云环境下信息系统安全等级保护要求的探讨

公安部信息安全等级保护评估中心
中关村信息安全测评联盟
（2015年7月2日）

标准概况

GB/T 22239-201X

- 第一部分：信息系统安全等级保护基本要求
- 第二部分：云计算安全等级保护基本要求

GB/T 28448-201X

- 第一部分：信息系统安全等级保护测评要求
- 第二部分：云计算安全等级保护测评要求

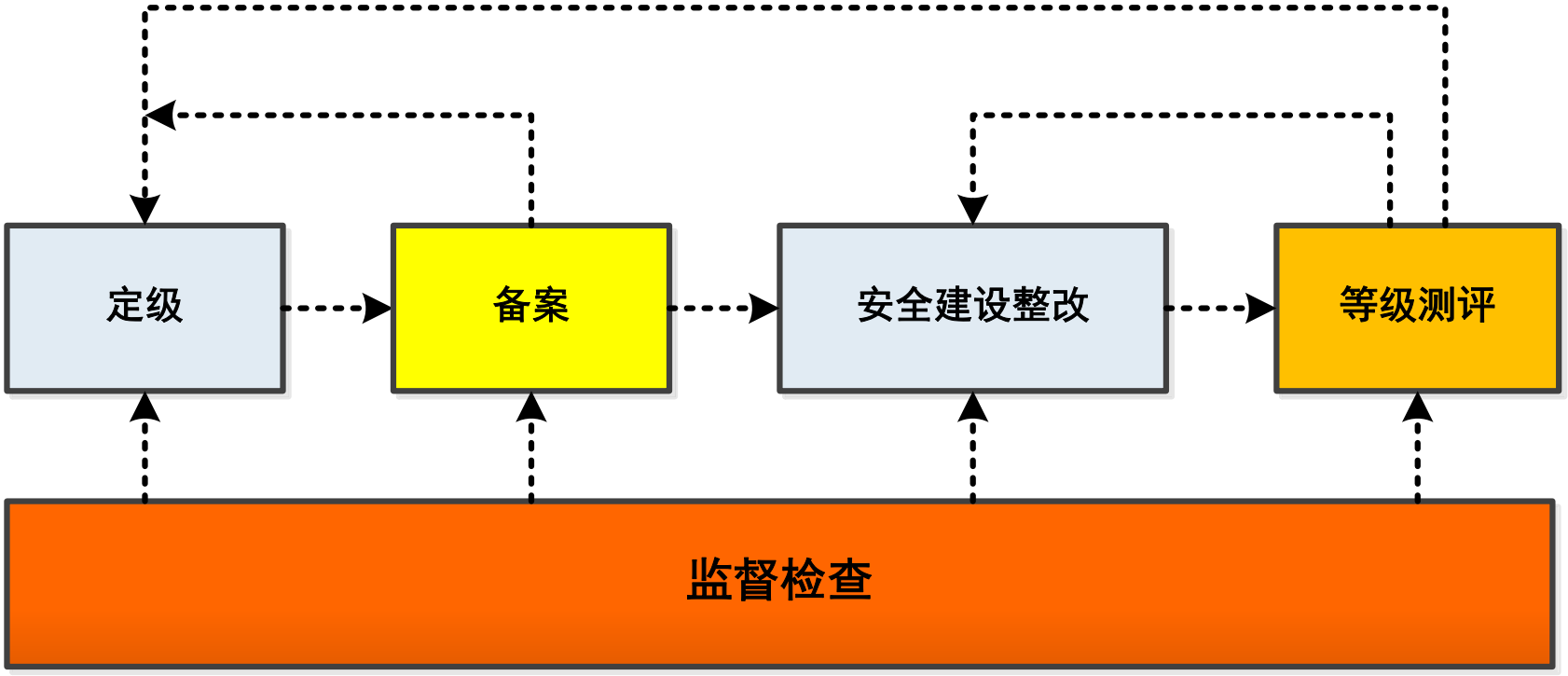
主要内容

对信息系统分等级实行安全保护

使用的信息安全产品实行分等级管理

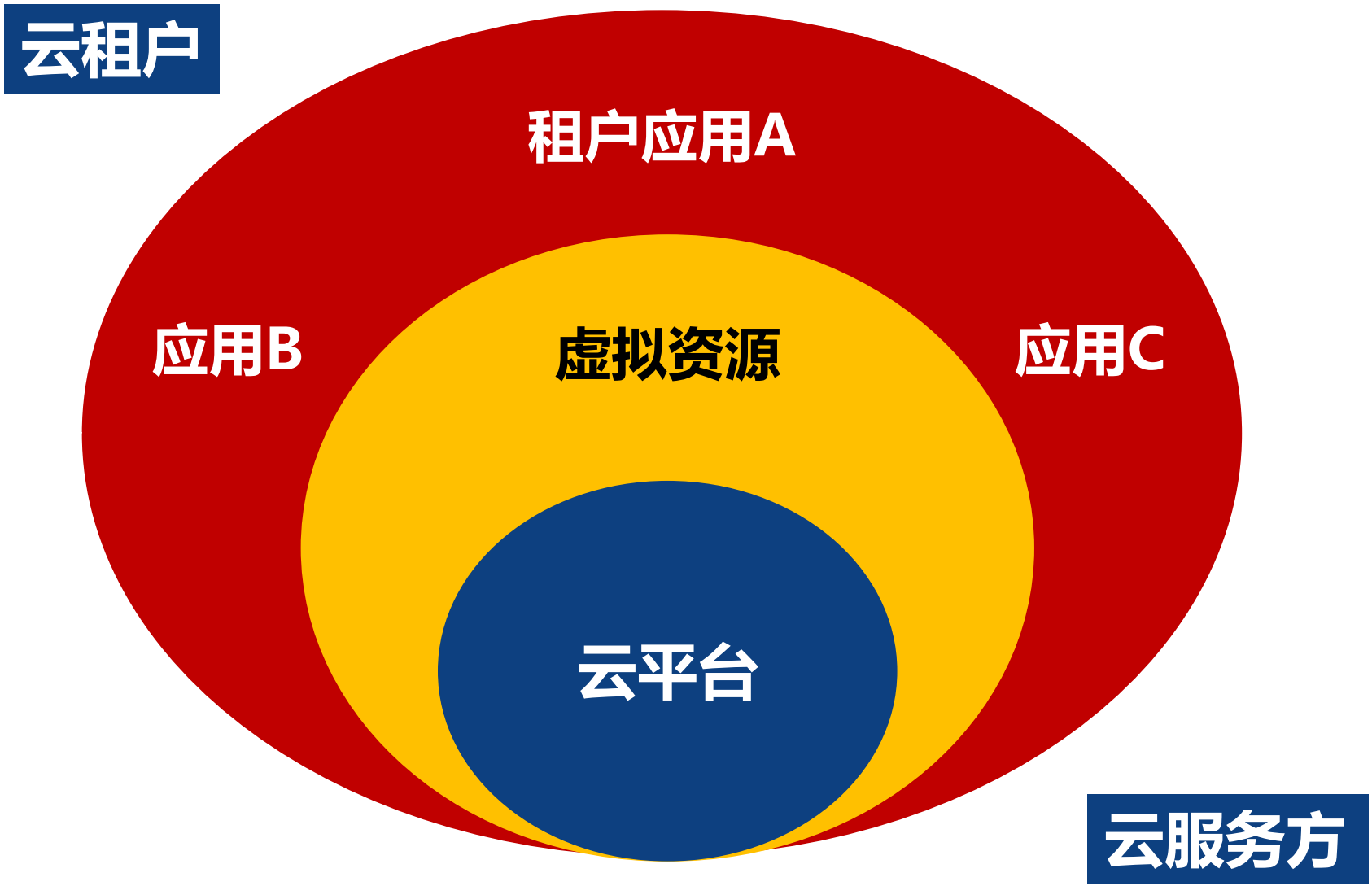
发生的信息安全事件进行分等级响应、处置

5个规定动作

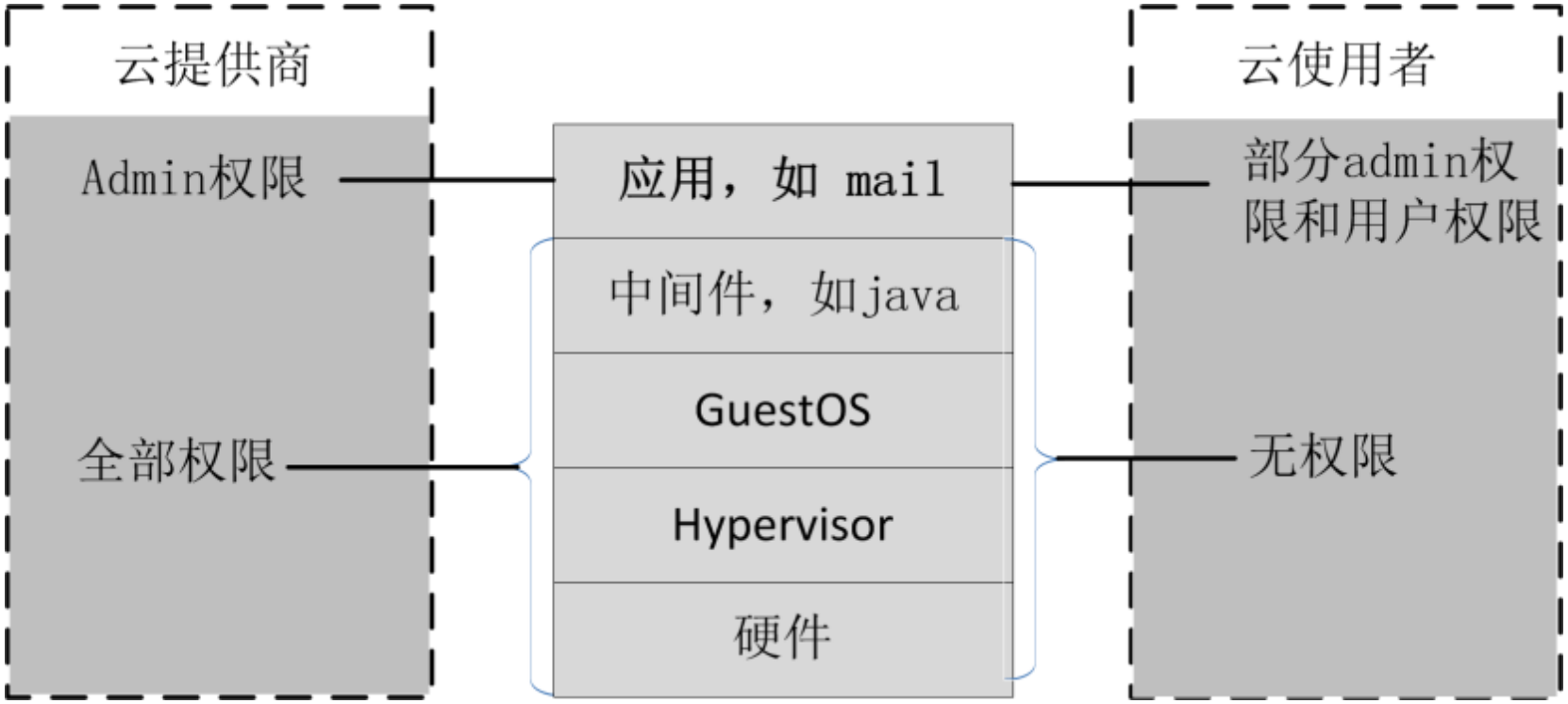


保护对象三要素

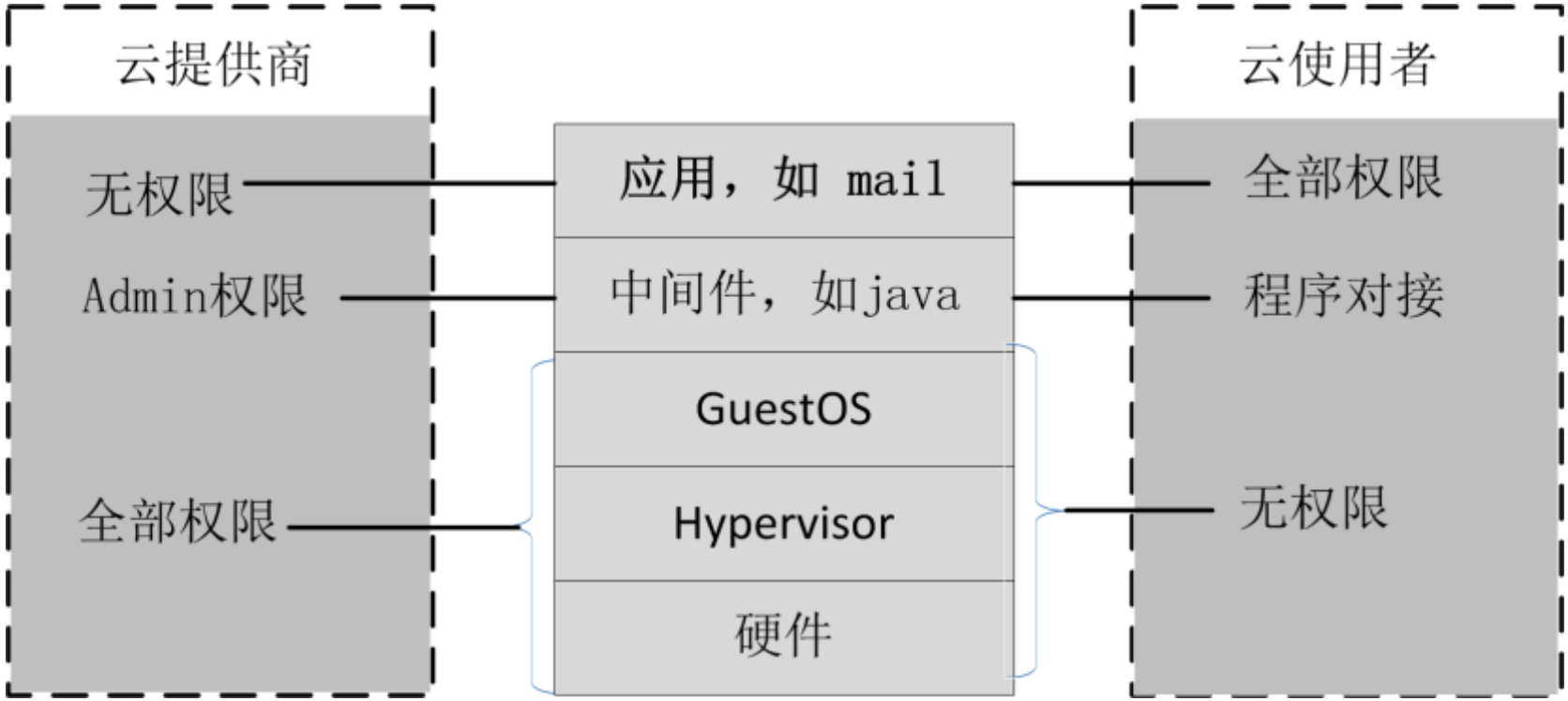
- 唯一确定的安全责任单位
- 具有信息系统的基本特征
- 承载单一或相对独立的业务应用


云租户
租户应用A
应用B
虚拟资源
应用C
云平台
云服务方

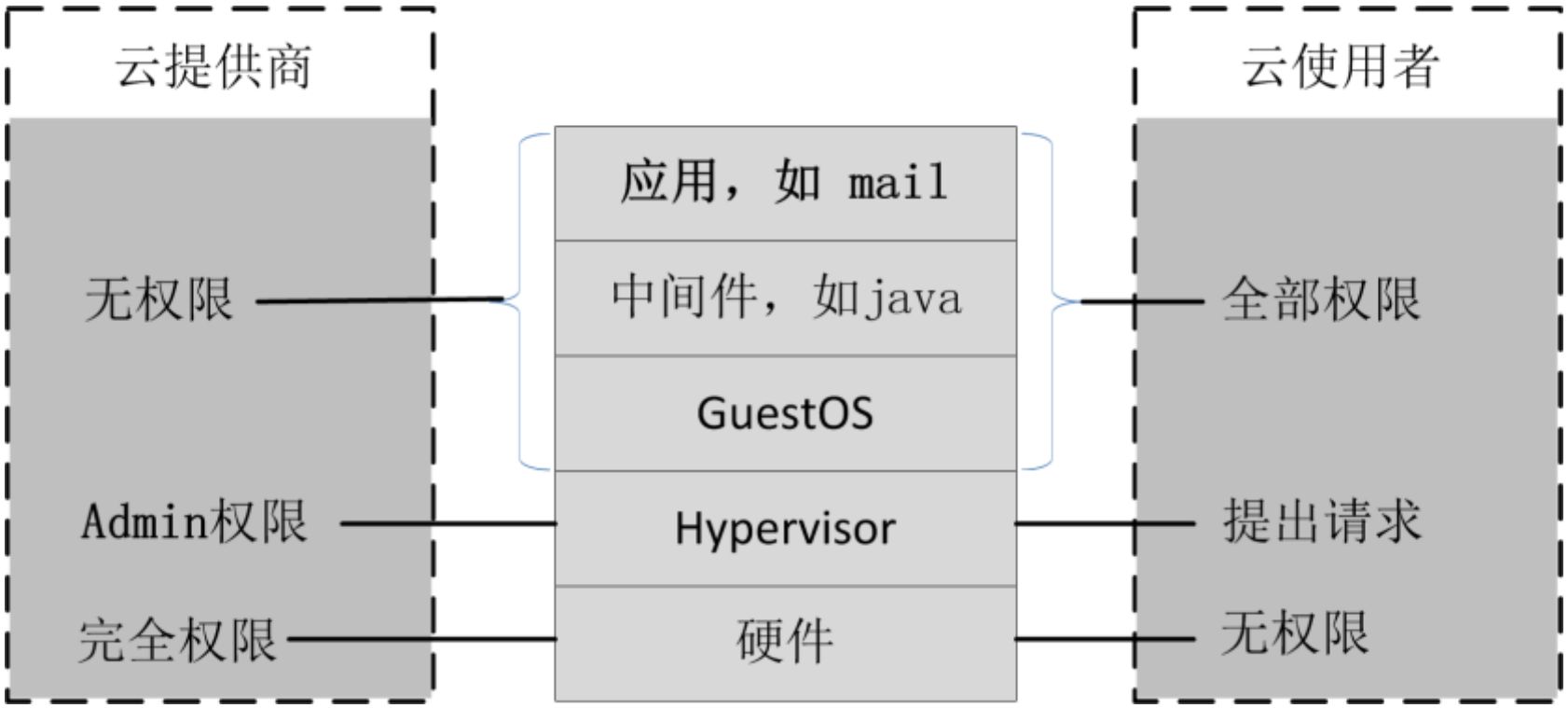
SAAS

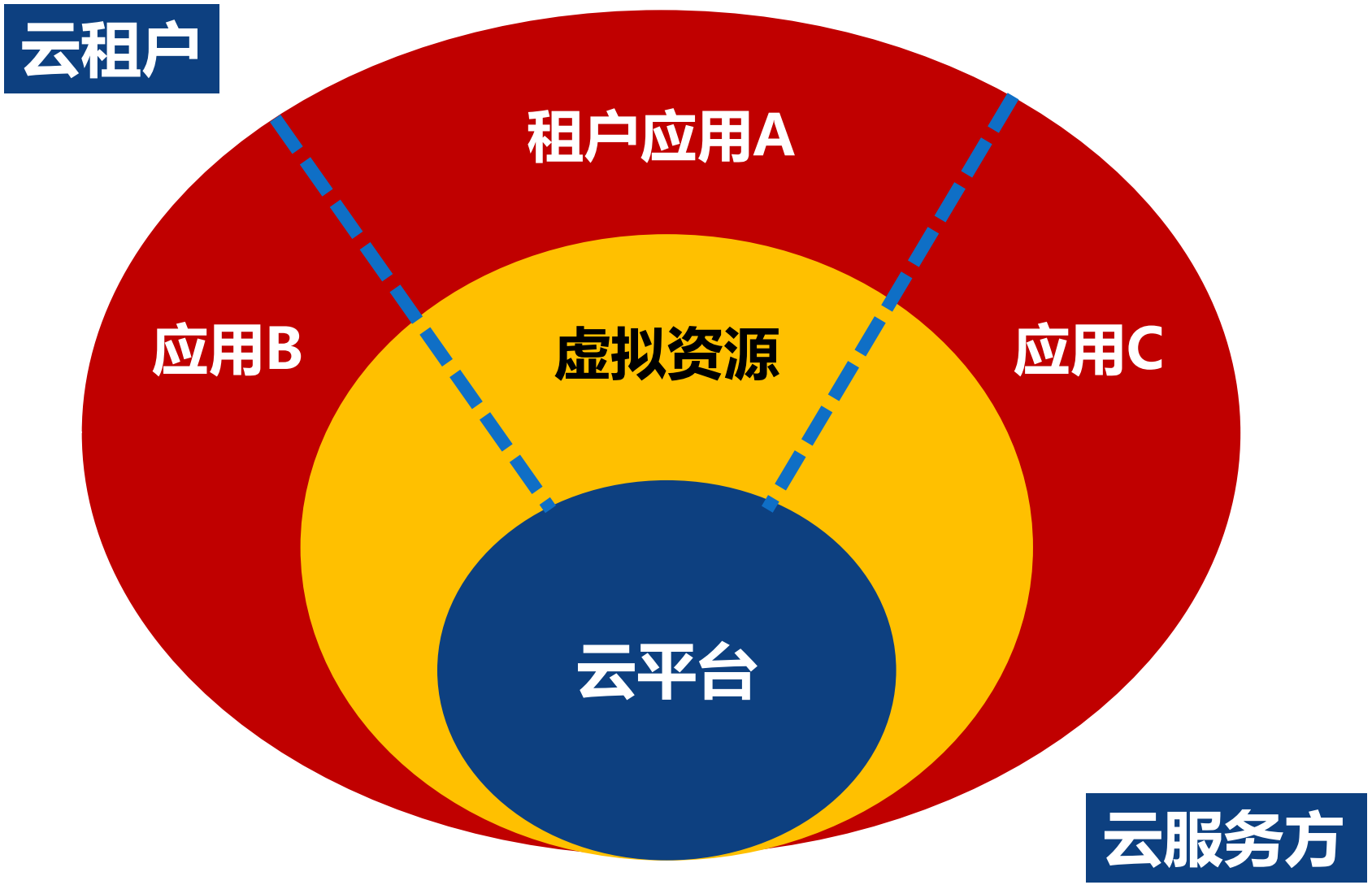

云提供商
Admin权限
全部权限
应用，如 mail
中间件，如java
GuestOS
Hypervisor
硬件
云使用者
部分admin权限和用户权限
无权限

PAAS


云提供商
无权限
Admin权限
全部权限
应用，如 mail
中间件，如java
GuestOS
Hypervisor
硬件
云使用者
全部权限
程序对接
无权限

IAAS


云提供商
无权限
Admin权限
完全权限
应用，如 mail
中间件，如java
GuestOS
Hypervisor
硬件
云使用者
全部权限
提出请求
无权限


云租户
租户应用A
应用B
虚拟资源
应用C
云平台
云服务方

层面	云计算系统保护对象（测评对象）
物理	机房及相关设施
网络	传统网络结构和虚拟化网络结构 传统网络设备、安全设备 虚拟化网络设备、安全设备
主机	传统主机、宿主机、虚拟机、主机安全软件
IaaS	虚拟化软件、虚拟机监视器（Hypervisor/VMM）、云操作系统
SaaS/PaaS	云应用开发框架、中间件
应用	业务应用系统
数据	虚拟化管理数据、用户隐私数据等

云计算安全威胁

- 1:数据泄露
- 2:数据丢失
- 3:账户或服务被劫持
- 4:不安全的接口
- 5: 拒绝服务攻击

6: 不怀好意的内部人员

7:滥用云服务

8:贸然采用云服务

9:共享隔离问题

平台安全

- 基础设施的组件自身安全应遵循《基本要求》
- 登录Hypervisor、云管理平台等的管理用户进行相应等级身份鉴别，确保云平台运维管理员和云服务管理员的权限分离
- 应在网络策略控制器和网络设备（或设备代理）之间建立双向身份验证机制；
- 应采取必要措施防止网络策略控制器和网络设备（或设备代理）之间的网络通信被窃听和嗅探。

资源隔离

- 应保证云平台管理流量与云租户业务流量分离
- 相同等级的系统共享资源池，应保证虚拟机仅能迁移至相同安全保护等级的资源池
- 禁止虚拟实例直接访问宿主机上的物理硬件
- 不同虚拟机之间的虚拟CPU指令隔离
- 应保证分配给虚拟机的内存空间仅供其独占访问
- 应保证虚拟机所使用的内存和存储空间回收时得到完全清除

资源隔离

- 虚拟机间依据访问控制策略实现访问
- 虚拟机间的通信有认证保护机制，保证每个VM有单独的信用凭证（新建虚拟机或者下线虚拟机重新启动时应有认证机制）
- 应提供开放接口，允许接入第三方安全产品，实现云租户的网络之间、安全区域之间、虚拟机之间的网络安全防护

数据安全

- 确保用于业务运行和数据处理及存储的物理设备位于中国境内，提供查询云租户数据及备份存储位置的方式
- 应保证云租户业务及数据能移植到其他云平台或者迁移到本地信息系统
- 应确保仅云租户拥有其数据库的最高管理权限
- 对虚拟机镜像文件进行完整性保护和更新，检测到非授权修改
- 对虚拟机快照文件进行保密性保护
- 提供虚拟机迁移过程中的完整性保护和信息防泄漏

审计与监控

- 应为安全审计数据的汇集提供接口，可供第三方审计
- 应根据云服务方和云租户的职责划分实现各自控制部分的集中审计
- 应保证云服务方对云租户系统和数据的操作可被云租户审计
- 应可以监控到所有虚拟机之间、虚拟机与宿主机之间的通信流量

管理要求

- 对云用户数据的访问和操作必须经过数据属主的授权，保留相关记录
- 签订服务水平协议SLA和签订隐私保护协议，并可向第三方提供相关证明。
- 供应链管理：文档提供、风险分析、措施描述、持续监控等

管理要求

- 监控管理：对通信线路、物理资源、主机、网络设备、虚拟资源、云管理平台和应用软件的运行状况、网络流量、用户行为等进行监测和报警
- 密钥管理：密钥仅在本地（机构内部）使用
- 开发：建立安全开发流程（SDLC），保证应用安全

谢谢！

请大家指正！