NIST定义了三个服务模型，它们描述了云服务的不同基础类别:

服务即软件 (SaaS)是由服务商管理和托管的完整应用软件。用户可以通过web浏览器、移动应用或轻量级客户端应用来访问它。

平台即服务(PaaS)抽象并提供开发或应用平台,如数据库、应用平台(如运行Python、PHP或其它代码的地方),文件存储和协作,甚至专有的应用处理（例如机器学习、大数据处理或直接API访问完整的SaaS应用的特性)。关键的区别在于，使用PaaS，您不需要管理底层的服务器、网络或其他基础设施。

基础设施即服务(IaaS)提供了基础性的计算资源，如计算、网络或存储。

我们有时称它们为“SPI”模型。

云计算，抢走了运维的一部分活，变成一个收费服务。机器运行环境维护（网络，主机，机房安全，重要应用运行环境）。

商业：一种新型技术，

任何工作都是一个系统性的工作。

云环境责任范围划分 以及应急预案。

2.0

云计算的边界模糊。对于管理来说，统一管理最为有效与方便。但是对于业务，都是分开应用。

权限要求，共同分担。但是要有主次责任。（云提供商与企业，安全与业务）

责任划分，范围以及效力。云环境选择以及优劣。

3.0

法律，合同，以及信息资产风险处理。

法律合规性

监控

电子取证

4.0

GRC，即治理（Governance），风险（Risk）和合规性（Compliance）

5.0

数据生命周期控制。

6.0

云账户及权限管理。

运维，应用稳定性。各种组件，自己的APP。

业务架构 以及互相关联。

迁移，拓展，减少，了解应用配置，减少模块组件之间的耦合。（运维）

负载均衡器思想。集群思想。最终单点的东西使用云服务来做。

单点的东西都要有备份。

7.0

基础设施安全

云平台资质，能力，基础信誉，安全保障。服务持续可用性。

8.0

虚拟化稳定性，以及安全性。

用户：正确的使用安全功能。阿里云 内网规则0.0.0.0 问题

9.0

事件响应，应急响应。

运维，安全，对外宣传等方面都有这个情况。

事件响应生命周期

准备：“建立事件响应能力，使组织对事件响应作好充分准备”。

处理事件的流程。

通讯和设施的处理人员。

事件分析硬件和软件。

内部文档及数据（端口列表、资产清单、网络拓扑图、当前网络流量基线）。

确定相关培训。

评估基础设施（通过主动扫描和网络监控，漏洞评估和开展风险评估）。

订阅第三方威胁情报服务。

检测与分析

警报（端点保护、网络安全监控、主机监控、帐号创建、特权提升、其他入侵指标、SIEM、安全分析（基线和异常检测）和用户行为分析）。

验证警报信息（减少误报）和升级。

分析事件的范围。

分配一位事件经理（事件负责人），协调进一步行动。

指定一位人员，向高级管理层传达事件遏制和恢复状态。

建立攻击时间表。

分析潜在数据丢失的程度。

通知和协调活动。

遏制、根除和恢复

遏制：使系统脱机。权衡数据丢失与服务可用性。确保系统在检测到时不会自毁。

消除与恢复：清理受影响的设备并将系统恢复正常操作。确认系统运行恢复正常，实施措施以防止类似事件。

记录事件和收集证据（证据保管链）。

总结

哪些方面可以做得更好？能否更快地发现攻击？有什么额外的数据有助于更快地隔离攻击？事件响应流程需要改进吗？ 如果需要，如何改进？

10.0

应用安全

SDL

11.0

数据安全及加密

数据流程。

客户，app，网络，服务器，存储方式（数据库）。

加密：算法及密钥

业务共享与数据传输。

灾难阻止与恢复。

12.0

云控制台身份管理。

13.0

云安全服务

14.0

云计算 的发展方向，以及实现。