C3安全峰会
CYBER | CLOUD | COMMUNICATION

等保新规下的云计算安全

李明 博士
公安部信息安全等级保护评估中心

C3安全峰会
CYBER | CLOUD | COMMUNICATION

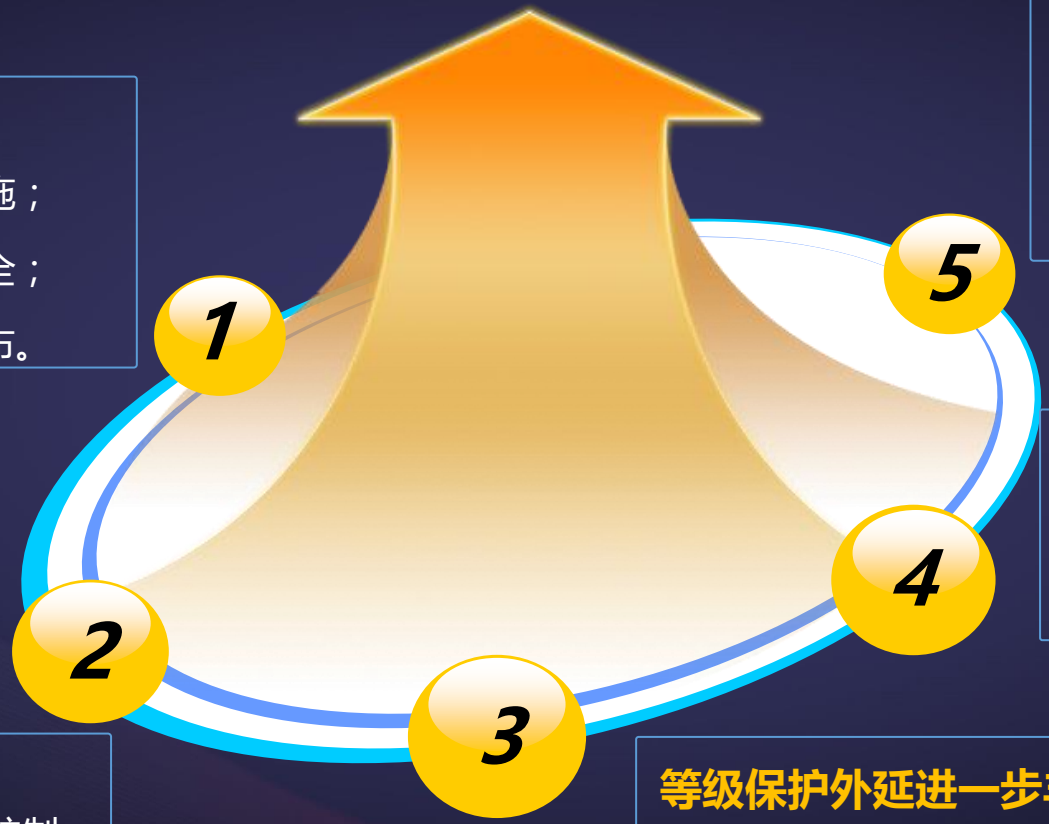
目录
CONTENTS

C3安全峰会
CYBER | CLOUD | COMMUNICATION

新形势下的等级保护

网络安全引起空前关注。

- 作用：辅助系统 - 支撑平台 - 基础设施；
- 关注：信息安全 - 信息保障 - 网络安全；
- 重视：《网络安全法》千呼万唤终颁布。



等级保护标准体系进一步提升适用性和可操作性。

- 核心标准启动修订
- 基本要求等标准扩充为系列标准

等级保护政策体系进一步细化和完善。

- 等级保护管理办法启动修订；
- 配套管理规范启动编制。

《网络安全法》确立制度地位。

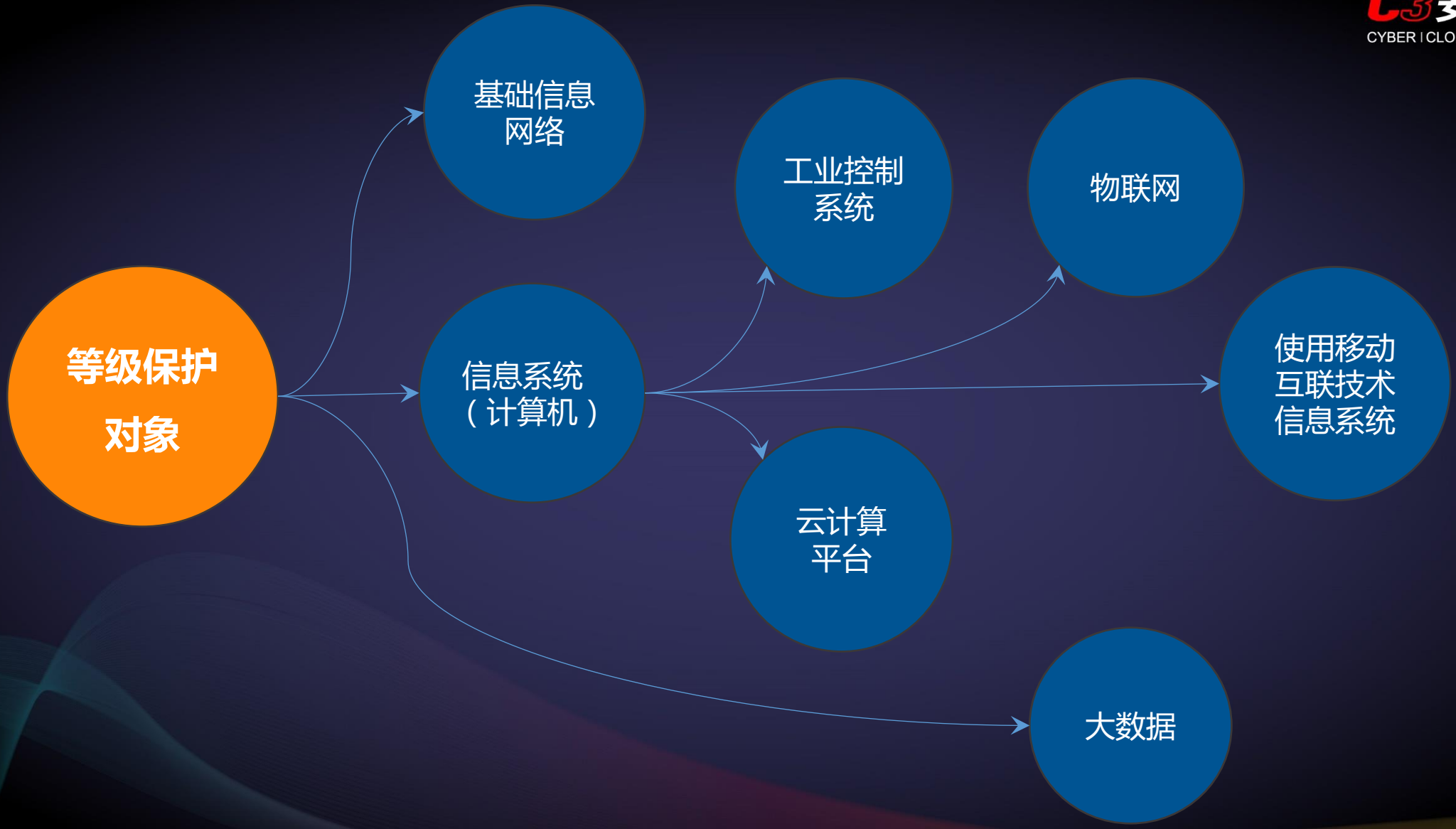
- 21条规定：国家实行网络安全等级保护制度；
- 31条规定：关键信息基础设施在网络安全等级保护制度的基础上，实行重点 保护。

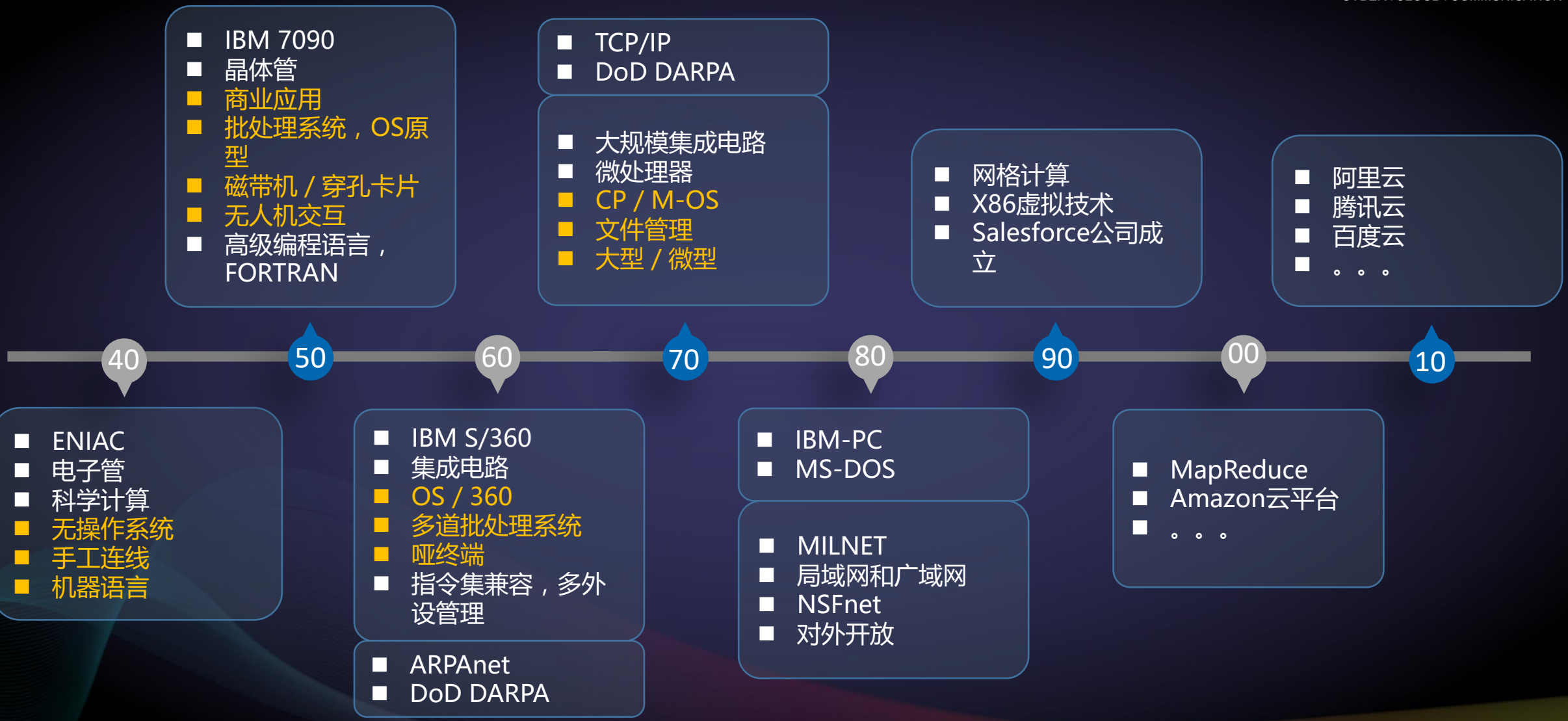
等级保护外延进一步丰富和完善。

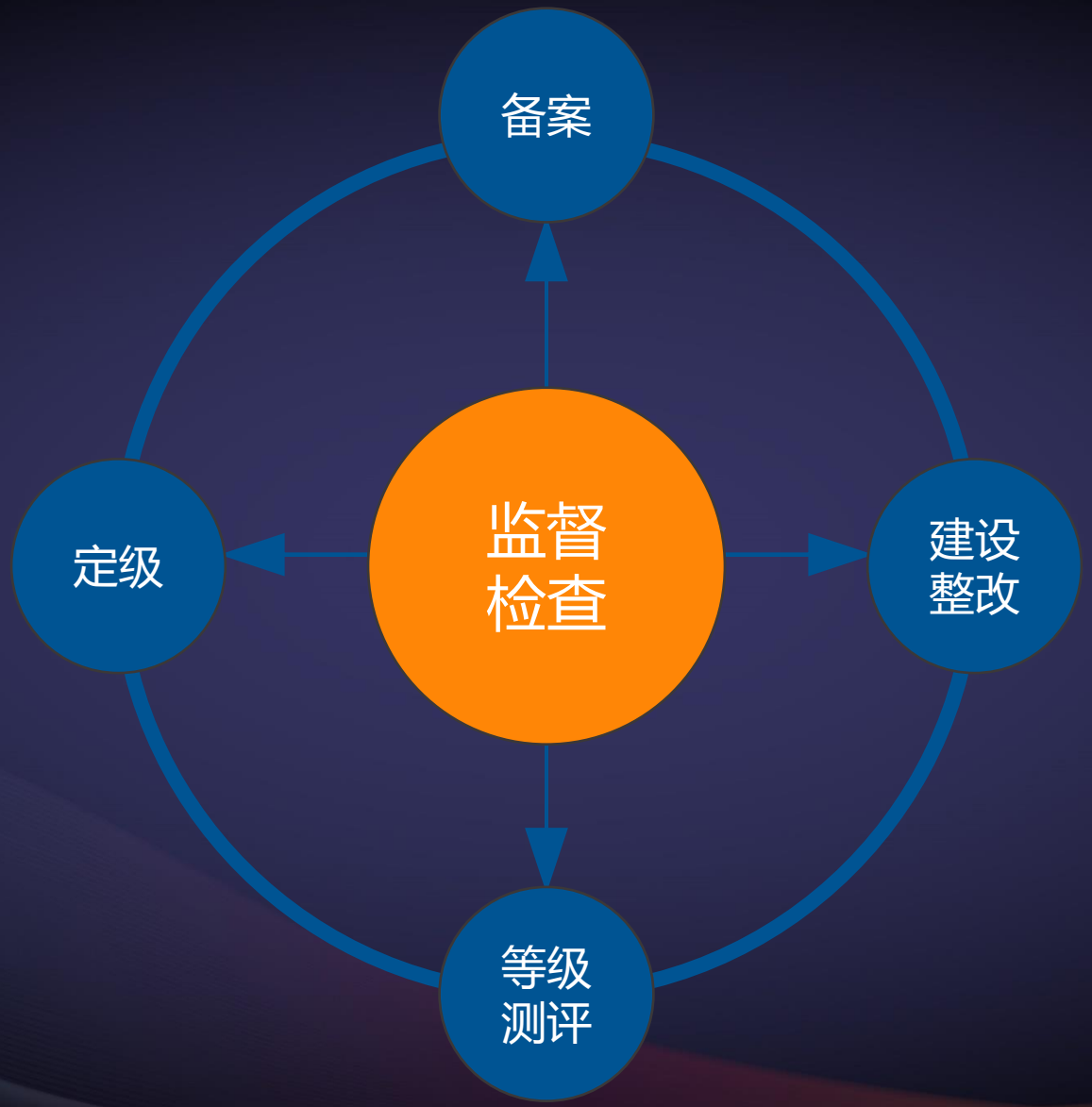
- 等级保护对象形态不断扩充（工业控制系统、云计算平台等）；
- 工作内容更加完善（供应链安全、通报预警等）。

第二十一条 国家实行网络安全等级保护制度。

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。


等级保护对象
基础信息网络
信息系统（计算机）
工业控制系统
物联网
使用移动互联技术信息系统
云计算平台
大数据

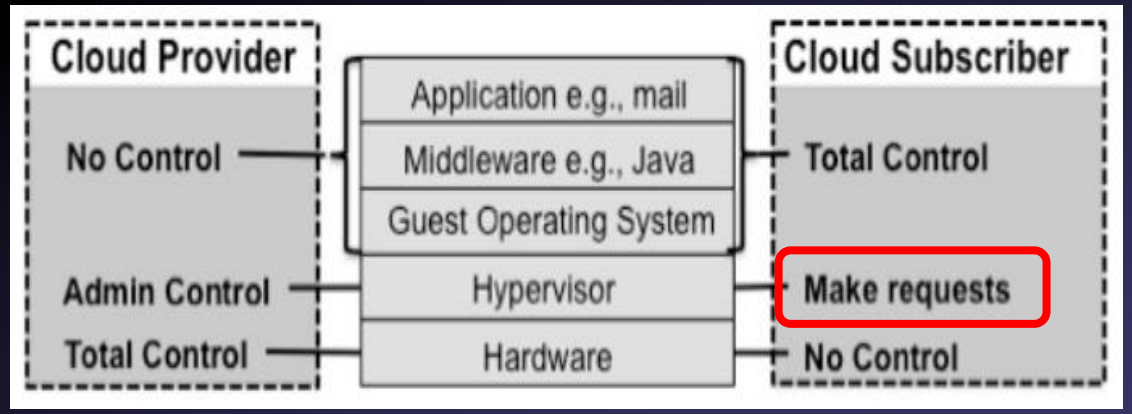

40
ENIAC
电子管
科学计算
无操作系统
手工连线
机器语言
50
IBM 7090
晶体管
商业应用
批处理系统，OS原型
磁带机 / 穿孔卡片
无人机交互
高级编程语言，FORTRAN
60
IBM S/360
集成电路
OS / 360
多道批处理系统
哑终端
指令集兼容，多外设管理
ARPAnet
DoD DARPA
70
TCP/IP
DoD DARPA
大规模集成电路
微处理器
CP / M-OS
文件管理
大型 / 微型
80
IBM-PC
MS-DOS
MILNET
局域网和广域网
NSFnet
对外开放
90
网格计算
X86虚拟技术
Salesforce公司成立
00
MapReduce
Amazon云平台
。。。
10
阿里云
腾讯云
百度云
。。。


备案
定级
监督
检查
建设
整改
等级
测评

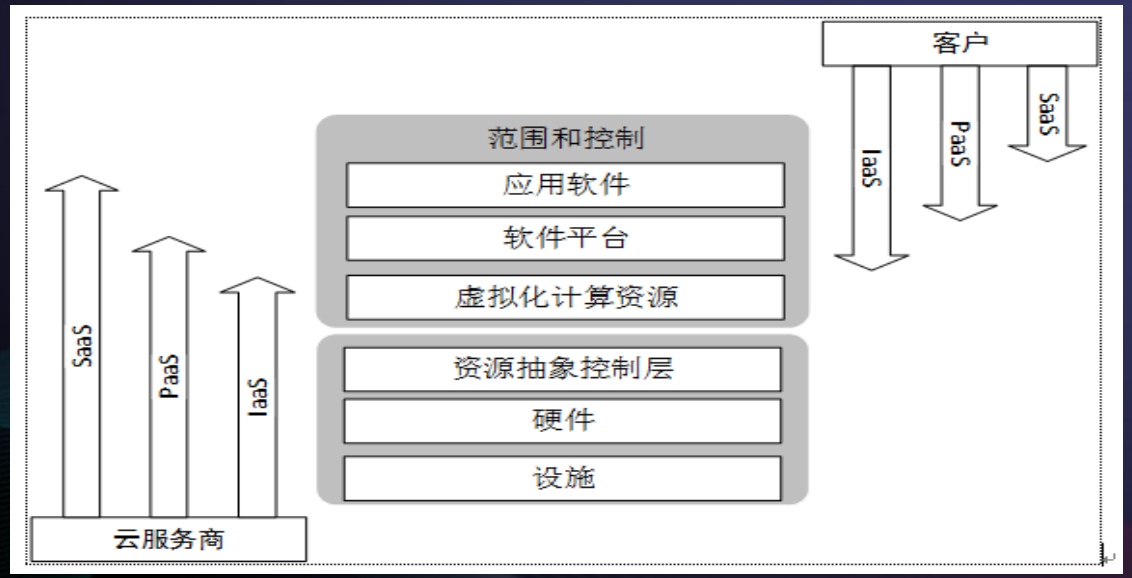
云计算典型模型

SP 800-146

IaaS组件栈和控制范围

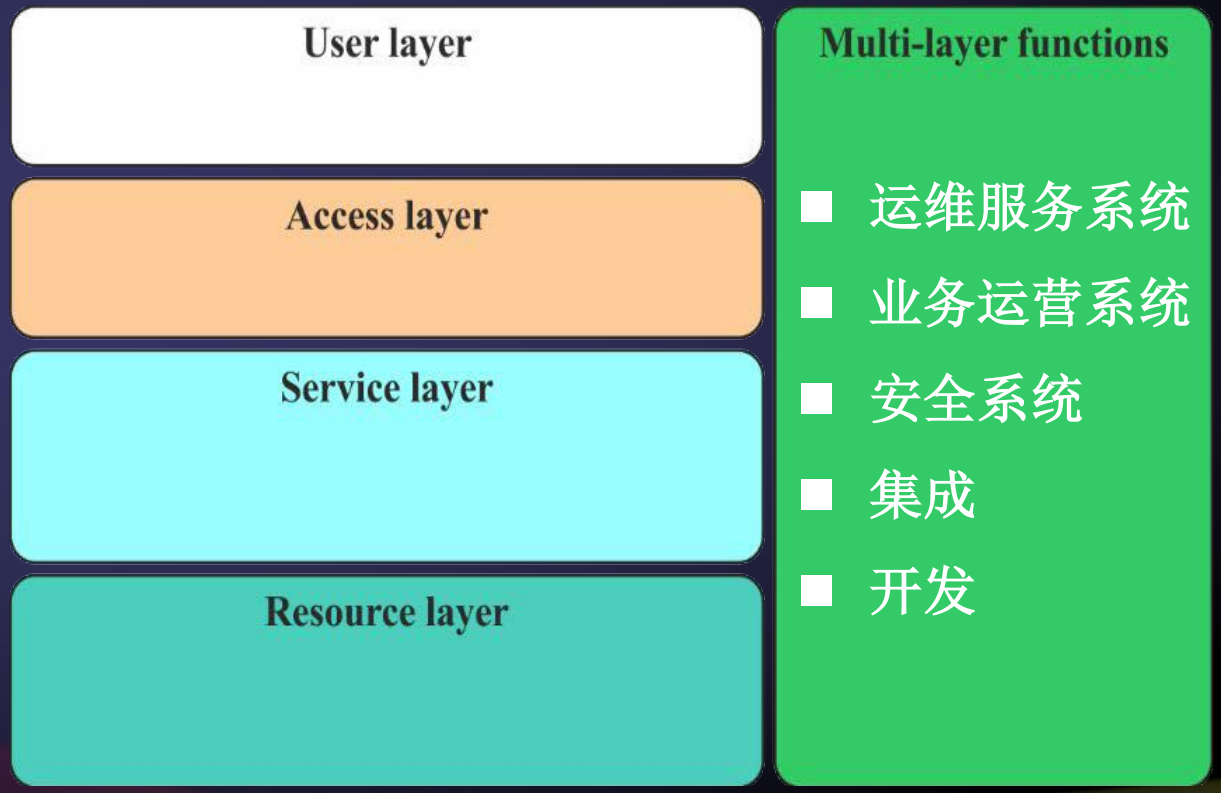


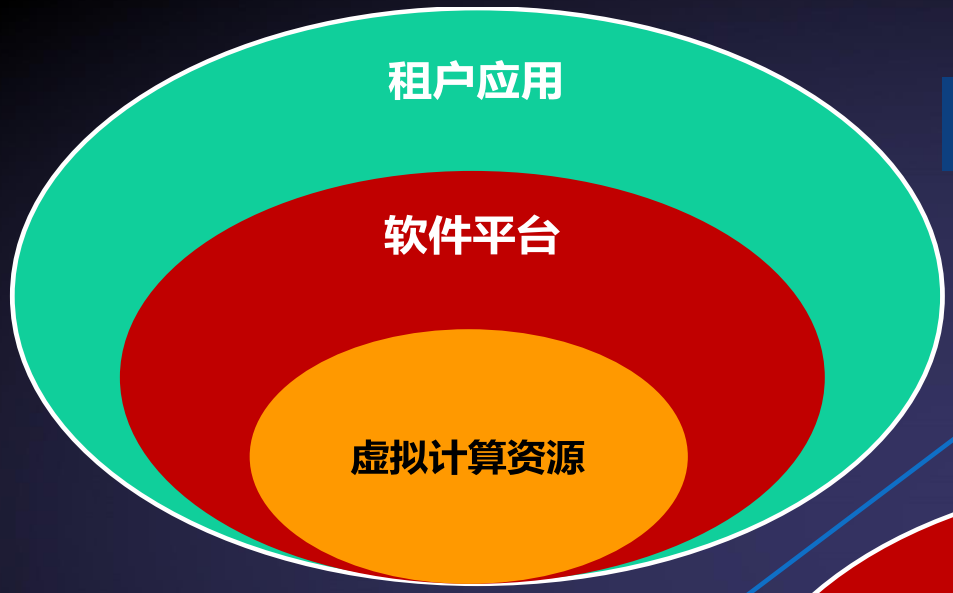
GB/T 31168‥ 2014



云计算模式与控制范围

ISO/IEC17789-2014
云计算层次框架

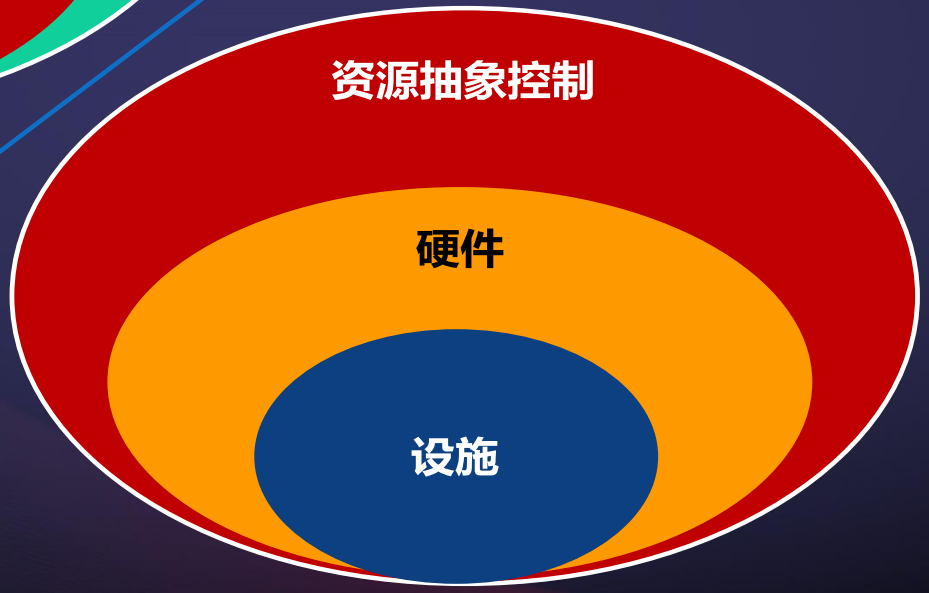




云租户

- 对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

云服务方



运营系统

运维系统

- 在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。

层面	云计算平台测评对象	传统信息系统测评对象
物理和环境安全	机房及基础设施	机房及基础设施
网络和通信安全	网络结构、网络设备、安全设备、**虚拟化网络结构、虚拟网络设备、虚拟安全设备**	传统的网络设备、传统的安全设备、传统的网络结构
设备和计算安全	网络设备、安全设备、**虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、**数据库管理系统、终端	传统主机、数据库管理系统、终端
应用和数据安全	应用系统、**云应用开发平台**、中间件、**云业务管理系统**、配置文件、**镜像文件、快照**、业务数据、用户隐私、鉴别信息等	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等

关注：统一身份认证、统一用户授权、统一访问控制、统一安全审计

侧重：动态监测预警、快速应急响应能力建设

重点：保障业务数据安全和用户数据隐私保护

- 在对业务应用系统（云租户系统）测评时，首先应关注基础支撑平台（云平台）是否已经测评，如未测评，则无法开展对业务应用系统（云租户系统）的测评
- 对业务应用系统（云租户系统）测评打分时，不但要考虑业务应用系统（云租户系统）自身得分，还应关注基础支撑平台（云平台）得分，基础支撑平台（云平台）得分高低将影响业务应用系统（云租户系统）得分

  举例：

  某租户系统自身安全得分90，部署在得分为100分的平台上综合得分为90，部署在得分为60分的系统上，综合得分为60

  这反映出云平台对租户系统提供安全支撑的价值，客观上迫使云服务商努力提升云平台的安全防护能力

C3安全峰会
CYBER | CLOUD | COMMUNICATION

信息安全技术 网络安全等级保护基本要求

第2部分：云计算安全扩展要求

（ GB / T 22239.2-201X，送审稿）

云计算安全扩展要求的特点

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- **标准的使用方法**
  - 新增基本要求第2部分：云计算安全扩展要求（ GB/T 22239.2 ），作为第1部分：安全通用要求（ GB/T 22239.1）在云计算安全领域的补充
  - 对云计算系统应用基本要求时应同时使用GB/T 22239.1和GB/T 22239.2的相关要求
  - 涵盖IaaS、PaaS、SaaS三种服务模式
  - 既对云服务商和云平台提出了要求，也对云租户和租户系统提出了要求
  - 附录中给出了不同服务模式下安全管理责任主体，方便标准使用者应用与自身角色相关的要求。

举例：

某云租户的云上业务系统采用IaaS模式部署在公有云上，在进行安全建设整改时，应首先根据22239.1安全通用要求做好保护，还应根据22239.2中有关云租户的要求做好云安全方面的保护。

某云服务商的云平台系统在进行安全建设整改时，应首先根据22239.1安全通用要求做好自身基础设施的安全保护，还应根据22239.2中有关云平台的要求，做好为云租户提供支撑服务的安全保护。

表A.1　GB/T 22239.2 与 GB/T 22239.1 关系表

类	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理位置选择	增加	扩展	扩展	扩展
	物理访问控制	继承	继承	继承	继承
	防盗窃和防破坏	继承	继承	继承	继承
	防雷击	继承	继承	继承	继承
	防火	继承	继承	继承	继承
	防水和防潮	继承	继承	继承	继承
	防静电	/	继承	继承	继承
	温湿度控制	继承	继承	继承	继承
	电力供应	继承	继承	继承	继承
	电磁防护	/	继承	继承	继承
	网络架构	扩展	扩展	扩展	扩展
	通信传输	继承	继承	继承	继承

谢谢，

敬请批评指正。