分类。《安全指南》根据客户承载信息的业务不能正常开展时可能造成的影响范围和程度，将业务分为一般业务、重要业务、关键业务三种类型，并明确了三种业务类型的认定标准。由于不同业务类型下的不同信息类型对应的云服务安全保护能力要求不同，客户应当根据自身业务类型及涉及信息类型分别选择具备一般保护能力/增强保护能力/高级保护能力的云服务商，如下图 2 所示。

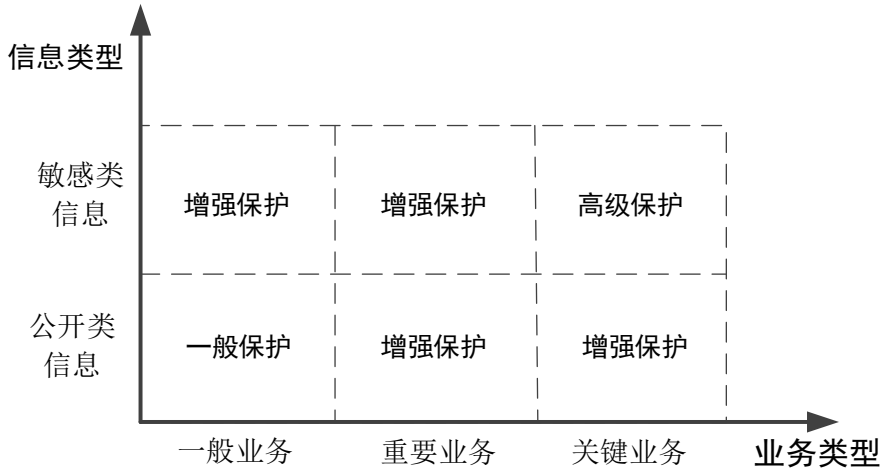

图 2：云服务商安全保护要求[iv]

在根据信息类型和业务类型确认相应的安全保护要求后，《安全指南》根据信息和业务的不同类型组合，对客户应当选择的云计算服务的安全能力提出了要求：

信息和业务类型	云服务的保护能力要求
承载公开类信息的一般业务	一般保护能力
▪ 承载敏感类信息的一般业务和重要业务 ▪ 承载公开类信息的重要业务和关键业务	增强保护能力
承载敏感类信息的关键业务	宜采用私有云或社区云，且达到高级保护能力

关于“一般保护能力”、“增强保护能力”和“高级保护能力”要求的具体指标要求，《安全指南》规定参见全国信安标委同日发布的配套标准《信息安全技术 云计算服务安全能力要求》（GB/T 31168-xxxx）（征求意见稿）。

使用云服务时需求分析不可少

除安全保护要求的分析和确定外，在规划阶段，《安全指南》另一个强调的重点是需要做好需求分析。根据征求意稿第 6.6 条的规定，客户应从 10 个方面对自己所需的云计算服务的需求进行分析，提出各项功能、性能及安全要求。该等需求主要从客户自身的业务特点以及不同云服务类型和部署模式的特点出发，其关键内容如下：

需求	考虑因素	建议或要求
服务类别	不同云服务类别下云服务商与客户的控制范围不同，例如： ▪ 在 SaaS 服务类别下，应用软件层的安全措施由客户和云服务商分担，其他安全措施由云服务商实施。 ▪ 在 PaaS 服务类别下，软件平台层的安全措施由客户和云服务商分担。客户负责自己开发和部署的应用及其运行环境的安全，其他安全措施由云服务商实施。 ▪ 在 IaaS 服务类别下，虚拟化计算资源层的安全措施由客户和云服务商分担。客户负责自己部署的操作系统、运行环境和应用的安全。云服务商负责虚拟机监视器及底层资源的安全。	客户可根据不同云服务类别的特点和自身数据及业务系统的安全管理要求，结合自身的技术能力、市场及技术成熟度等因素选择云服务类型。
部署模式 （典型模式：公有云、社区云和私有云）	▪ 是否与其他客户共享云计算平台。从公有云到社区云再到私有云，共享能力依次降低。 ▪ 对云计算平台管理技能的要求。若采用私有云、社区云，且云计算平台由客户承担管理任务，则需要客户具备专业的技术人才，对人员技能的要求远比公有云高。 ▪ 业务的可扩展性要求。公有云可扩展性相对较高；社区云和私有云的灵活程度会受到具体的部署	不同的部署模式下，云计算基础设施部署的场所、客户访问云计算服务的网络链路、是否与其他客户共享资源等属性有较大差异，客户需要综合分析部署模式对自身数据和业务的影响，选择适合的部署模式，使安全风险可控。

需求	考虑因素	建议或要求
	场所和策略的影响。	
功能需求的稳定性和通用性	当客户的业务功能需求不断变化时，云服务商需要不断开发、测试和部署新的组件；而云计算的多客户共享资源特点使得云计算平台基于客户的功能定制或变更较为困难，因此，云服务商通常愿意提供通用性较好、功能相对稳定和成熟的服务。	可优先迁移或部署功能需求不经常发生变化的业务。
资源的动态需求特点	有些业务具有临时、周期性特点，可能会出现访问和请求的突发高峰，要求可根据访问需求动态分配资源。此类业务采用云计算服务，可以满足动态、灵活的资源需求，且客户只需为业务系统所占用的资源支付使用费用。	优先迁移或部署资源有动态、周期变化需求的业务，可在满足业务性能需求的前提下节省资金。
时延	不同类型的应用对云计算服务的时延要求差异明显，例如，电子邮件通常容许出现短暂的服务中断和较大的网络时延，但自动化控制与实时应用一般都对时延要求较高。	应针对业务系统对响应速度方面的要求做详尽分析，确定业务本身对时延的容忍度，以及可能采取的补救措施等。
业务持续性	云计算服务是否会中断、是否能持续访问。	在采用云计算服务前，应对云计算服务的可靠性、持续性需求进行充分评估，应关注中断频率与预期恢复时间。
可移植性与互操作性	▪ 移植是指将数据和业务系统从一个云服务商迁移到另一个云服务商的云计算平台，或迁移回客户的数据中心。可移植性实现难度与采用的云计算服务类别有关，	应制定将数据和业务系统从某一云计算平台迁移到其他云计算平台或自有数据中心的计划，充分考虑云计算服务与其他已有或将来的业务系统集成

需求	考虑因素	建议或要求
	通常从 IaaS、PaaS 到 SaaS 可移植性的难度逐渐增加。 ▪ 部署在云计算平台上的业务系统可能需要与其他系统进行数据交互，不同云计算平台间及与自有信息系统之间的数据交换与访问目前还较为困难。同时，云服务商为了商业竞争的目的，对可移植性和互操作性支持一般不够积极。	需求。
数据的存储位置	▪ 云服务商可能会将数据中心分布在不同的地区，甚至不同的国家；云计算服务的运行管理对客户往往缺少透明性，客户难以掌握数据和副本在存储设备和数据中心的具体位置。 ▪ 根据国家的有关规定，存储、处理客户数据的数据中心和云计算基础设施不得设在境外。	因客户需求需要将数据中心和云计算基础设施设在境外的情况，应遵守相关法规和政策。
监督能力	客户对云计算平台中的数据没有直接的控制权。	客户应通过合同明确云服务商的责任和义务，强调客户对数据和业务系统运行状态的知情权；要求云计算平台提供必要的监管接口和日志查询功能，建立有效的评估、检查机制，实现对云计算服务的有效监管。

云服务商应当具备哪些安全能力要求？

《安全指南》第 7.1 条明确了为客户提供云计算服务的云服务商应具备 10 个方面的安全能力。根据该等安全能力的特征，我们将其分为四大类，主要包括：

(1) 技术安全能力：系统开发与供应链安全、系统与通信保护、访问控制、维护、配置管理；

(2) 制度与人员安全能力：审计、风险评估与持续监管、安全组织与人员；

(3) 应急安全能力：应急响应与灾备；以及

(4) 物理与环境保护能力等。

关于上述安全能力的技术标准与要求，《安全指南》规定参见全国信安标委同日发布的配套标准《信息安全技术 云计算服务安全能力要求》（GB/T 31168-xxxx）（征求意见稿）。

全生命周期管理

《安全指南》将云服务的生命周期划分为四个阶段：规划准备、选择服务商与部署、运行监管、退出服务；强调进行全生命周期安全管理；并对每个阶段的具体的安全管理要求作出了具体的规定。

总体而言，《安全指南》是一个推荐性的技术性规范，因此，并不会对现有的云计算服务的法律监管和实践带来直接影响。但其中的风险管理措施、安全责任和边界划分规则、安全要求和服务需求分析，以及其他思考和分析框架，对于企业采购和使用云计算服务的风控制度的建立和完善、云计算服务协议的规范和完善，以及私募投资活动中对云计算安全保护相关业务或模块的理解和分析，都有一定的参考价值。

◇◇◇◇

本文作者为柯杰律师事务所张方（合伙人）、陈佳莉对本文亦有贡献。

[i] 引自《信息安全技术 云计算服务安全指南》征求意见稿，附录 A，图 A2：云服务商与云客户责任划分边界。
[ii] 引自《信息安全技术 云计算服务安全指南》征求意见稿，附录 A，表 A1：云服务商与云客户责任划分边界说明。
[iii] 《安全指南》将云能力类型分为 3 类，应用能力类型、基础设施能力类型和平台能力类型。其中，应用能力类型是指，云服务客户能使用云服务商应用的一种云能力类型；基础设施能力类型是指，云服务客户能配置和使用计算、存储或网络资源的一类云能力类型；平台能力类型是指，云服务客户能使用云服务商支持的编程语言和执行环境来部署、管理和运行客户创建或获取的应用的一类云能力类型。《安全指南》特别指出，云能力类型不等于云服务类别，一种云服务类别能包含一种或多种云能力类型的能力。
[iv] 引自《信息安全技术 云计算服务安全指南》征求意见稿第 6.5 条所附图 2：安全保护要求。