云计算安全标准及合规体系简介

深圳云塔信息技术有限公司

2016年12月

个人简介

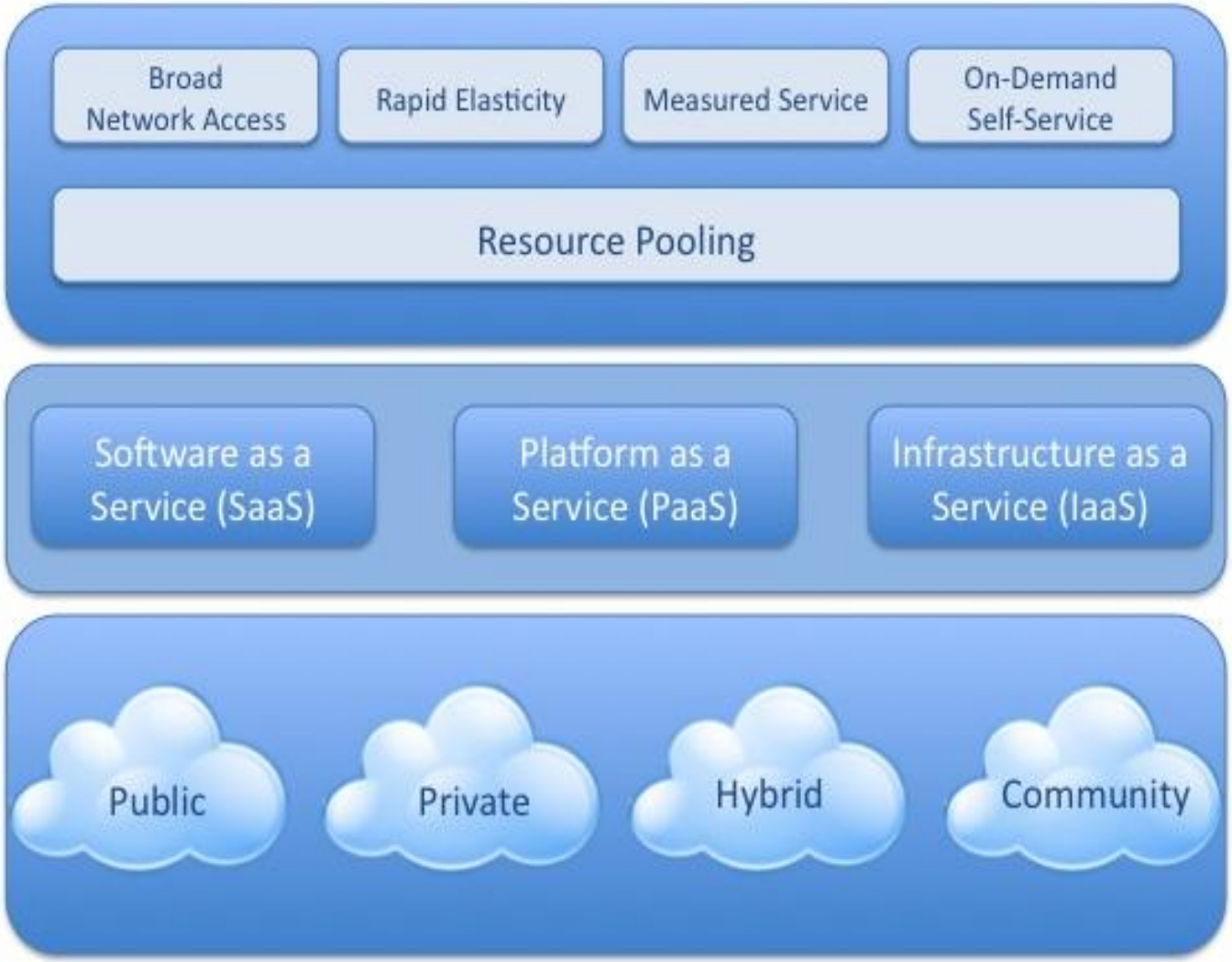
- 孙军，男，华中科技大学　硕士
- ISO27001主任审核员
- 注册信息安全专家（CISP）
- ITSS独立评估师
- IPMP国际项目管理认证
- 国家认证的系统分析师、信息系统项目管理师、软件评测师

- 云安全联盟（CSA）深圳分会秘书长
- 中国系统分析员顾问团高级顾问

- 曾在中国电信、UT斯达康、华为等公司从事软件研发、测试、信息安全等工作18年，具有扎实的理论基础和丰富的实践经验，参与多项国家标准的研制
- 现任深圳云塔信息技术有限公司COO
- 主导翻译OWASP安全测试指南一书，由电子工业出版社出版

目录

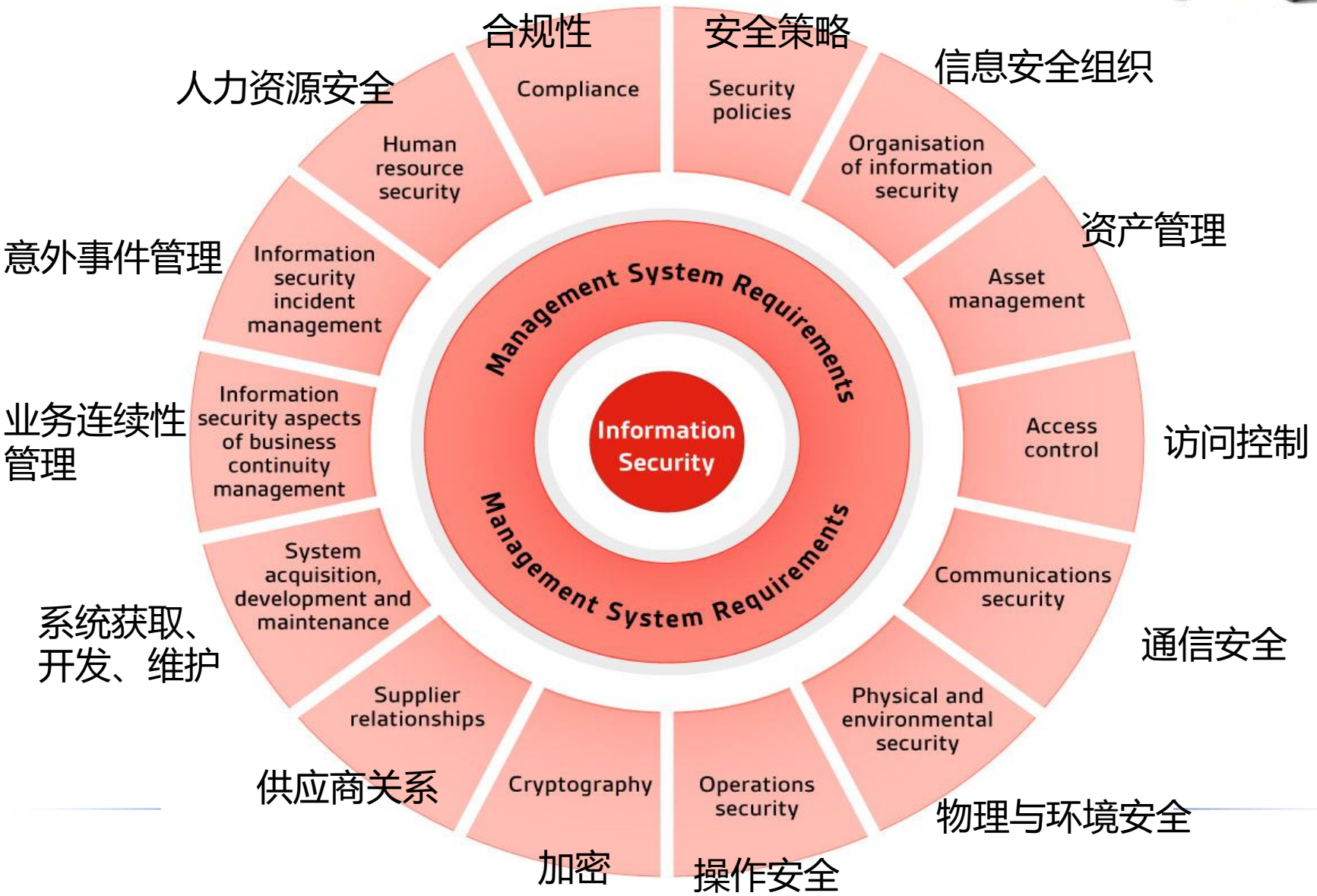
概述


Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

目录

- 云计算概述
- ISO27001、STAR/C-STAR
- 云等保
- 可信云服务认证
- ITSS云服务评估

ISO27001:2013控制域（14个）



CSA云计算关键领域安全指南V3.0

云计算介绍

- 知识域 1 - 云计算体系架构

云基础设施安全

- 知识域 7 - 传统安全、业务连续性和灾难恢复
- 知识域 8 - 数据中心运行
- 知识域 13 - 虚拟化

云安全与风险管理

- 知识域 6 - 互操作性与可移植性
- 知识域 9 - 事故响应
- 知识域 2 - 治理与企业风险管理
- 知识域 3 - 法律问题
- 知识域 4 - 合规与审核
- ENISA风险报告

云计算数据安全

- 知识域 5 - 信息管理与数据安全
- 知识域 11 - 加密与密钥管理

云应用与用户安全

- 知识域 10 - 应用安全
- 知识域 12 - 身份、授权和访问管理

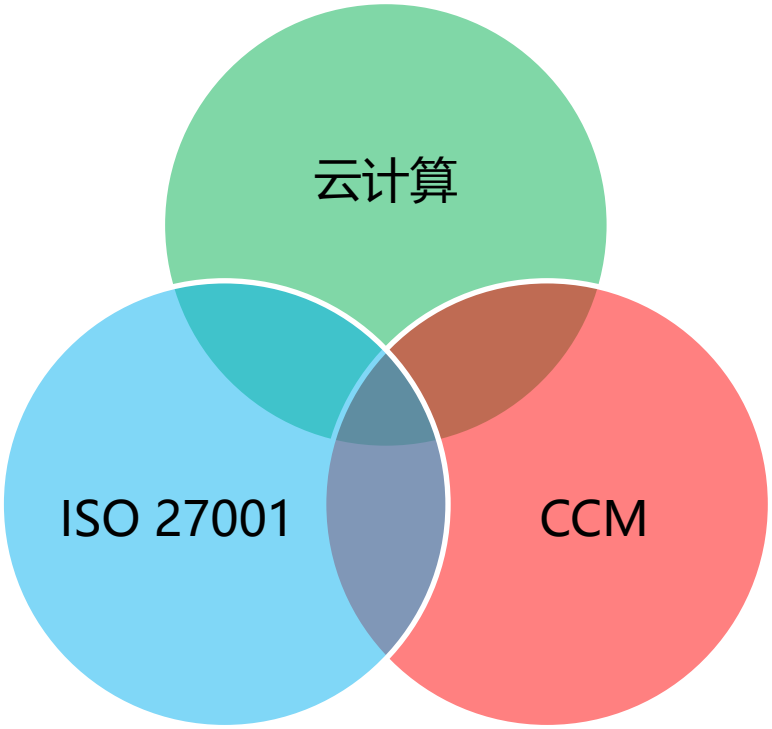
选择云服务

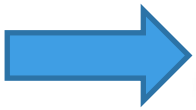
- 知识域 7 - 传统安全、业务连续性和灾难恢复
- 知识域 8 - 数据中心运行
- 知识域 14 - 安全即服务 SecaaS

CSA云控制矩阵CCM控制域（16个）

1. 应用和接口安全
2. 审核保证及合规性
3.业务连续性管理和操作弹性
4.变更控制和配置管理
5.数据安全和信息生命周期管理
6.数据中心安全
7.加密和密钥管理
8.治理和风险管理
9.人力资源
10.标识和访问管理
11.基础设施和虚拟化安全
12.互操作性和可移植性
13.移动安全
14.安全事件管理、电子证据及云端调查取证
15.供应链管理、透明性及责任
16.威胁和脆弱性管理

CSA STAR认证





C-STAR认证

C-STAR

云安全技术服务（差距分析、风险评估、能力提升）
云安全培训（CCSK、企业内训、评估师培训）
云安全评估

GB/T 22080 - 2008 信息技术- 安全技术 - 信息安全管理体系 - 要求（GB/T 22080 - 2008 Information technology - Security techniques - Information security management systems - Requirements	云控制矩阵（Cloud Controls Matrix，CCM） 16个控制域，133个控制目标，云计算安全的全方位控制体系。	GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求（GB/T 22239—2008 Information security technology — Baseline for classified protection of information system）	GB/Z 28828-2012 信息安全技术公共及商用服务信息系统个人信息保护指南（GB/Z 28828—2012 Information security technology - Guideline for personal information protection within information system for public and commercial services）

目录

- 云计算概述
- ISO27001、STAR/C-STAR
- 云等保
- 可信云服务认证
- ITSS云服务评估

等保2. 0时代到来

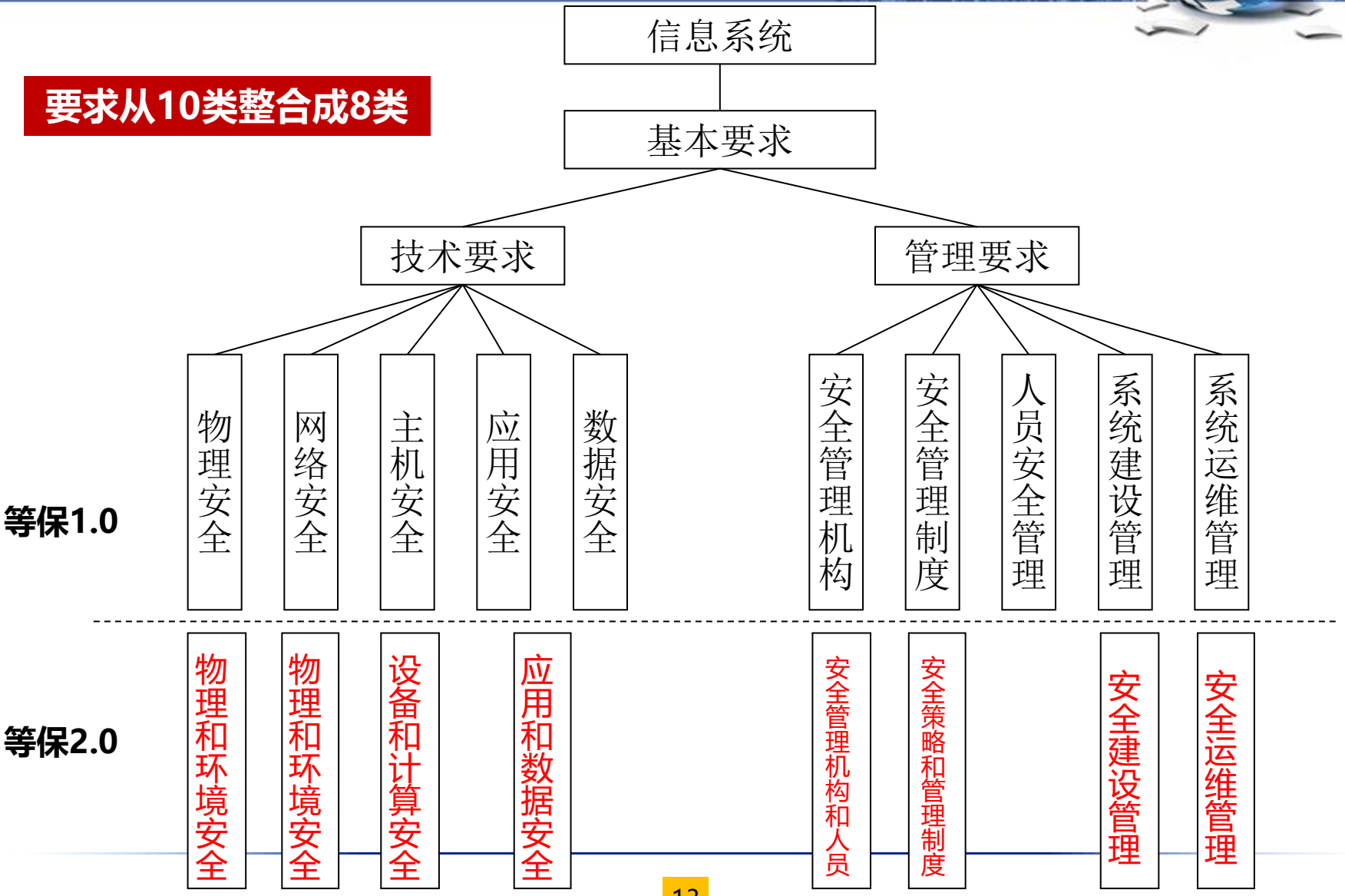
- GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》

- GB/T 22239.1-XXXX 信息安全技术 网络安全等级保护基本要求 第1部分 安全通用要求；
- GB/T 22239.2-XXXX 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 22239.3-XXXX 信息安全技术 网络安全等级保护基本要求 第3部分 移动互联安全扩展要求；
- GB/T 22239.4-XXXX 信息安全技术 网络安全等级保护基本要求 第4部分 物联网安全扩展要求；
- GB/T 22239.5-XXXX 信息安全技术 网络安全等级保护基本要求 第5部分 工业控制安全扩展要求；
- GB/T 22239.6-XXXX 信息安全技术 网络安全等级保护基本要求 第6部分 大数据安全扩展要求

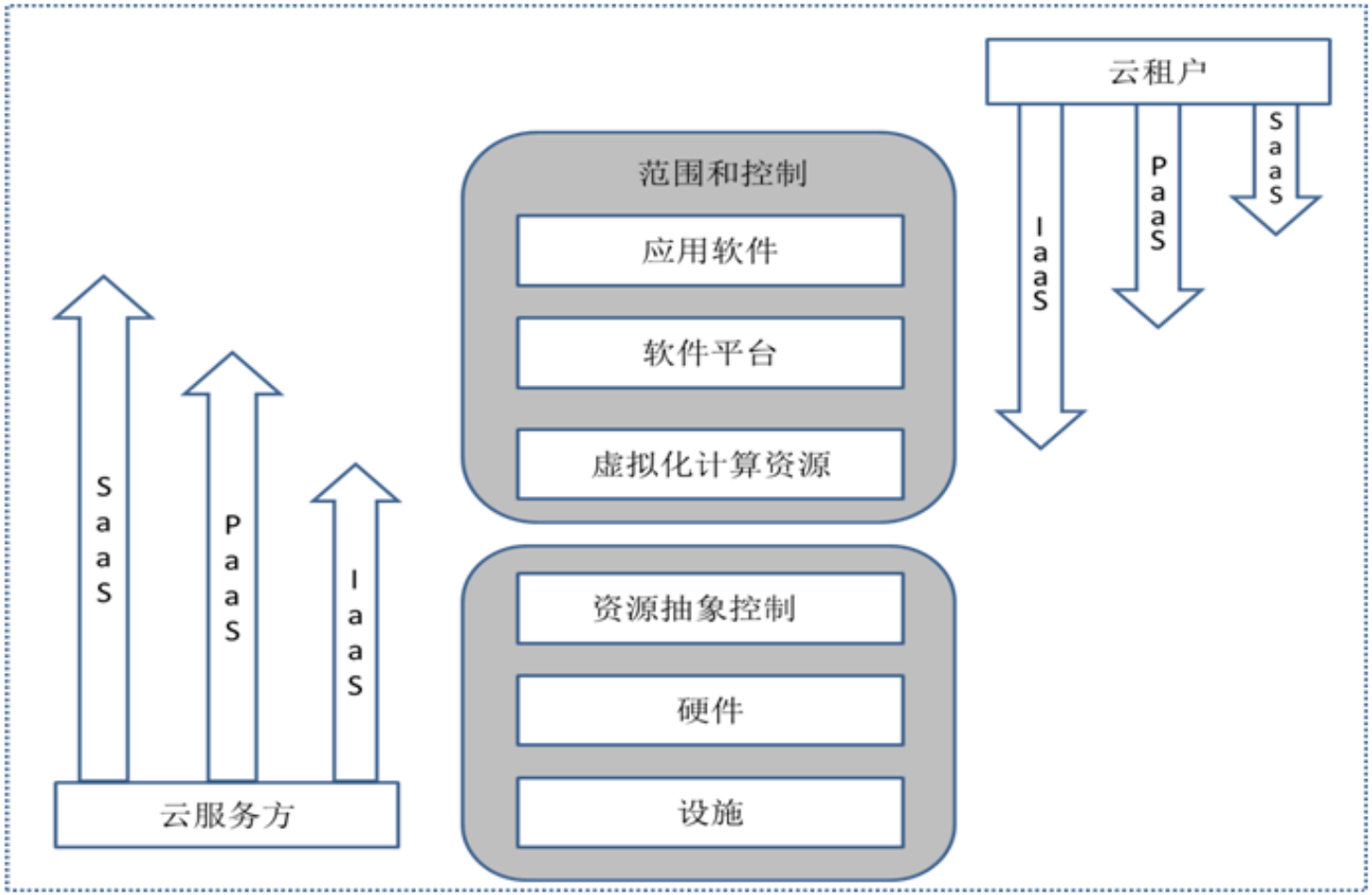
标准从1个扩展为6个

等级保护基本要求

要求从10类整合成8类



云等保明确了云服务商和云租户的责任



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。

相关标准

- GB/T 31167-2014《信息安全技术 云计算服务安全指南》
  - 面向政府部门，提出了使用云计算服务时信息安全管理和技术要求，尤其是使用社会化的云计算服务时，应特别关注的安全问题。

- GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》
  - 面向云服务商，提出云服务商向政府部门提供服务时应具备的安全能力要求，要求分为一般要求和增强要求。

目录

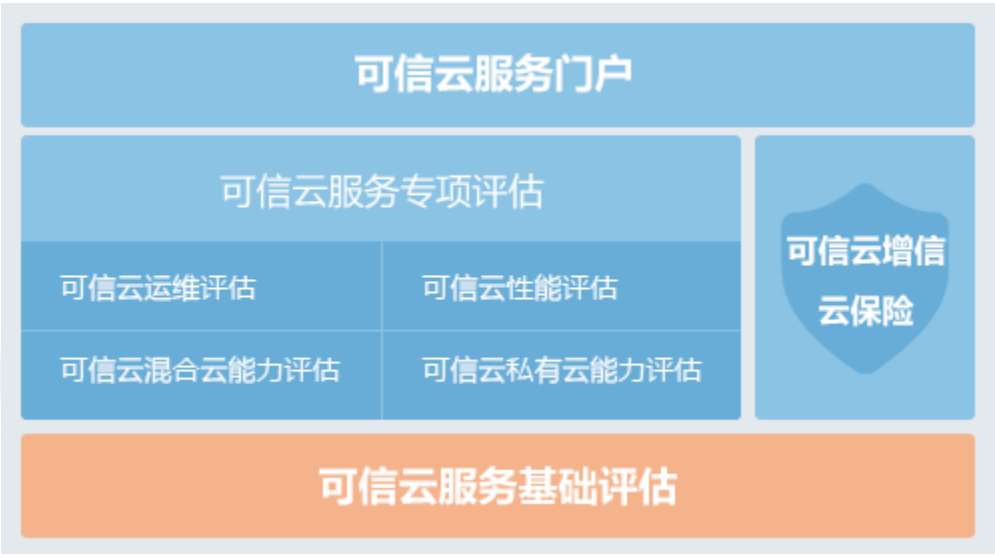
- 云计算概述
- ISO27001、STAR/C-STAR
- 云等保
- 可信云服务认证
- ITSS云服务评估

可信云简介

数据中心联盟
Data Center Alliance

TRUCS
可信云服务认证

CAICT 中国信息通信研究院
China Academy of Information and Communications Technology



可信云评估方法和内容

评估方法

文档审核 | 技术测评 | 现场查验 | 技术专家评审 | 外部复审

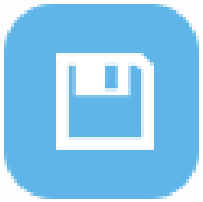
事中监测

云主机可用性和性能检测 | PAAS平台可用性和性能检测

数据安全	服务质量	权益保障	+ 专项评估
存储持久性	服务功能	变更、终止条款	服务性能
数据可销毁性	服务可用性	赔偿条款	
数据可迁移性	资源调配能力	用户约束条款	
数据私密性	故障恢复能力	服务商免责条款	运维管理
数据知情权	网络接入性能		
服务可审查性	服务计量准确性		

可信云评估对象：12项云服务评估

云主机

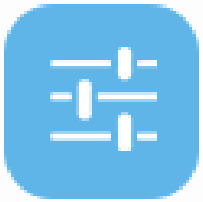


对象存储

块存储

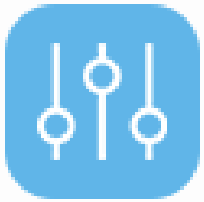
云引擎

云缓存



本地负载均衡

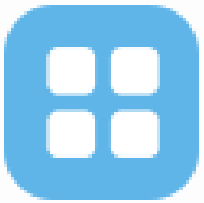
云分发



全局负载均衡

云桌面

企业移动化管理服务



在线应用

云数据库

目录

- 云计算概述
- ISO27001、STAR/C-STAR
- 云等保
- 可信云服务认证
- ITSS云服务评估

依据

- 国家标准：《信息技术 云计算 云服务运营通用要求》（报批中）
- 《推动云计算创新发展培育信息产业新业态的意见》（国发[2015]5号）
- 《云计算综合标准化体系建设指南》（工信厅信软〔2015〕132号）

概况

- 中国电子工业标准化技术协会信息技术服务分会(ITSS分会)
- 评估机构
  - 中国电子技术标准化研究院（赛西）
  - 中国软件评测中心
  - 工业和信息化部电子第五研究所（赛宝）
- 对象：公有云、私有云
- 级别：基础级、增强级

评估内容


人员结构
岗位结构
人员技能
人员
运营管理层
运维操作层
流程
资源
计算资源
存储资源
网络资源
支撑环境
技术
资源池化
计量
监控
调度
安全保障

评估方法


文档审查
对云服务的技术、管理、运营等文档的完整性、准确性和一致性进行审查。
技术测评
利用专业测试手段或测试工具，对云服务的功能、性能、安全等进行测试。
现场抽查
对云服务的实际运营情况、服务记录情况等进行现场检查，检查其是否符合相关要求。
访谈人员
通过访谈的方式，向云服务的管理人员、技术人员、运维人员等人了解云服务运营的具体措施与实施情况。

云计算安全学习指引

CCSP

Certification of Cloud Security Professional 云计算安全专家认证

由CSA和ISC²(国际信息安全认证联盟)2015年联合推出，是CCSK的进阶认证

进阶

CCSK

Certification of Cloud Security Knowledge 云计算安全知识认证

2011年CSA正式推出，经过5年发展，已经成为云安全人才领域最权威的认证之一

C-CCSK

中国CCSK认证及考试

C-CCSK™
China-Ceritificate of
Cloud Security Knowledge

謝謝！

地址：深圳市南山区高新南七道数字技术园A3栋5楼
热线：400-991-7218
http://www.cloudta.net