网络安全等级保护2.0
云计算与大数据相关工作介绍

网络空间安全测评工程技术中心　　王翔宇

CSTC
中国软件评测中心
（工业和信息化部软件与集成电路促进中心）

CSTC中国评测

目 录

CSTC中国评测

中国软件评测中心
INTRODUCTION

中国软件评测中心（工业和信息化部软件与集成电路促进中心），简称中国软件评测中心，作为国内权威的第三方软、硬件产品及系统质量检测、认证机构，是直属于工业和信息化部的一类科研事业单位。成立近30年来，中国软件评测中心秉承“专业就是实力”的宗旨，共承担了10万余款软硬件产品和1万余项信息系统工程的测试任务，共测评了800多个网络信息安全类项目，1300多个网络信息安全类系统。业务网络覆盖全国500多个城市，先后成立了广州、深圳、重庆、大连、上海、无锡、济宁、青岛等多个分中心，服务范围涵盖了全国31个省及直辖市。网络空间安全测评工程技术中心在武汉成立华中办事处。

通过评测、监理、认证、评估、设计等主营业务，构建基于第三方服务的科技产业链，旗下的赛迪评测、赛迪监理、赛迪认证、赛迪评估、赛迪设计等业务在业内拥有权威地位。

先后申请了40余个国家科研项目，建立了多个国家技术服务平台和重点实验室，开发了具有自主知识产权的30余种专业测试工具，获得了70余项软件著作权，具有3项专利，拥有20余项国家级管理体系认证及资质证书，并主持或参与了数十余项信息技术领域国家标准和行业标准的制定。

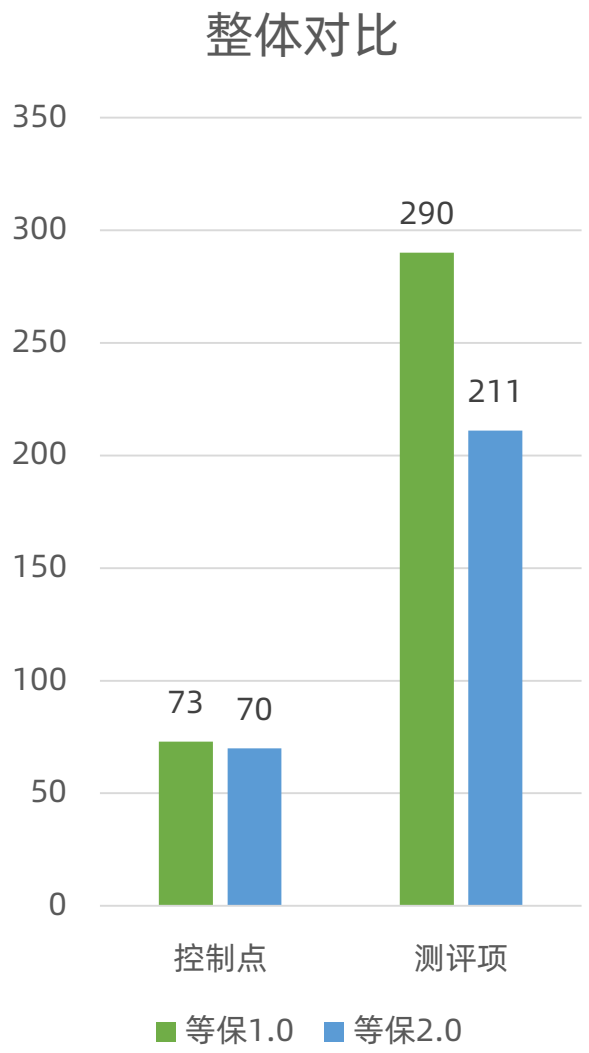
等级保护2.0简介
防护理念的变化

通用要求方面，等保2.0标准的核心是“优化”。删除了过时的测评项，对测评项进行合理性改写，新增对新型网络攻击行为防护和个人信息保护等新要求。

等保2.0标准采用“一个中心、三重防护”的理念，从等保1.0标准被动防御的安全体系向事前预防、事中响应、事后审计的动态保障体系转变，注重全方位主动防御、安全可信、动态感知和全面审计。

安全管理中心中对集中管控做出了明确要求，未来统一的集中管理平台将成为刚需。

新增关键词：态势感知、可信计算、安全管理中心、密码技术



等级保护2.0标准体系

- 网络安全等级保护条例（总要求、上位文件）
- 计算机信息系统安全保护等级划分准则（GB 17859-1999）(上位标准）
- 网络安全等级保护实施指南（ GB/T25058-2019 ）
- 网络安全等级保护定级指南（ GB/T22240 ）（正在修订）
- 网络安全等级保护基本要求（ GB/T22239-2019 ）
- 网络安全等级保护设计技术要求（ GB/T25070-2019 ）
- 网络安全等级保护测评要求（ GB/T28448-2019 ）
- 网络安全等级保护测评过程指南（ GB/T28449-2018 ）

CSTC中国评测

新发布相关标准（27项）

标准发布时间2019年08月31日
标准实施时间2020年03月01日

GB/T 25058-2019 网络安全等级保护实施指南
GB/T 20272-2019 操作系统安全技术要求
GB/T 21050-2019 网络交换机安全技术要求
GB/T 20009-2019 数据库管理系统安全评估准则
GB/T 18018-2019 路由器安全技术要求
GB/T 20979-2019 虹膜识别系统技术要求
GB/T 37971-2019 智慧城市安全体系框架
GB/T 37932-2019 数据交易服务安全要求
GB/T 37973-2019 大数据安全管理指南
GB/T 20273-2019 数据库管理系统安全技术要求
GB/T 37980-2019 工业控制系统安全检查指南
GB/T 37931-2019 Web应用安全检测系统安全技术要求和测试评价方法
GB/T 37934-2019 工业控制网络安全隔离与信息交换系统安全技术要求
GB/T 37933-2019 信息安全技术工业控制系统专用防火墙技术要求
GB/T 37962-2019 工业控制系统产品信息安全通用评估准则
GB/T 37988-2019 信息安全技术数据安全能力成熟度模型
GB/T 37972-2019 云计算服务运行监管框架
GB/T 37935-2019 可信计算规范可信软件基
GB/T 37941-2019 工业控制系统网络审计产品安全技术要求
GB/T 37939-2019 网络存储安全技术要求
GB/T 37964-2019 个人信息去标识化指南
GB/T 37950-2019 桌面云安全技术要求
GB/T 37954-2019 工业控制系统漏洞检测产品技术要求及测试评价方法
GB/T 37952-2019 移动终端安全管理平台技术要求
GB/T 37953-2019 工业控制网络监测安全技术要求及测试评价方法
GB/T 37955-2019 数控网络安全技术要求
GB/T 37956-2019 网站安全云防护平台技术要求

最新发布标准（8项）2020年10月1日起实施

GB/T 17901.1-2020 信息技术 安全技术 密钥管理 第1部分：框架

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 38540-2020 信息安全技术 安全电子签章密码技术规范

GB/T 38541-2020 信息安全技术 电子文件密码应用指南

GB/T 38542-2020 信息安全技术 基于升入特征识别的移动智能终端身份鉴别技术框架

GB/T 38556-2020 信息安全技术 动态口令密码应用技术规范

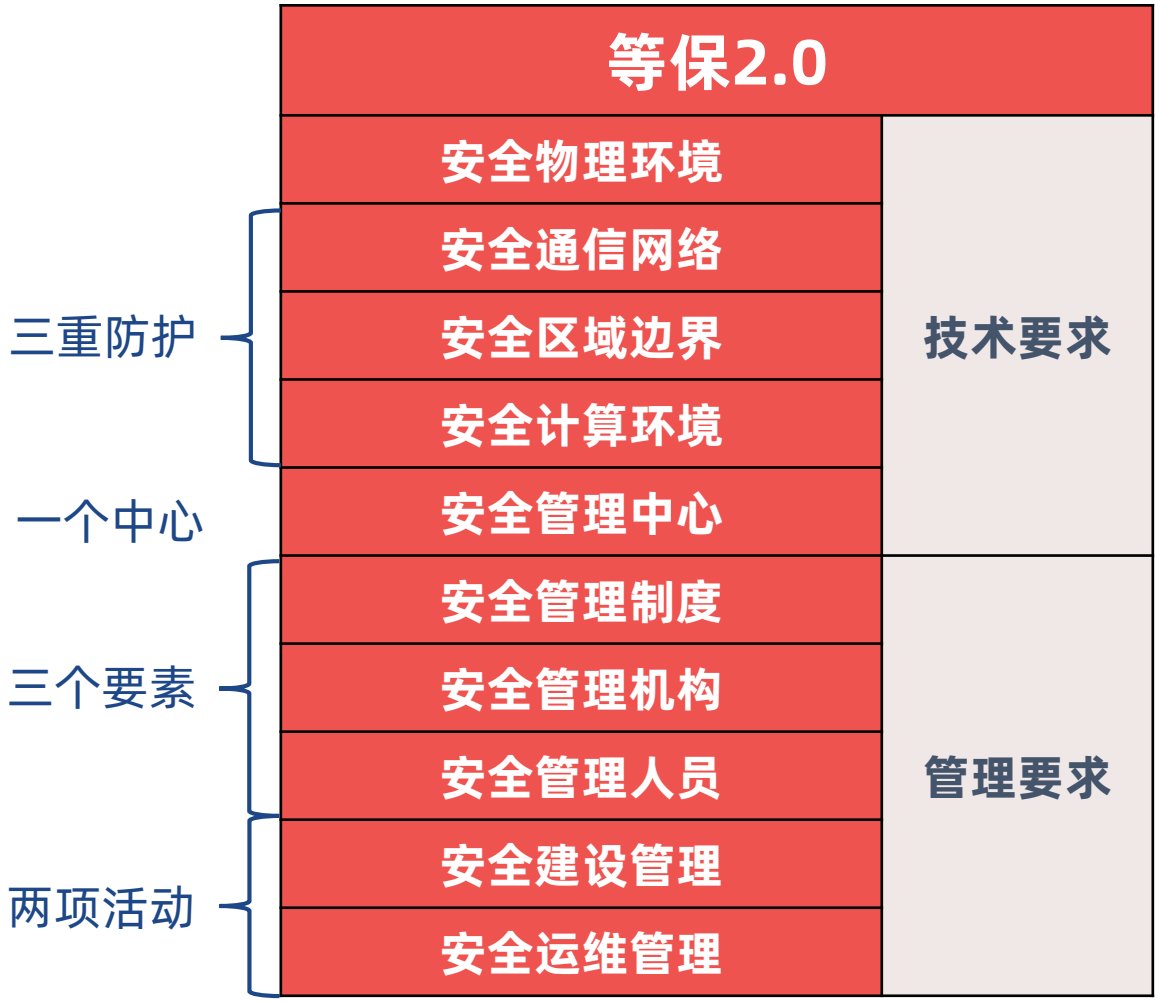
GB/T 38558-2020 信息安全技术 办公设备安全测试方法

GB/T 38561-2020 信息安全技术 网络安全管理支撑系统技术要求

等保2.0安全架构的划分

技术层面以“一个中心，三重防护”为依据进行划分

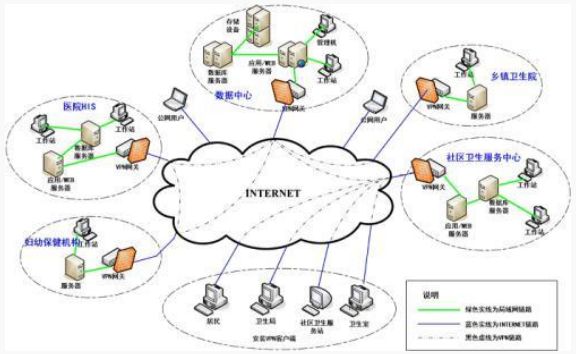
管理层面以“三个要素，两项活动”为依据进行划分



等级保护2.0标准覆盖范围

CSTC中国评测

基础信息网络



对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。跨省全国性业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

云计算平台

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。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。

物联网

物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。

移动互联

采用移动互联技术的等级保护对象应作为一个整体对象定级，主要包括移动终端、移动应用、无线网络以及相关应用系统等。

工业控制系统

工业控制系统主要由生产管理层、现场设备层、现场控制层和过程监控层构成，其中：生产管理层的定级对象确定原则见(其他信息系统)。设备层、现场控制层和过程监控层应作为一个整体对象定级，各层次要素不单独定级。对于大型工业控制系统，可以根据系统功能、控制对象和生产厂商等因素划分为多个定级对象。

大数据

应将具有统一安全责任单位的大数据作为一个整体对象定级，或将其与责任主体相同的相关支撑平台统一定级。

云计算与大数据的定级

等保2.0对定级对象

大数据

应将具有统一安全责任单位的大数据作为一个整体对象定级， 或将其与责任主体相同的相关支撑平台统一定级。

云计算平台

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。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。

基础信息网络

对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。

跨省全国性业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

采用移动互联技术的信息系统

采用移动互联技术的等级保护对象应作为一个整体对象定级，主要包括移动终端、移动应用、无线网络以及相关应用系统等。

物联网

物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。

工业控制系统

工业控制系统主要由生产管理层、现场设 备层、现场控制层和过程监控层构成，其中:生产管理层的定级对象确定原则见(其 他信息系统)。设备层、现场控制层和过程监控层应作为一个整体对象定级，各层次 要素不单独定级。

对于大型工业控制系统，可以根据系统功 能、控制对象和生产厂商等因素划分为多个定级对象。

其他信息系统

作为定级对象的其他信息系统应 具有如下基本特征:

a) 具有确定的主要安全责任单位。作为定级对象的信息系统应 能够明确其主要安全责任单位;

b) 承载相对独立的业务应用。 作为定级对象的信息系统应承载 相对独立的业务应用， 完成不 同业务目标或者支撑不同单位或 不同部门职能的多个信息系统应 划分为不同的定级对象;

c) 具有信息系统的基本要素。 作为定级对象的信息系统应该是 由相关的和配套的设备、 设施 按照一定的应用目标和规则组合 而成的多资源集合，单一设备 (如服务器、终端、网络设备等) 不单独定级。

云计算与大数据的定级

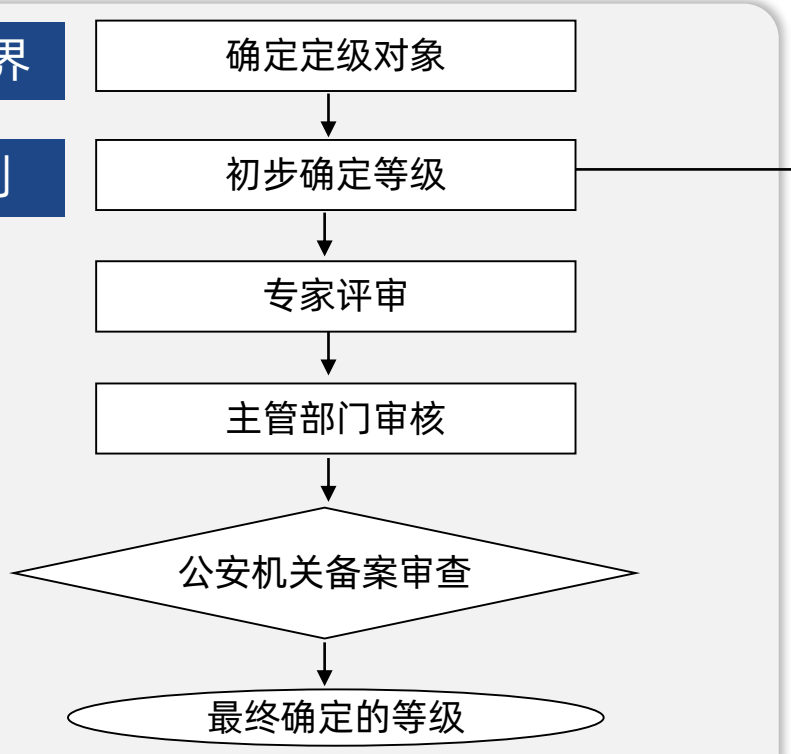
等保2.0对定级流程

“等级保护对象定级工作一般流程” 与 “定级方法流程”

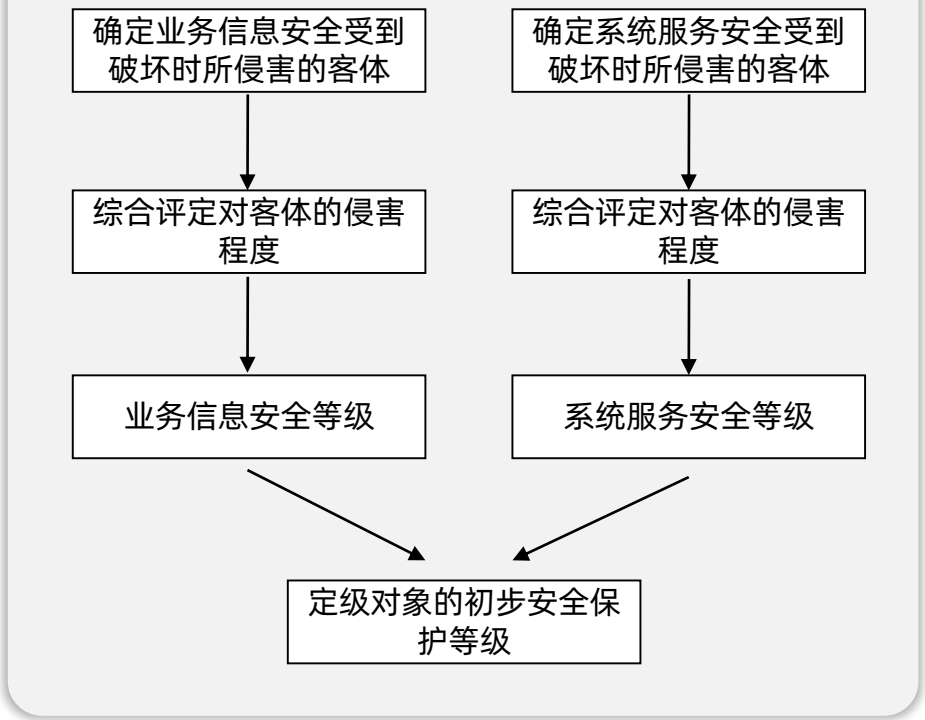
如何划分责任与边界

如何确定系统级别

等级保护对象定级工作一般流程



定级方法流程



云计算与大数据的定级

云计算平台与云计算应用的划分与定级

相关标准中的划分基本原则

责任分担原则：一个或多个责任主体的划分，云服务商和云服务客户（云租户），云计算平台与云计算应用

云服务模式适用性原则：IaaS、PaaS、SaaS

云计算平台

服务模式	安全层面	对象及资产
	安全计算环境	云产品（服务）
		云产品（服务）数据
SaaS	安全计算环境	虚拟机、数据库服务、中间件、容器、云应用开发平台、云产品（服务）等
PaaS/IaaS	安全计算环境	云操作系统、虚拟机监视器、云业务管理系统、云产品（服务）
		虚拟网络/安全设备、虚拟机镜像
		云产品（服务）服务器（虚拟机）、宿主机、终端、云管平台服务器
		网络设备、安全设备
		管理数据（配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据、个人信息）
	安全通信网络	网络架构、物理链路、通信数据
	安全区域边界	物理网络边界、虚拟网络边界
	安全管理中心	云管理平台、云平台监控系统
	安全管理	安全相关人员、机房、介质以及管理文档
	安全物理环境	物理机房、云计算基础设施部署的相关机房及基础设施

云计算应用

服务模式	安全层面	对象及资产
IaaS	安全计算环境	云服务客户业务应用系统
		业务数据
		虚拟机、数据库、中间件等
		虚拟网络设备、虚拟安全设备
	安全通信网络	虚拟网络架构
	安全区域边界	虚拟网络边界防护服务
	安全管理中心	安全管理平台
	安全管理	安全相关人员、介质以及管理文档
PaaS	安全计算环境	容器、数据库
		业务应用系统
		业务数据
	安全管理中心	安全管理平台
	安全管理	安全相关人员、介质以及管理文档
SaaS	安全计算环境	业务数据
		业务应用系统
	安全管理	安全相关人员、介质以及管理文档

CSTC中国评测

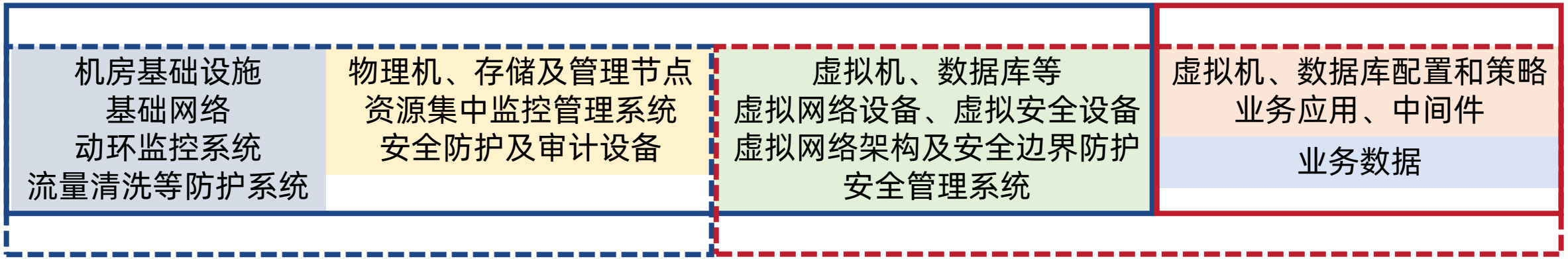
云计算平台与云计算应用的划分与定级

私有云划分

云计算平台和云计算应用一般为同一个责任主体，系统边界的划分主要依据云服务模式

典型划分方式（同一责任主体）

私有云平台



每个云计算应用单独定级备案

云计算应用可按业务进行划分，一个云计算应用可包含多个子系统

几种特殊情况：

涉及到其他托管、运维单位

采用云计算技术构建的业务应用系统

网站群系统

云计算与大数据的定级

大数据安全责任主体的划分及定级

责任主体	组成部分
数据所有者	大数据资源
大数据应用提供者	大数据应用
大数据平台提供者	大数据平台
基础设施提供者	基础设施

同一责任主体的单一大数据应用和大数据平台

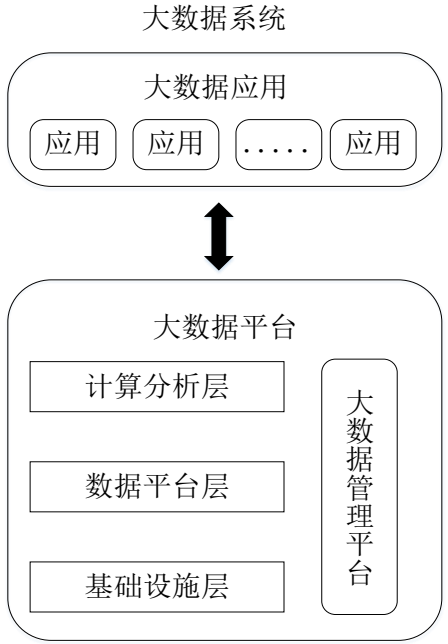
- 定级对象比较清晰，系统划分比较明确，大数据应用和大数据平台结合紧密
- 应将二者作为整体的大数据系统

同一责任主体的多个大数据应用基于同一个大数据平台

- 大数据应用进行分别定级，大数据平台分别定级
- 大数据平台等级不低于大数据应用的安全保护等级
- 应注重大数据平台对于不同大数据应用的访问控制和对于不同数据的分级、分类安全管控等措施

不同责任主体的大数据应用和大数据平台

- 明确大数据平台先确定安全等级，完成定级备案，并通过等级测评，才能开展大数据应用的等保定级及后续工作



云计算与大数据的定级

安全保护等级的确定

CSTC中国评测

信息系统被破坏时所侵害的客体	对应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

业务信息（S）

涉及到其他单位信息 ↑
财务、金融信息，交易信息 ↑
大量个人信息 ↑

系统服务（A）

对外提供服务 ↑
业务连续性要求高 ↑
跨地域提供服务 ↑

1. 云计算应用及大数据应用的级别不应高于云计算平台及大数据平台的级别
2. 以修订后最终发布的 GB/T 22240 定级指南为准

等级保护定级备案工作

安全要求及属性标识

CSTC中国评测

安全保护等级	定级结果的组合
第一级	S1A1
第二级	S1A2，S2A2，S2A1
第三级	S1A3，S2A3，S3A3，S3A2，S3A1
第四级	S1A4，S2A4，S3A4，S4A4，S4A3， S4A2，S4A1
第五级	S1A5，S2A5，S3A5，S4A5，S5A4， S5A3，S5A2，S5A1

S：信息安全类要求

A：服务保证类要求

G：其他安全保护类要求

注：标准正文中取消对控制点的 “S”、 “A”、 “G”标注

安全通用要求

分类	安全控制点	属性标识
安全物理环境	电力供应	A
	电磁防护	S
安全通信网络	可信验证	S
安全区域边界	可信验证	S
安全计算环境	身份鉴别	S
	访问控制	S
	可信验证	S
	数据完整性	S
	数据保密性	S
	数据备份恢复	A
	剩余信息保护	S
	个人信息保护	S
其他	……	G

云计算与大数据的定级

安全保护等级的含义

保护对象等级	重要程度	监督管理强度等级	安全保护能力等级	威胁源	损害	恢复
第一级	一般网络	自主保护级	第一级安全保护能力	个人、拥有很少资源 一般的自然灾难	关键资源损害	恢复 部分功能
第二级	一般网络	指导保护级	第二级安全保护能力	小型组织、拥有少量资源 一般的自然灾难	重要资源损害	在一段时间内恢复 部分功能
第三级	重要网络	监督保护级	第三级安全保护能力	有组织的团体、拥有较为丰富资源 较为严重的自然灾难	主要资源损害	较快恢复 绝大部分功能
第四级	特别重要网络	强制保护级	第四级安全保护能力	国家级、敌对组织、拥有丰富资源 严重的自然灾难	资源损害	迅速恢复 所有功能
第五级	极其重要网络	专控保护级		未公布		

《网络安全等级保护条例》（征求意见稿）

《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）

《网络安全等级保护基本要求》（GB/T 22239-2019）

CSTC中国评测

测评工作流程

依据标准

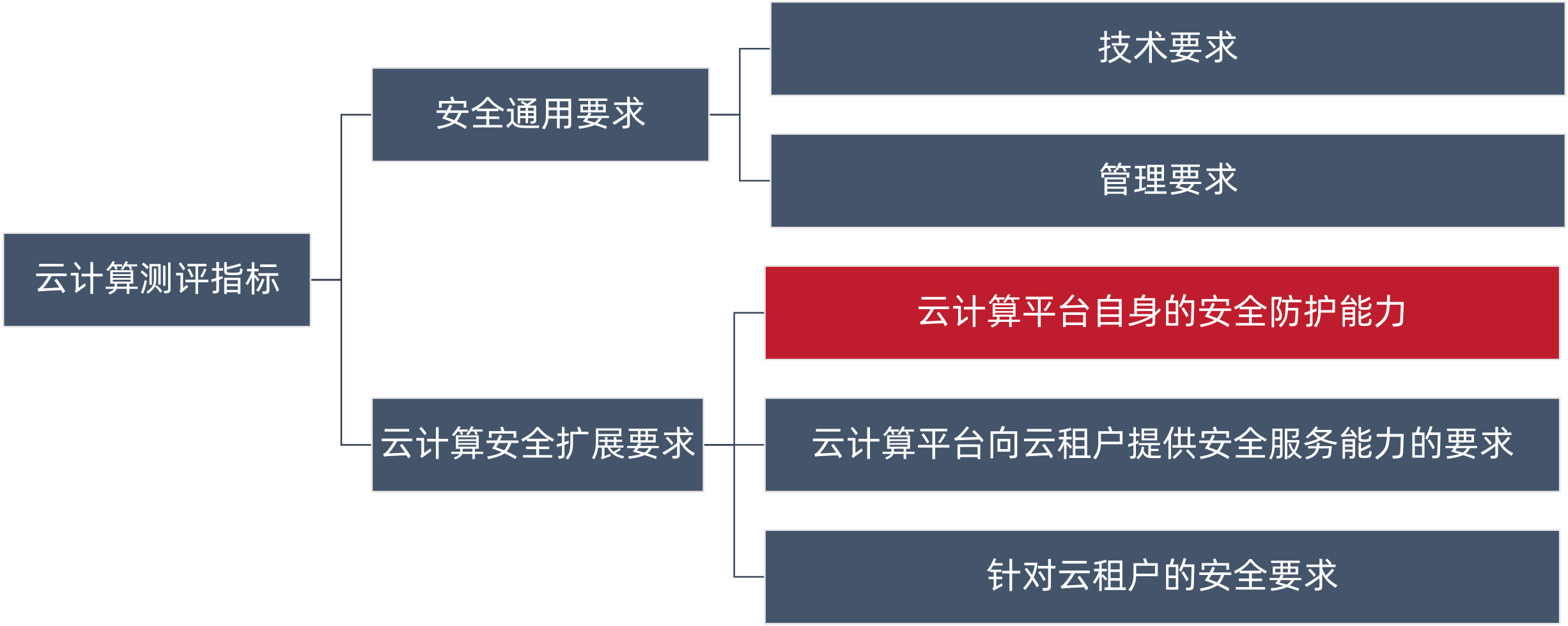
GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中的安全通用要求和对应安全扩展要求

测评顺序

一般为先测评云计算平台和大数据平台，后测评云计算应用和大数据应用

在云计算应用和大数据应用的测评报告中需要引用平台的测评报告

云计算安全测评指标选择



云计算安全扩展要求指标选取（3级）

层面	控制项	控制点	IaaS	PaaS	SaaS	云租户
安全物理环境	基础设施位置	1	1	1	1	1
安全通信网络	网络架构	5	5	1	1	0
安全区域边界	访问控制	2	2	0	0	0
	入侵防范	4	4	0	0	0
	安全审计	2	2	0	0	0
安全计算环境	身份鉴别	1	1	1	1	0
	访问控制	2	2	0	0	0
	入侵防范	3	3	0	0	0
	镜像和快照保护	3	3	0	0	0
	数据完整性和保密性	4	4	2	2	0
	数据备份恢复	4	3	1	1	1
	剩余信息保护	2	2	1	1	0
安全管理中心	集中管控	4	4	1	1	0
安全建设管理	云服务商选择	5	0	5	5	5
	供应链管理	3	3	3	3	0
安全运维管理	云计算环境管理	1	1	1	1	0
合计	16	46	40	17	17	7

云计算安全测评部分解读

安全计算环境：

身份鉴别

a)当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

目前双向身份认证较难实现，对云计算平台管理时，管理员可以明确自己的管理目标，但如何确认自己登录的管理目标是预期的，比较难以实现，因为目标是明确的，所以现在在测评过程中一般要求对管理的终端进行认证。

入侵防范

a) 应能检测虚拟机之间的资源隔离失效，并进行告警；

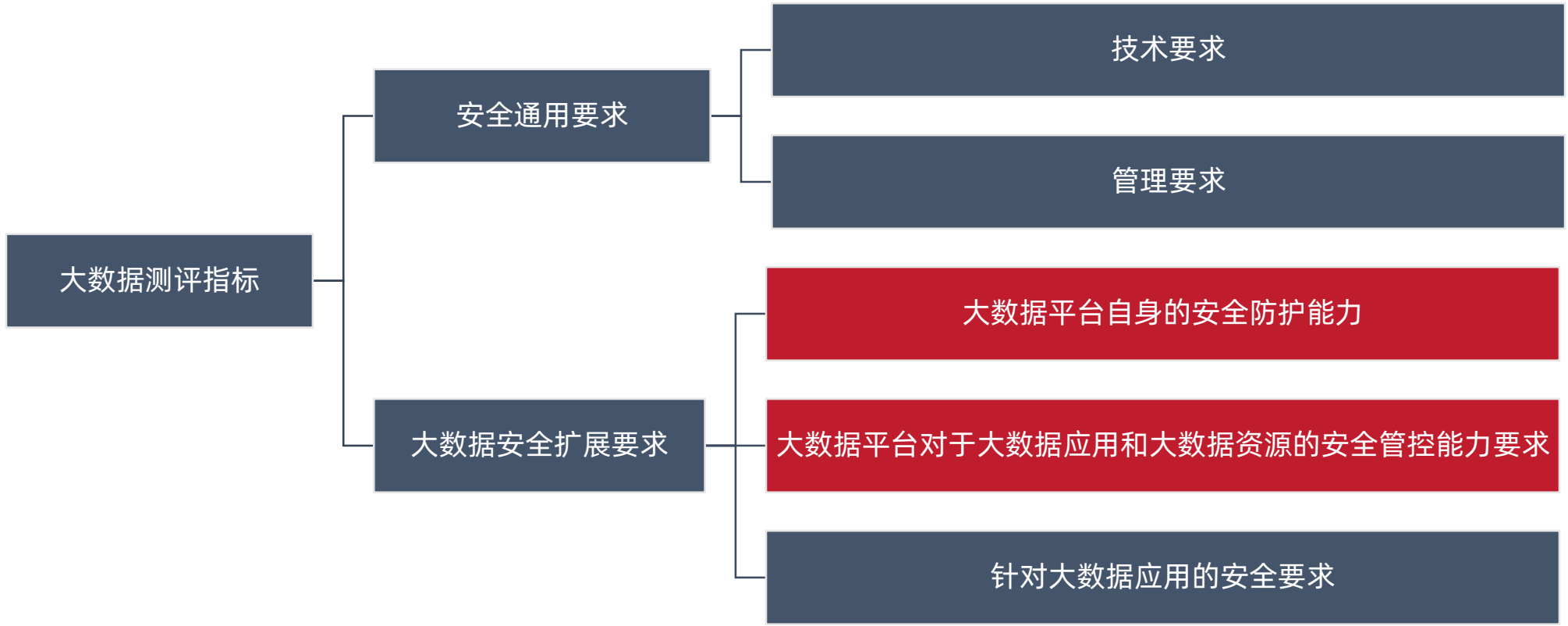
因为云平台从设计之初虚拟机之间的资源就是相互隔离的，只有在逃逸的情况下才有可能访问非授权的资源，目前的技术不能对未知的0DAY进行完全检测，在测评的过程中要求对已知的逃逸事件进行检测，且对异常流量进行分析告警，但未知的在测评过程中较难实现验证，一般验证已知的漏洞，目前大部分云厂商通过对HIDS的二次开发实现。

b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

可能是创建时在管理平台注册失败，但虚拟机已经生成，或者是管理员通过底层的命令创建的虚拟机不存在管理数据为中或数据库中的状态不对。

CSTC中国评测

大数据安全测评指标选择



数据采集	数据存储	数据应用	数据交换	监控手段
• 授权 • 身份鉴别 • 数据真实可信	• 数据分类分级 • 敏感数据保密性 • 数据备份	• 数据脱敏 • 数据去标识化 • 细粒度授权访问控制	• 数据完整性 • 接口访问控制	• 集中管控 • 业务连续性 • 全生命周期跟踪和记录

大数据安全扩展要求指标选取（3级）

CSTC 中国评测

大数据平台测评指标（23/24）

序号	安全类或层面	第三级安全评估方法指标选取
1	安全物理环境	a)
2	安全通信网络	a)、b)
3	安全计算环境	a)、b)、c)、d)、e)、f)、g)、h)、i)、j)、k)、l)、m)、n)
4	安全建设管理	b)、c)
5	安全运维管理	a)、b)、c)、d)

大数据应用测评指标（10/24）

序号	安全类或层面	第三级安全评估方法指标选取
1	安全物理环境	a)
2	安全通信网络	a)
3	安全计算环境	k)
4	安全建设管理	a)、b)、c)
5	安全运维管理	a)、b)、c)、d)

CSTC中国评测

大数据安全测评部分解读

安全计算环境

f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
h) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
j) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；
o) 大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。（第四级要求）

落实 ↓ ↑ 指导

安全运维管理

b) 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；
c) 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；
d) 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

等级保护测评高风险判定-安全物理环境

测评项	判例内容
机房出入口控制措施	机房出入口区域无任何访问控制措施，机房无电子或机械门锁，机房入口也无专人值守；办公或外来人员可随意进出机房，无任何管控、监控措施，存在较大安全隐患，可判高风险。
机房防盗措施	机房无防盗报警系统，也未设置有专人值守的视频监控系统，出现盗窃事件无法进行告警、追溯的，可判高风险。
机房温湿度控制措施	机房无有效的温湿度控制措施，或温湿度长期高于或低于设备允许的温湿度范围，可能加速设备损害，提高设备的故障率，对设备的正常运行带来安全隐患，可判高风险。

等级保护测评高风险判定-安全通信网络和区域边界

测评项	判例内容
网络区域划分	应按照不同网络的功能、重要程度进行网络区域划分，如存在重要区域与非重要网络在同一子网或网段的，可判定为高风险。
关键线路、设备冗余	对可用性要求较高的系统，若网络链路为单链路，核心网络节点、核心网络设备或关键计算设备无冗余设计一旦出现故障，可能导致业务中断，可判定为高风险。
互联网边界访问控制	互联网出口无任何访问控制措施，或访问控制措施配置失效，存在较大安全隐患，可判定为高风险。 与互联网互连的系统，边界处如无专用的访问控制设备或配置了全通策略，可判定为高风险。
外部网络攻击防御	关键网络节点（如互联网边界处）未采取任何防护措施，无法检测、阻止或限制互联网发起的攻击行为，可判定为高风险。
网络层恶意代码防范	主机和网络层均无任何恶意代码检测和清除措施的，可判定为高风险。

等级保护测评高风险判定-安全计算环境

测评项	判例内容
设备弱口令	网络设备、安全设备、操作系统、数据库等存在空口令或弱口令帐户，并可通过该弱口令帐户登录，可判定为高风险。
设备安全审计措施	重要核心网络设备、安全设备、操作系统、数据库等未开启任何审计功能，无法对重要的用户行为和重要安全事件进行审计，也无法对事件进行溯源，可判定为高风险。
不必要服务处置	网络设备、安全设备、操作系统等存在多余系统服务/默认共享/高危端口存在，且存在可被利用的高危漏洞或重大安全隐患，可判定为高风险。
已知重大漏洞修补	对于一些互联网直接能够访问到的网络设备、安全设备、操作系统、数据库等，如存在外界披露的重大漏洞，未及时修补更新，无需考虑是否有POC攻击代码，可判定为高风险。
测试发现漏洞修补	通过验证测试或渗透测试能够确认并利用的，可对网络设备、安全设备、操作系统、数据库等造成重大安全隐患的漏洞（包括但不限于缓冲区溢出、提权漏洞、远程代码执行、严重逻辑缺陷、敏感数据泄露等），可判定为高风险。
操作系统恶意代码防范	Windows操作系统未安装防恶意代码软件，并进行统一管理，无法防止来自外部的恶意攻击或系统漏洞带来的危害，可判定为高风险。

CSTC中国评测

相关工作

相关细化标准

信息安全技术 网络安全等级保护云计算测评指引

信息安全技术 网络安全等级保护大数据基本要求

云计算服务安全评估

2019年7月2日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部联合发布关于《云计算服务安全评估办法》（以下简称“评估办法”）的公告，并建立云计算服务安全评估工作协调机制。公告指出云服务商可向云计算服务安全评估工作协调机制办公室申请安全评估并提供相关申报材料

云计算服务安全评估主要是面向为党政机关、关键信息基础设施运营者提供云计算服务的云平台（注：前期已经通过党政部门云计算服务网络安全审查的云平台，视同为已通过云计算服务安全评估，不需要再重新申请）

云计算服务安全评估主要参照：GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》；GB/T 31167-2014《信息安全技术 云计算服务安全指南》

THANKS

第三期云课堂

时间：3月18日 下午14:30-15:20

主题：电信和互联网行业网络安全监管要求及政策解读

CSTC
中国评测

专业就是实力