云服务安全解决之道

Solutions to the security issues of cloud services

赛宝认证中心 CEPREI Certification Body

刘小茵

香港 2014.06.19

提纲

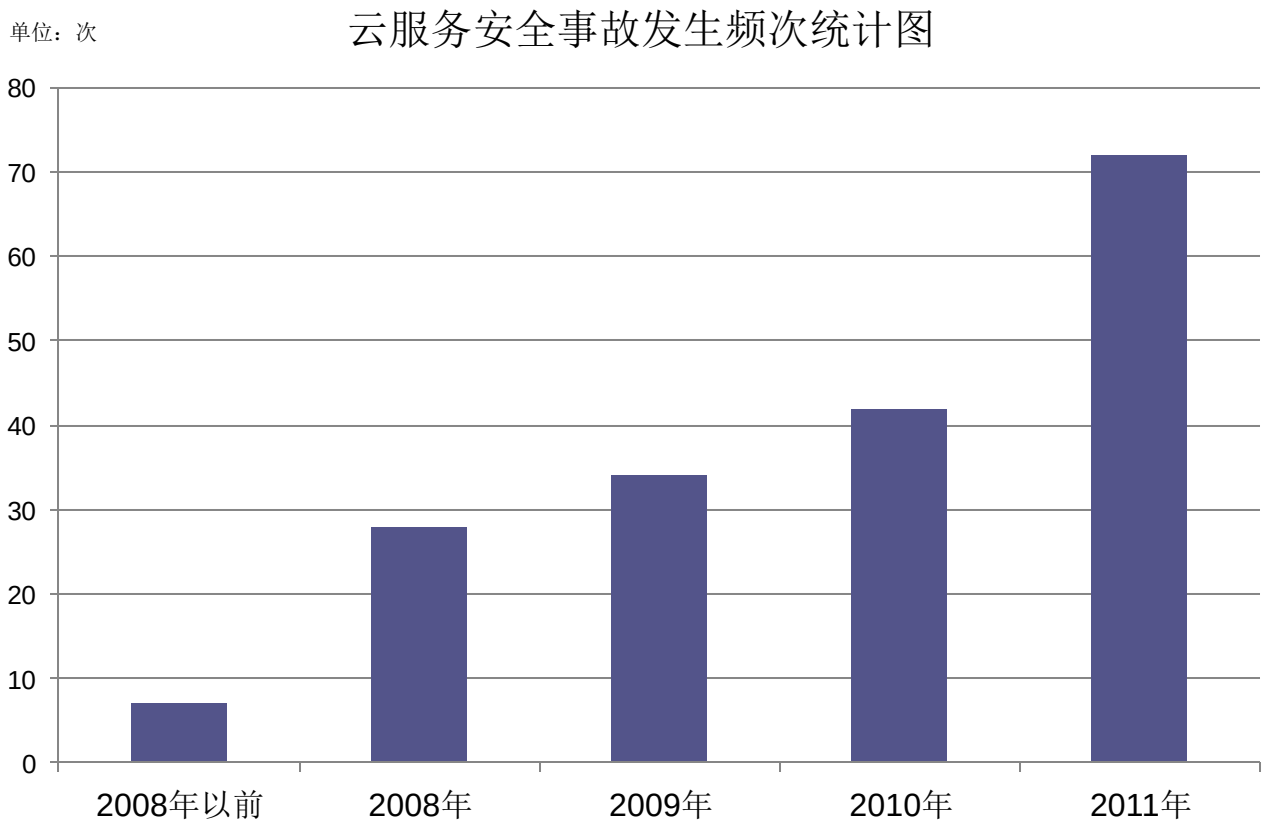
1 云服务安全所面临的问题

2 云服务安全解决之道：风险评估

3 云服务安全解决之道：安全管理

4 云服务安全解决之道：评估评价

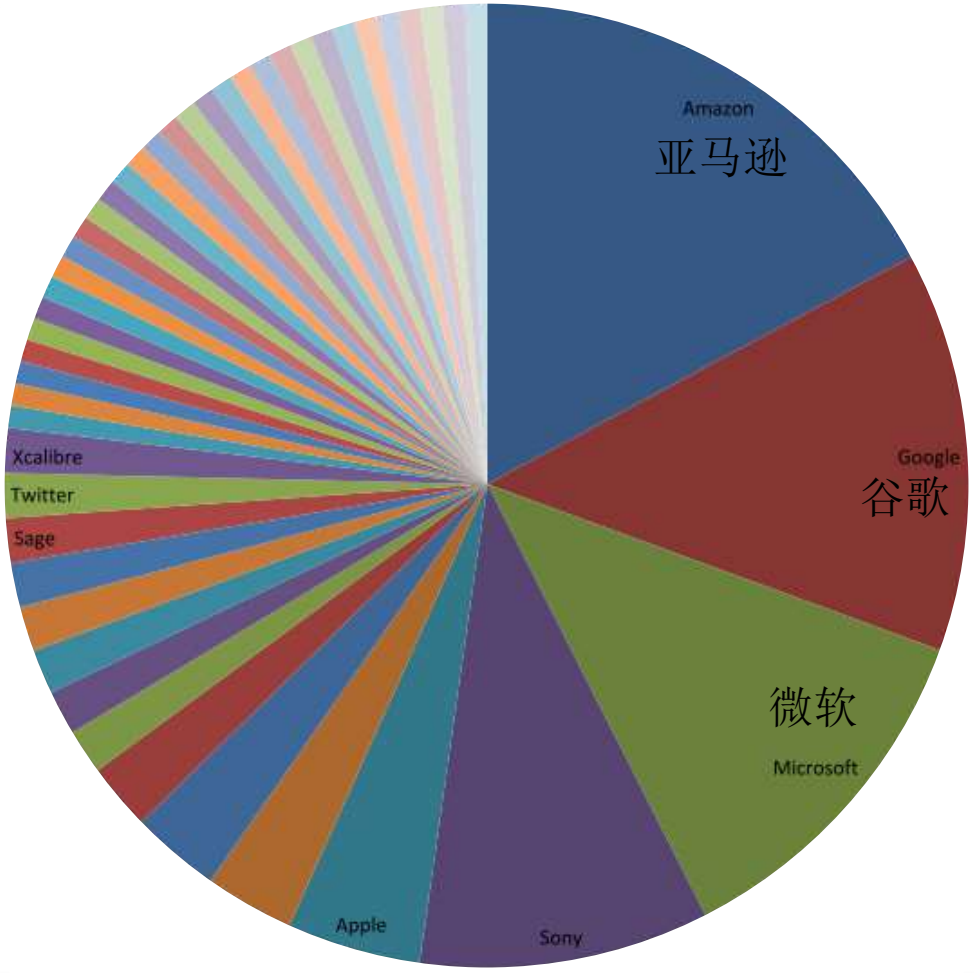
云服务安全事故统计



2010年至2011年被报告的安全事故数量翻倍

来源：CSA 2013云安全事故统计

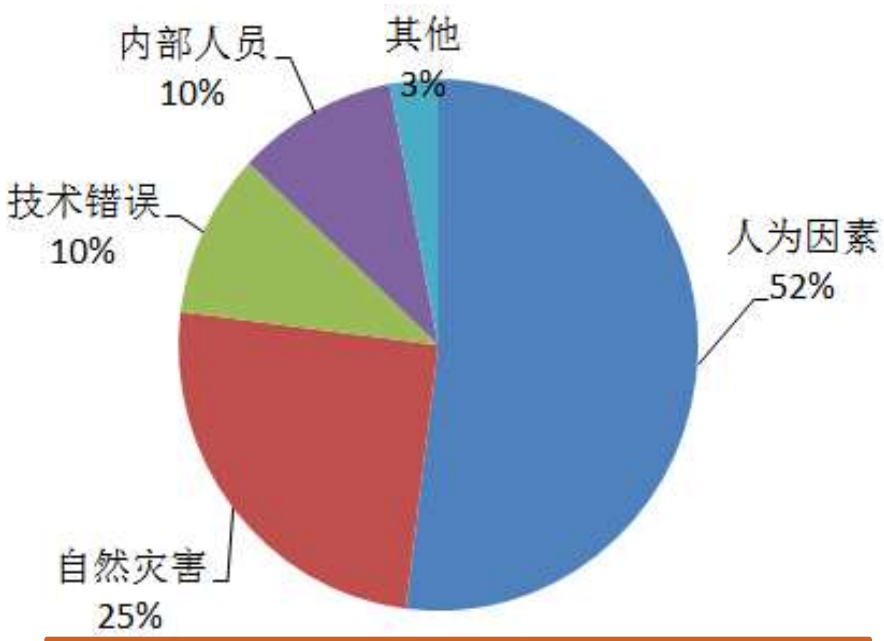
云服务安全事件统计



云安全事故
知名云服务企业均榜上有名

来源：CSA 2013云安全事故统计

安全是信息产业领域永恒的主题



信息安全事件中
属于管理方面原因比重高达**70%**以上

云计算的安全问题大部分是传统IT就存在的安全问题：

传统的信息安全理论仍旧对解决云计算安全适用

剩下的部分安全问题来自于：

- 新的服务模式带来的潜在问题
- 新技术的使用带来的新的管理问题
- 老技术的新用法带来的安全问题的扩大化

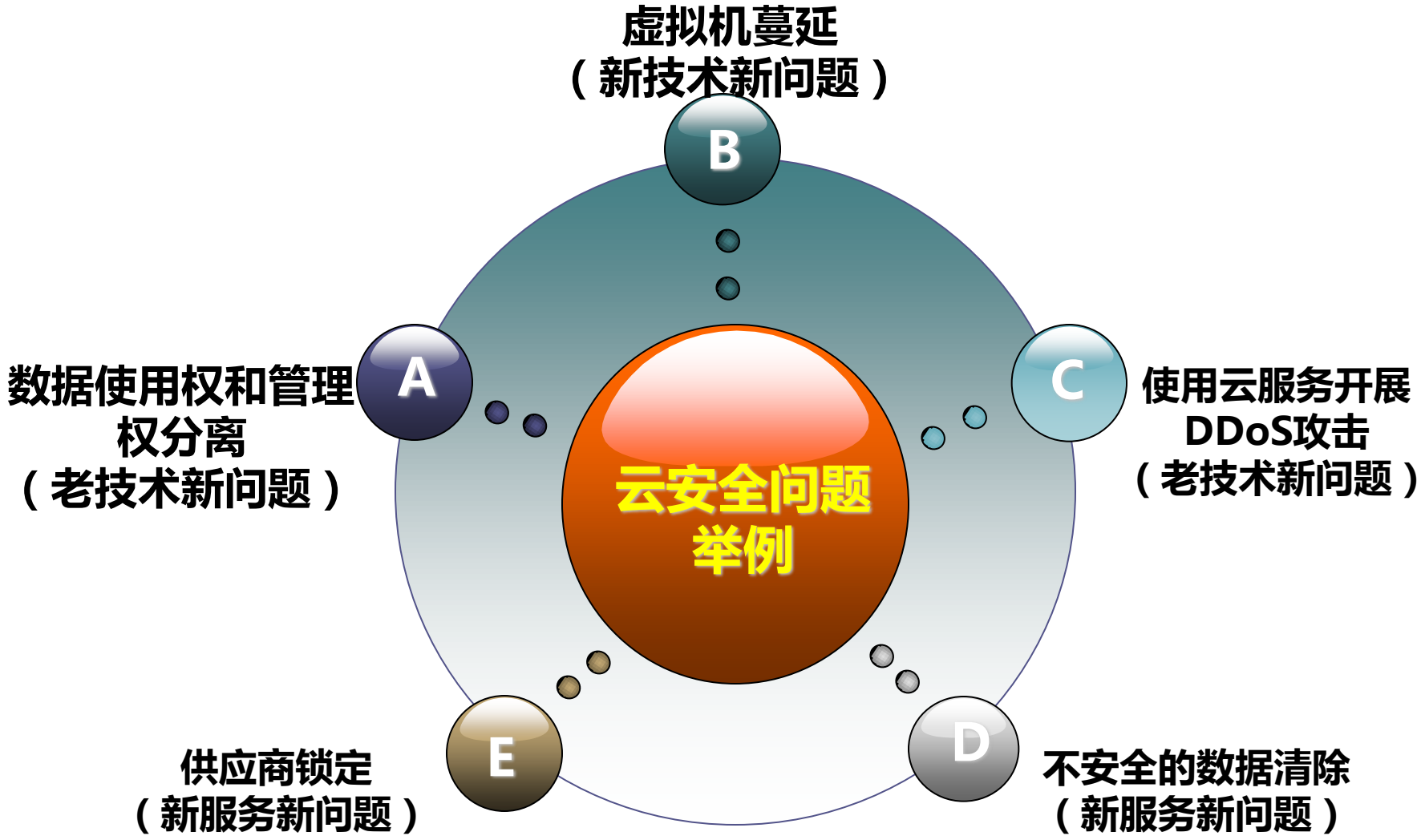
云计算重点关注风险

云计算重点关注风险


1.供应商锁定
2.控制权丧失
3. 符合性挑战
4. 商业声誉丧失
5. 服务中断
6. 云服务提供商并购
7. 服务供应链问题
1.电子证据
2. 数据审查风险
3. 数据保护风险
4. Licence风险
1. 资源耗尽
2. 隔离失效
3. 恶意内部人员
4. 数据传输丢失
5. 数据泄漏
6. 不安全的数据清除
7. DDoS；8. EDoS
9. 密钥丢失
10. 恶意扫描
11. 服务管控失效
12. 责任不清
13. 管理接口威胁

其他风险（不限云计算）

1. 网络中断	2. 网络管理失效
3. 修改网络流量	4. 程序后门
5. 社会工程攻击	6. 操作记录遗失
7. 安全记录遗失	8. 备份丢失
9. 未授权访问	10. 设备失窃
11. 自然灾害	


虚拟机蔓延
（新技术新问题）
B
数据使用权和管理权分离
（老技术新问题）
A
C
使用云服务开展DDoS攻击
（老技术新问题）
云安全问题举例
E
D
供应商锁定
（新服务新问题）
不安全的数据清除
（新服务新问题）

云安全问题归类

新技术新问题

电子证据
数据审查风险（M）
数据保护风险
Licence风险（M）
数据泄漏
EDoS（M）

老技术新问题

控制权丧失
符合性挑战（M）
隔离失效
恶意内部人员（M）
数据传输丢失
DDoS
密钥丢失
恶意扫描

新服务新问题

供应商锁定（M）
商业声誉丧失（M）
服务中断
云服务提供商并购（M）
服务供应链问题（M）
资源耗尽
服务管控失效（M）
责任不清（M）
管理接口威胁
不安全的数据清除

注：（M）代表主要是管理类问题

三分技术，七分管理

统计数据表明，在所有的计算机安全事件中，

人

10

由

比

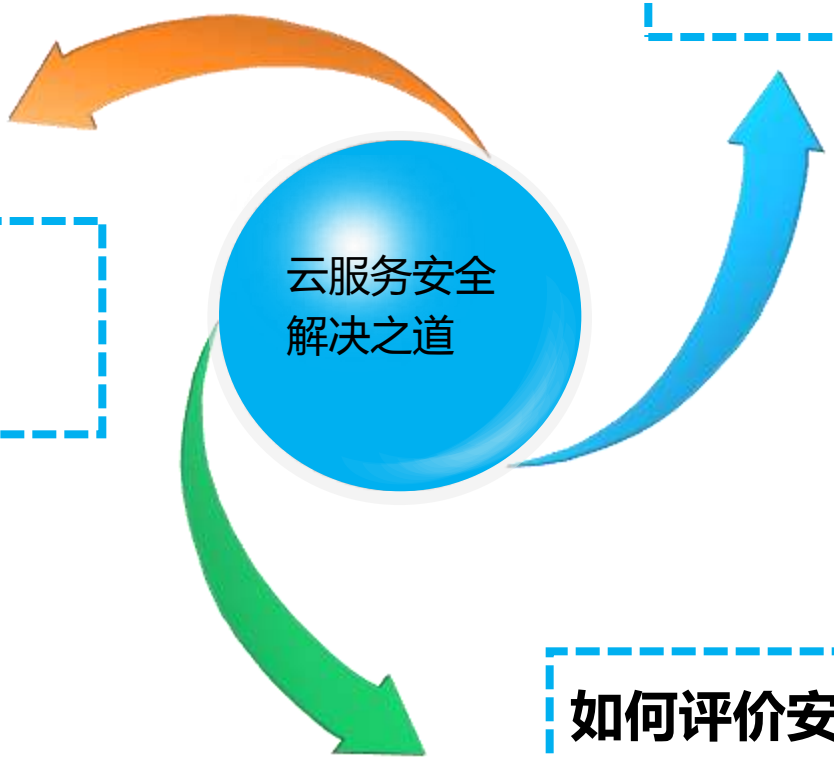
以通过科学的信息安全管理来避免。

这一结论

同样适用于云计算环境下

云服务解决之道

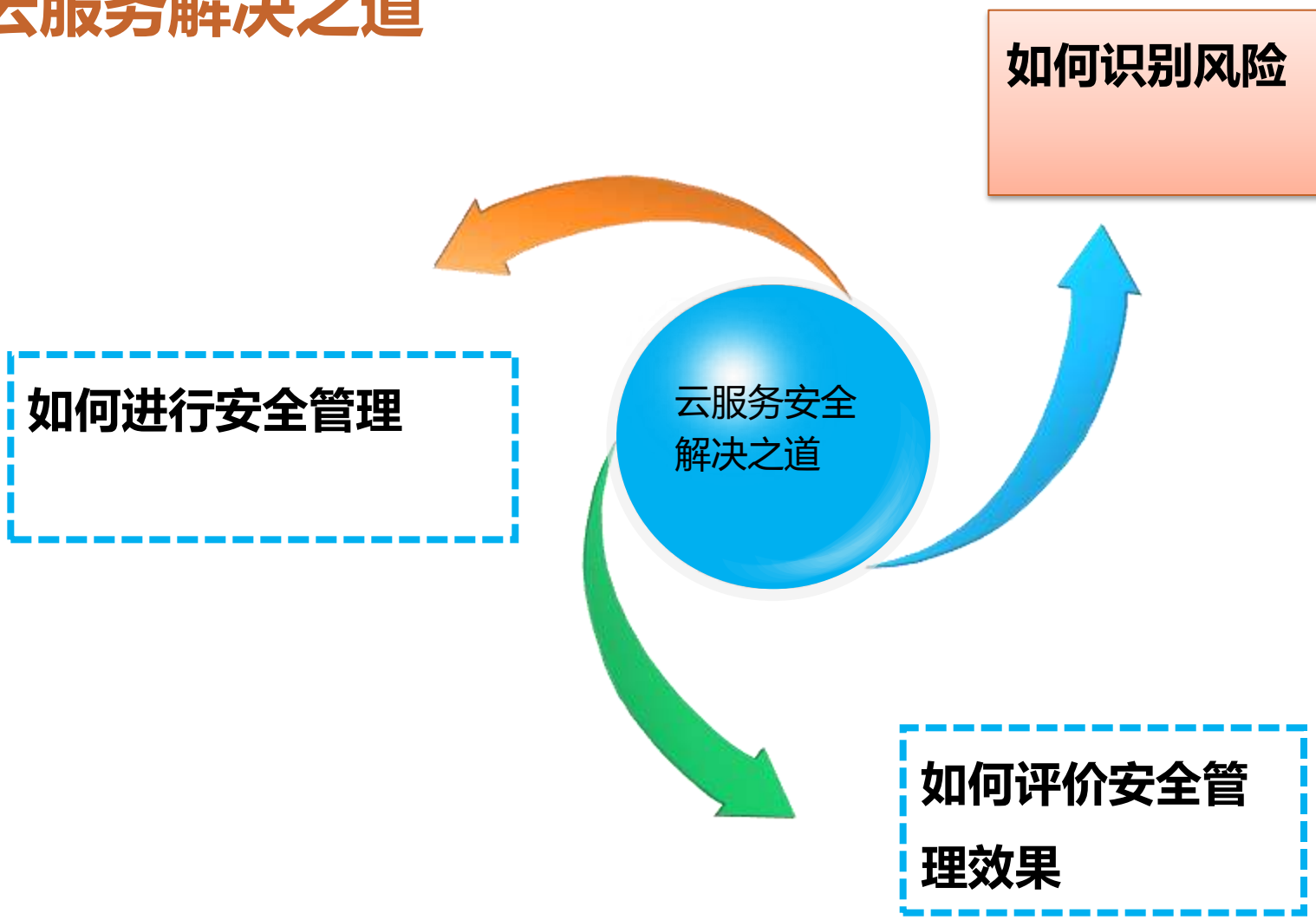
如何识别风险



如何进行安全管理

如何评价安全管理效果

云服务解决之道



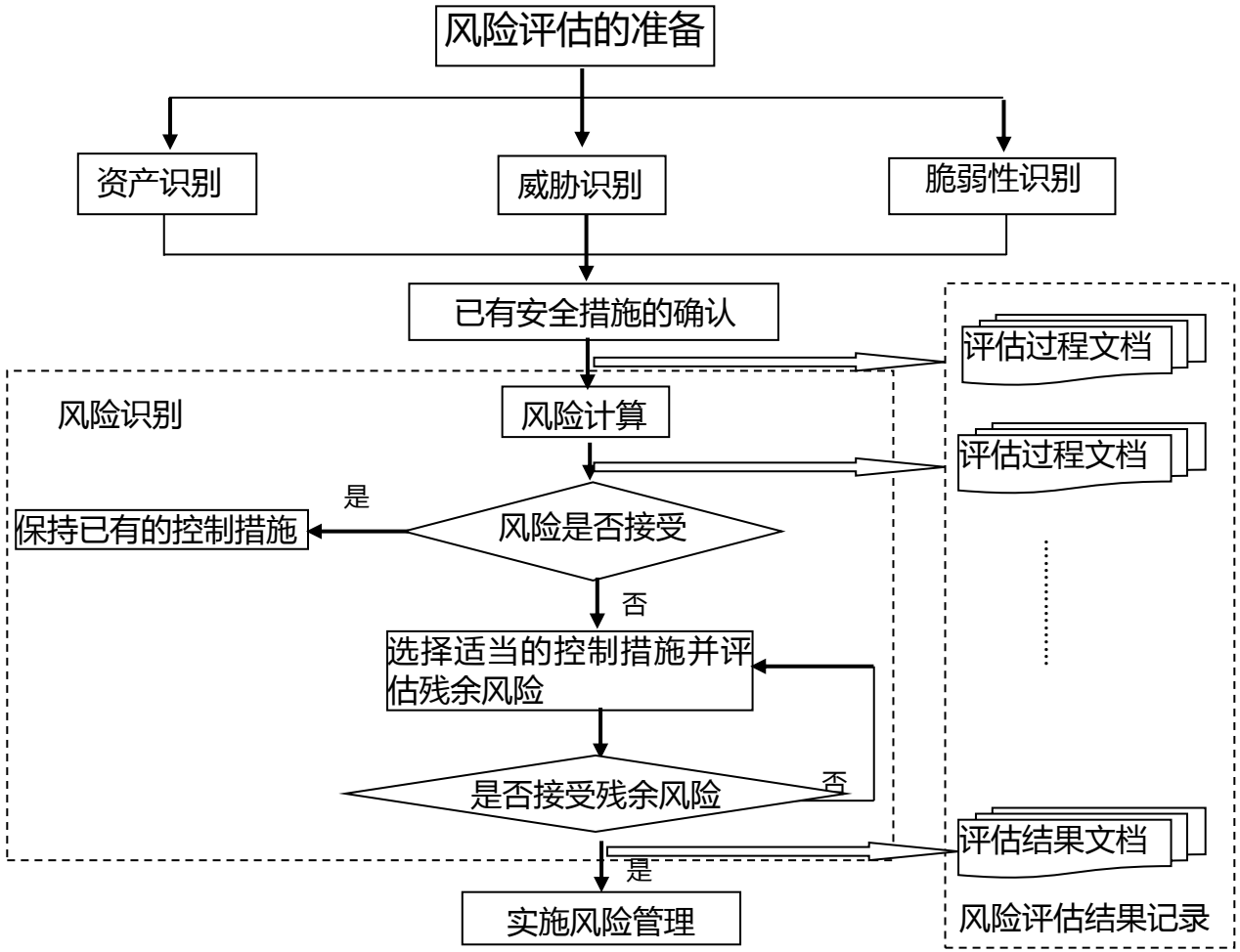
云服务解决之道：风险评估

《云计算基础设施平台
信息安全风险评估规范》

云服务解决之道：风险评估

- ✓ 通过风险评估导出信息系统的安全需求，信息安全建设以风险评估为起点，控制安全风险，保障云服务正常安全开展
- ✓ 通过对云服务业务系统潜在风险要素的识别、分析、评价，发现云服务业务系统的安全风险，通过安全加固，使高风险降低到可接受的水平，从而提高信息安全风险管理的水平
- ✓ 正确、全面地了解和理解安全风险，决定如何处理安全风险，在信息安全的投资、信息安全措施的选择、信息安全保障体系的建设等问题中做出合理的决策
- ✓ 持续的风险评估工作可以成为检查云服务业务系统负责单位或部门的绩效的有力手段

云服务解决之道：风险评估

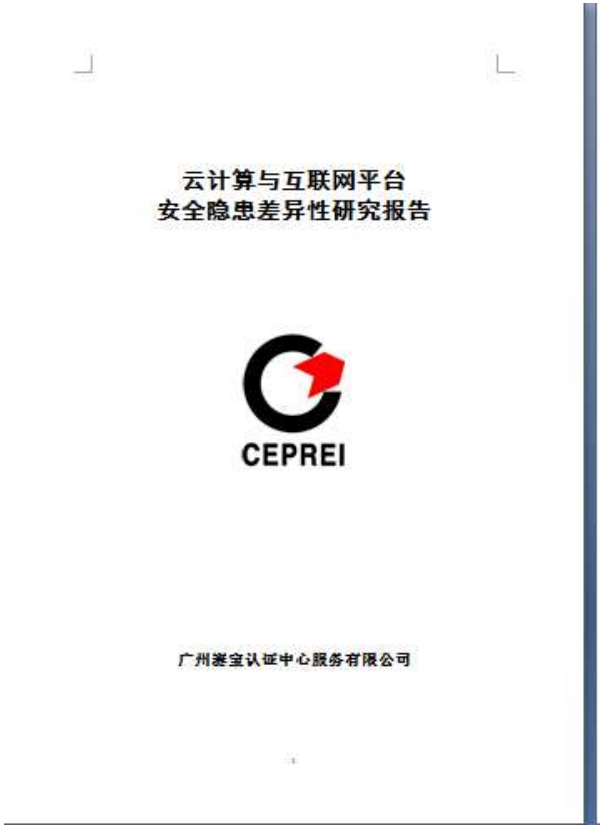


风险评估总体流程：
整体风险评估流程按照《GB/T 20984信息安全技术信息安全风险评估规范》进行

整个风险评估流程中的重点在于资产识别、威胁识别、脆弱性识别和已有安全措施的确认。依据**CSA、ENISA、OWASP、Gartner**等最新研究成果对规范进行更新

给出**云计算重点领域**的具体化的安全评估规范：**多租户、虚拟化、数据安全、业务连续性**等领域

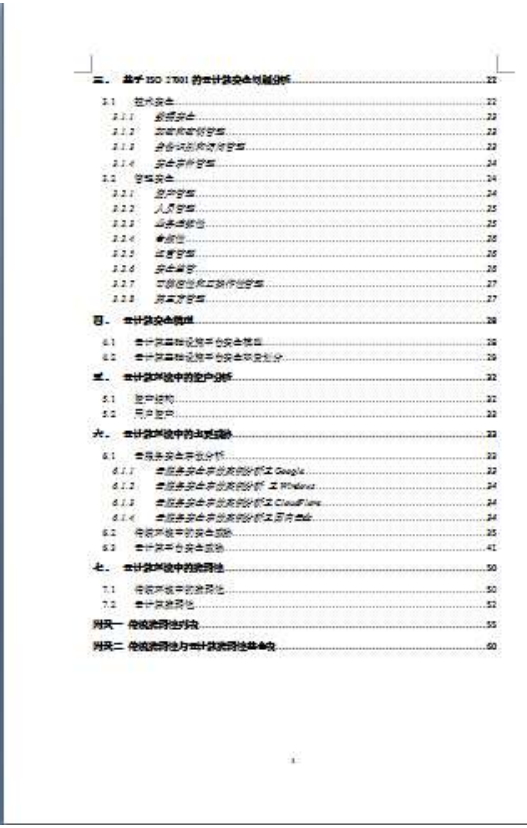
云服务解决之道：风险评估



云计算与互联网平台
安全隐患差异性研究报告

CEPREI

广州赛宝认证中心服务有限公司



云服务解决之道：风险评估

虚拟化安全的评估（例）

虚拟基础设施架构设计评估：专门针对网络、服务器和虚拟机隔离以及虚拟基础设施管理设计，评估虚拟基础设施的架构和设计的安全性。

虚拟基础设施选型：在虚拟化工具选择方面是否结合业务需求及IT架构的情况，针对开源的工具是否考虑了其获取渠道的安全性，虚拟机的可移植性和互操作性如何。

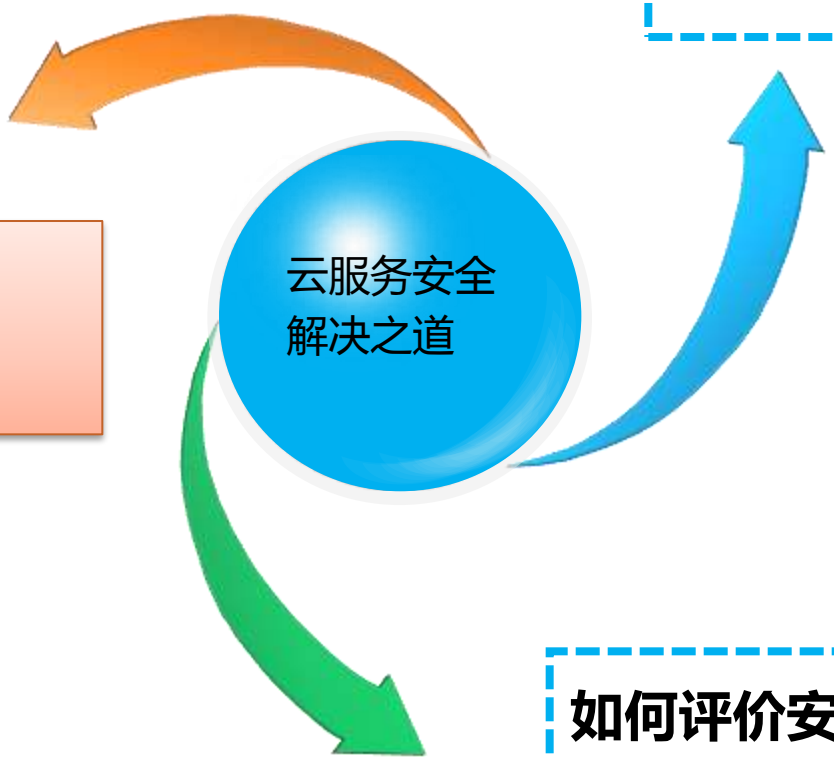
虚拟基础设施配置检查：评估虚拟机和服务器的配置是否安全。针对虚拟化软件漏洞的扫描器能够快速定位虚拟化软件自身缺陷漏洞，同时对Hypervisor的访问控制进行检查与加固，不允许对Hypervisor进行未经授权的更改。

虚拟网络评估：对实际网络、虚拟逻辑网络、虚拟管理中心以及虚拟安全设备（如虚拟火墙）进行评估与安全测试，特别对云管理员的角色权限要进行检查与测试，避免有权限失效的漏洞。

安全评估检查表（例）				
评估领域	**安全特性**	**评估内容**	**评估手段**	**评价结果**
虚拟基础设施架构设计评估	保密性	不同安全级别的虚拟网络隔离	查看网络拓扑图、现场测试不同网络间的访问控制	
		网络安全防护机制	渗透性测试、查看过往安全事件记录及处理、结合风险评估查看网络拓扑图	
		多租户安全管理	查看多租户管理策略、查看Hypervisor的用户权限管理策略、渗透性测试	
	完整性	虚拟机变更（包括配置变更、环境变更、安全设置变更等）检测	检查Hypervisor监控功能中是否有虚拟机变更提醒/报警功能	
	可用性	虚拟机安全迁移	查看是否建立了安全链路、回退机制，及虚拟化管理平台的兼容性如何	
		脆弱性管理	使用漏洞扫描工具、查看补丁更新时间、检查管理机制	
		虚拟化环境的可扩展性	检查虚拟化环境对于主流虚拟化工具的支持程度	

云服务解决之道

如何识别风险



如何进行安全管理

如何评价安全管理效果

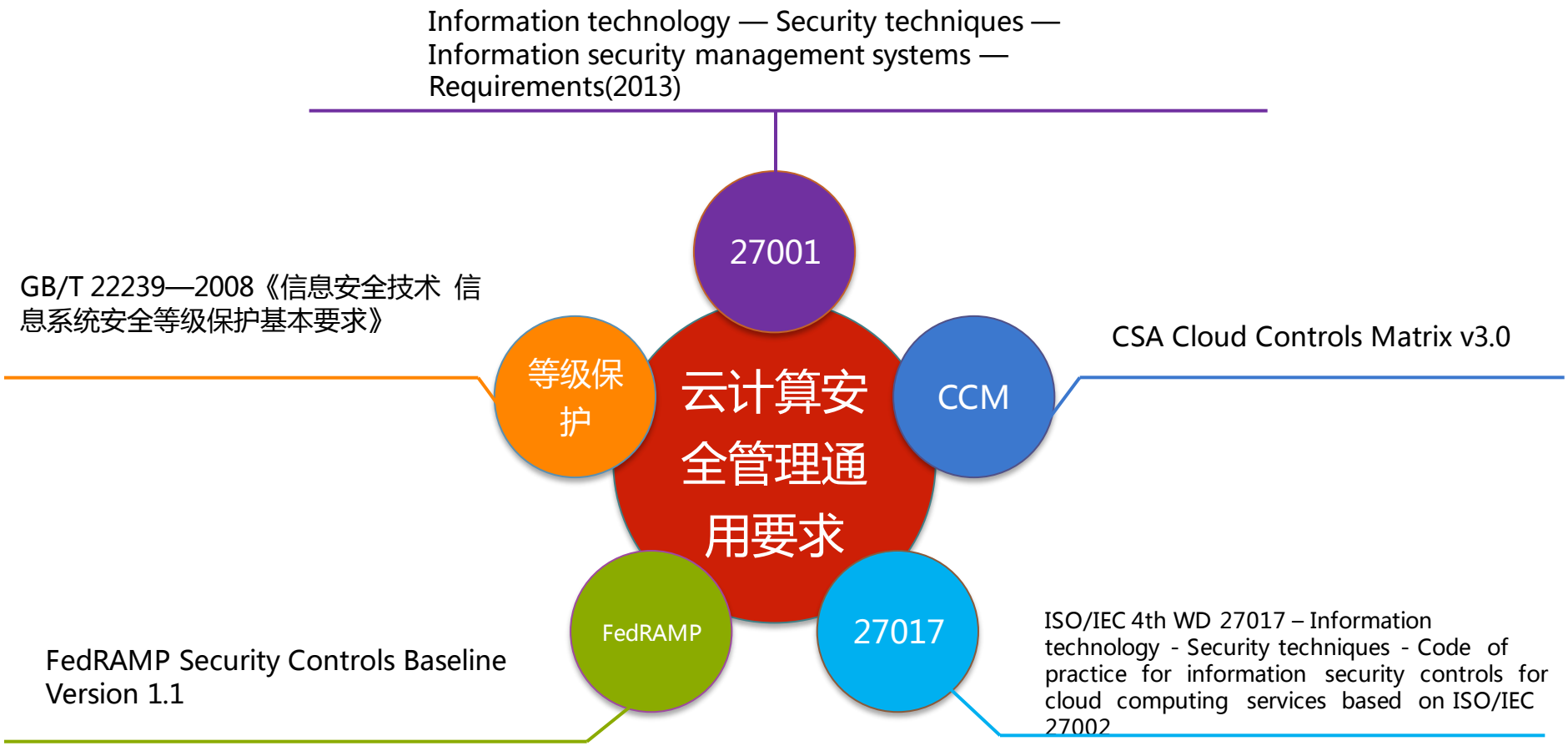
云服务解决之道：安全管理

《云计算安全管理通用要求》

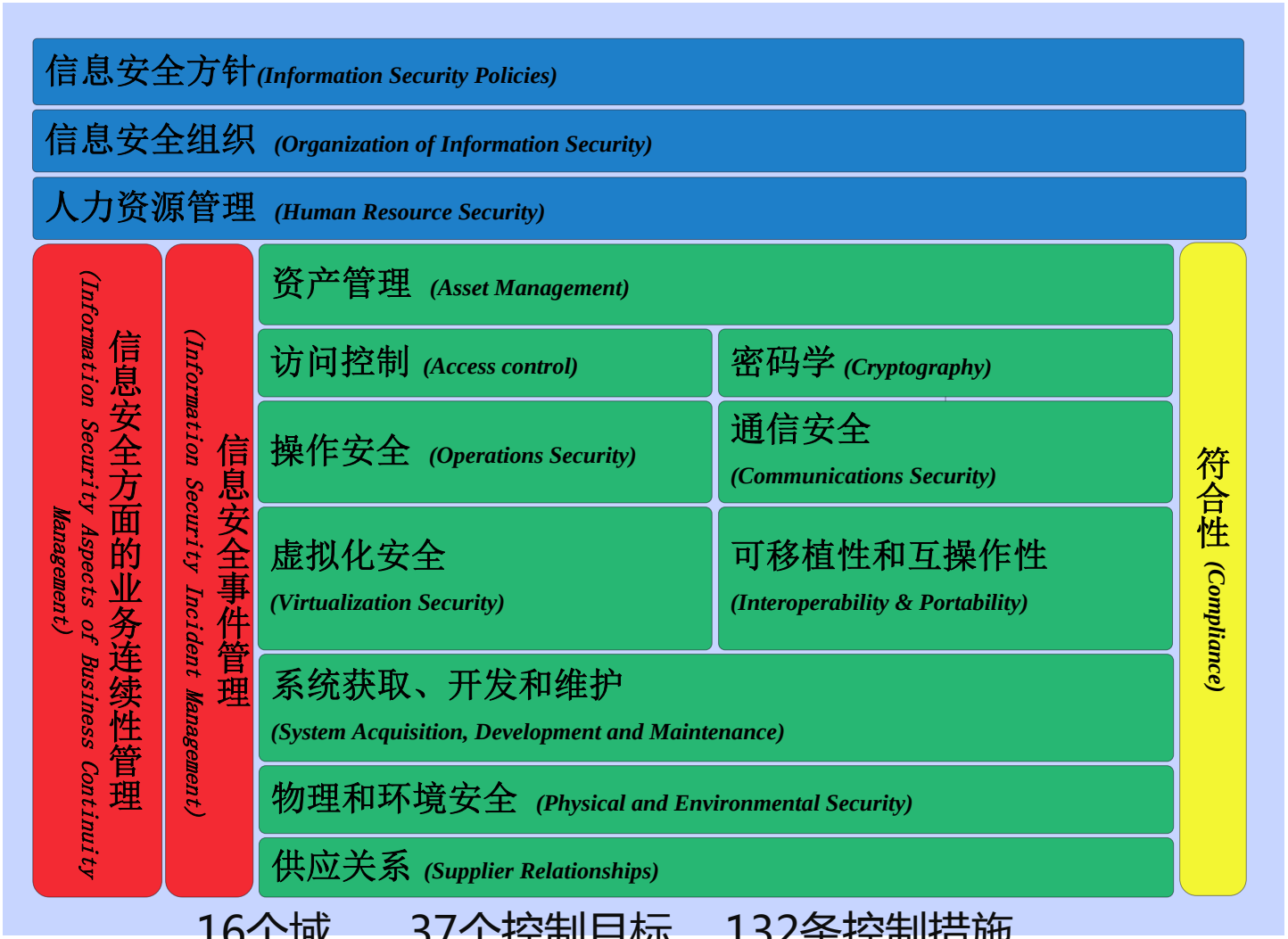
Cloud Computing Security Management – General Requirements

包含16个域、37个控制目标、132条控制措施

云服务解决之道：安全管理



云服务解决之道：安全管理



16个域　37个控制目标　132条控制措施

控制域 	是否是新增域 √X	更新控制数 	新增控制数 	总控制数 ALL
1 安全方针	×	2	0	2
2 信息安全组织	×	3	0	8
3 人力资源管理	×	2	2	8
4 资产管理	×	6	2	10
5 访问控制	×	11	0	14
6 密码学	×	2	0	2
7 物理和环境安全	×	0	0	15
8 操作安全	×	5	0	14
9 通信安全	×	3	0	7
10 系统获取、开发和维护	×	2	0	13
11 供应关系	×	3	0	5
12 信息安全事件管理	×	4	2	9
13 信息安全方面的业务连续性管理	×	4	0	4
14 符合性	×	3	3	11
15 虚拟化安全	√	0	5	5
16 可移植性和互操作性安全管理	√	0	5	5

《云计算安全管理通用要求》更新域—示例

依据CCM SEF-03进行更新
Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to.....
强调云计算参与各方的互相配合与协调

依据等级保护8.2.5.12（G4）进行更新
应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点

12、信息安全事件管理		
12.1 信息安全事件的管理和改进 *目标*：确保持续、有效地管理信息安全事件，包括对安全		
12.1.1	职责和规程	*控制措施* 应建立管理职责和规程，明确组织内部人员、租户及其他相关各方的职责，确保快速、有效和有序地响应信息安全事件
12.1.2	报告信息安全事态	*控制措施* 应与组织内部人员、租户及其他相关各方报告的渠道，定期进行信息安全事态报告，全事态尽可能快地通过适当的管理渠道进
12.1.3	报告信息安全弱点	*控制措施* 应要求信息系统和服务的所有雇员 方人员记录并报告他们观察到的或怀疑的任何系统或服务的安全弱点，任何情况下用户均不应尝试验证弱点。
12.1.4	评估和确定信息安全事态	*控制措施* 信息安全事态应被评估，并且确定是否划分成信息安全事件。
12.1.5	信息安全事件响应	*控制措施* 应具有与信息安全事件响应相一致的文件化规程。应严格控制参与涉及关键或机密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案。

《云计算安全管理通用要求》更新域—示例

12、信息安全事件管理		
12.1 信息安全事件的管理和改进 *目标*：确保持续、有效地管理信息安全事件，包括对安全事件和		
12.1.6	信息安全事件通报	*控制措施* 提供商应当将信息安全事件的相关信息以便捷的方式，如网页页面的形式，告知受其影响的租户、供应商及其他相关方。
12.1.7	信息安全事件应急响应测试	*控制措施* 信息安全事件应急响应计划应定期或在组织和环境发生重大变更之时进行测试。信息安全事件应急响应计划应当包含受其影响的租户及其他相关
12.1.8	对信息安全事件的总结	*控制措施* 从信息安全事件的分析和解决过程中所获取 被用于降低事件在未来发生的可能性或影响
12.1.9	收集证据	*控制措施* 组织应定义和应用用于识别、收集、获取和 为证据的信息的程序。应提供一定的透明机制，确保受到该安全事件影响的租户及其他相关方在一定范围内具有参与该调查的机会。

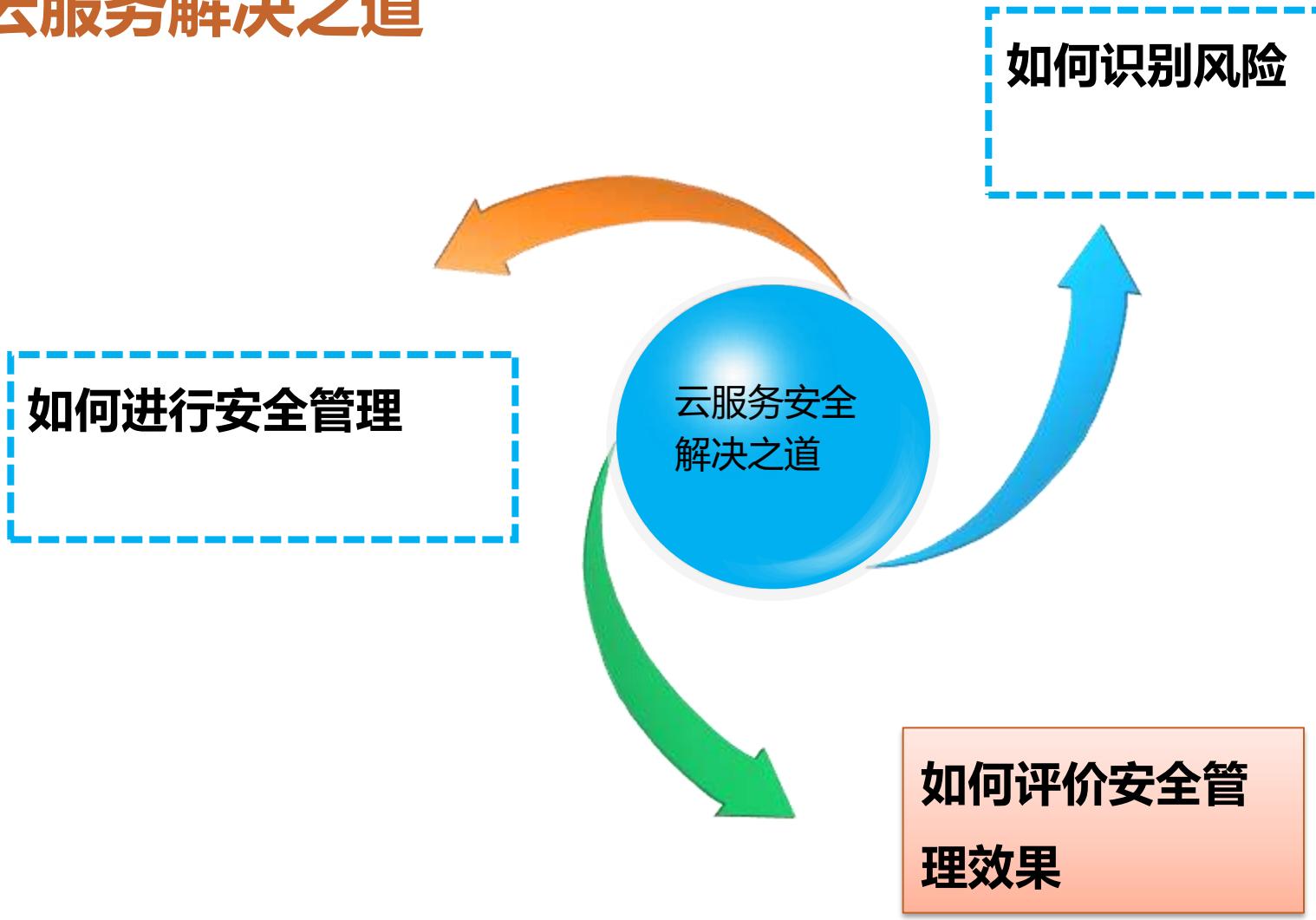
依据CCM STA-02进行新增
The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).

依据CCM BCR-02进行新增
Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. ……

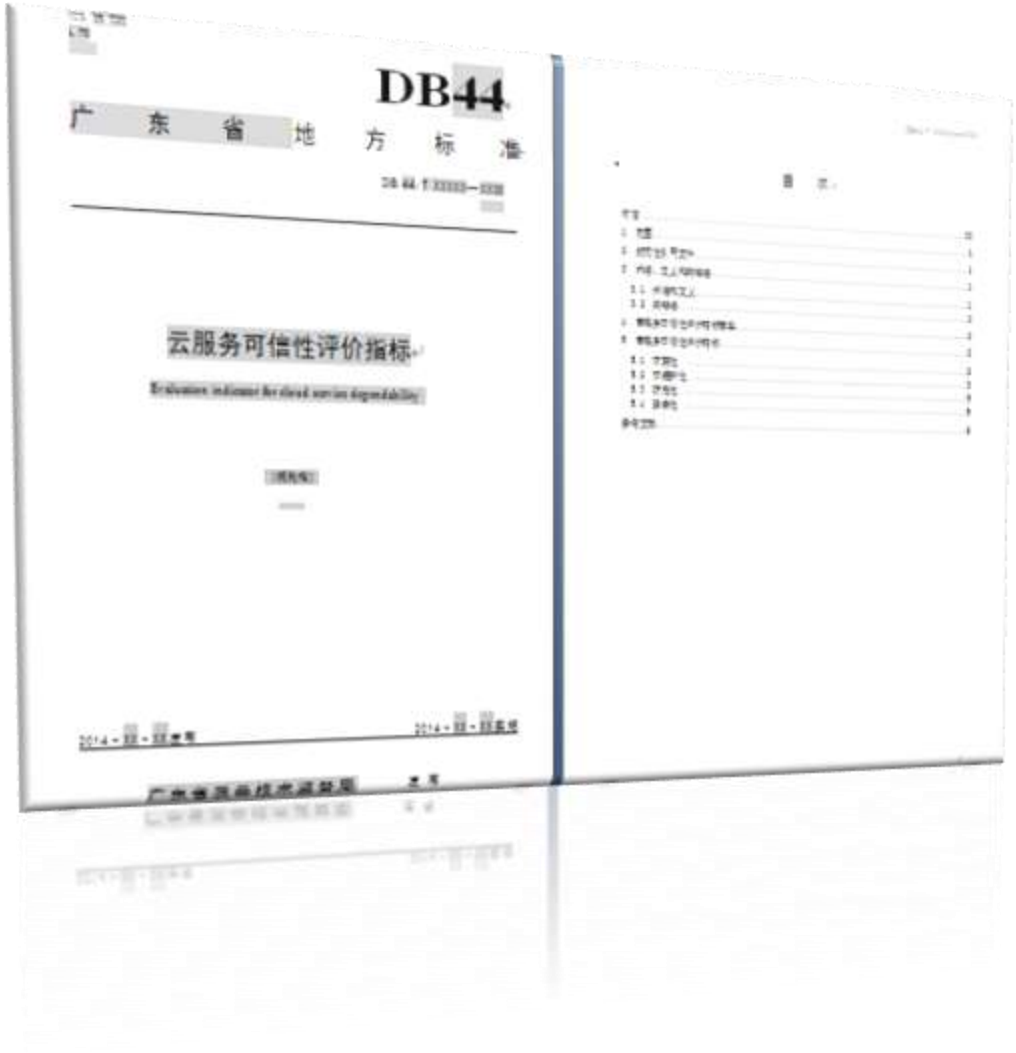
《云计算安全管理通用要求》新增域—示例

15、虚拟化安全		
15.1 虚拟化安全管理 目标：确保虚拟化环境的安全。		
15.1.1	操作系统加固与基础控制	控制措施 应对操作系统进行加固，确保只提供业务所需的端口、协议和服务；并采用合适的技术控制，如防病毒软件、文件完整性监视、日志、入侵检测，以此作为安全基线模板。
15.1.2	变更检测（虚拟机镜像监测）	控制措施 应确保所有虚拟机映像完整性，对虚拟机映像进行的变更要有日志记录并进行警报；变更要通过电子方式通知客户。
15.1.3	迁移中的安全保护	控制措施 应使用安全和加密的通信通道把物理服务器，应用或数据迁移到虚拟服务器；适用时，应使用和开发网络相隔离的网络进行迁移。
15.1.4	**VMM安全** **Hypervisor的加固**	控制措施 应对所有**hypervisor**管理函数及驻有虚拟化系统的系统管理控制台的访问进行访问限制
15.1.5	多租户隔离	控制措施 应建立策略和过程，对多租户进行适当隔离。

云服务解决之道



云服务解决之道：可信评价



云服务可信性

cloud service dependability

在规定条件下，系统持续交付有效 ，可信赖云服务的能力 。包括可靠性、可维护性、防危性和安全性等4种基本属性。

云服务解决之道：可信评价

云服务可信性评价指标构成

在云计算安全方面：

★你到底做的怎么样？
★怎么向客户展示你做的怎么样？
★如何评价你的供应商做的怎么样？

云服务安全解决之道：检查审核

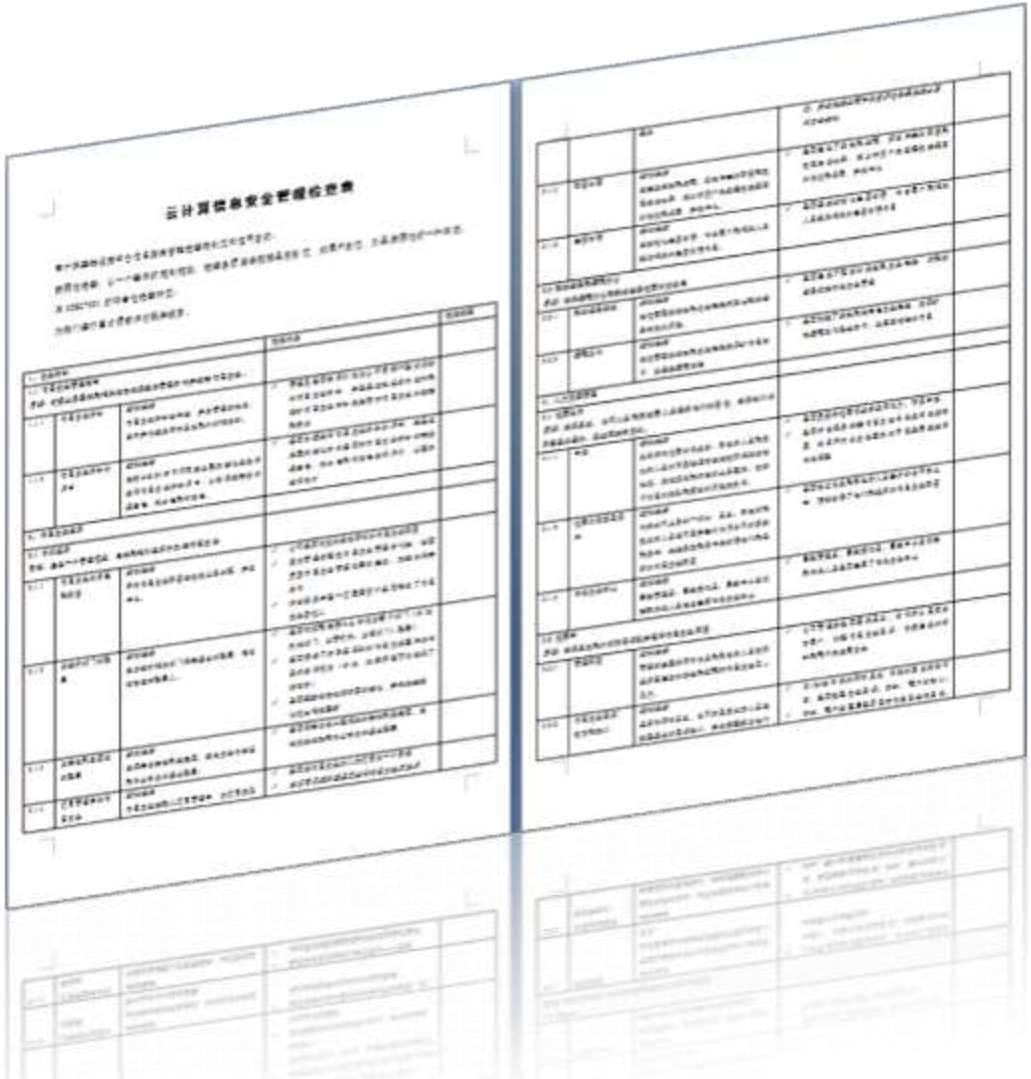
开发认证框架由3个层面构建，每一个层面都将对云服务供应商的运营的可信度和透明度提供一个增值层，以及对云用户提供更高层次的安全保障。

●初级层是CSA STAR自我评估：云服务提供商向CSA STAR Registry登记处提交一份能说明他们能力（且符合CSA最佳业务实践）的报告。

●第二个等级——CSA STAR CERTIFICATION（CSA STAR认证），是由第三方独立评估的：认证将平衡GB/T22080管理系统标准与CSA云服务控制矩阵(CCM)的要求。

●第三等级：STAR认证能增强日后的连续监控认证（第三等级现还在研制中）

云服务安全解决之道：检查审核



云服务安全性审核

根据成熟的标准和规范，对云服务的安全性从技术和管理的角度开展全方位的评价，在帮助用户检查其安全管理的有效性的同时提出改进的建议。


云安全联盟中国落地发布会
暨政产学研战略合作协议签约仪式
China Representative Office Announcement & Multi-sector Strategic Partnership MOU

云服务安全解决之道：检查审核

CEPREI
GB/T 22080

+

cloud security alliance®
CSA
CCM

STAR认证是信息安全管理体系认证（GB/T 22080）的增强版本，旨在应对与云安全相关的特定问题。

该项目采用中立性认证技术对云服务供应商安全性开展缜密的第三方独立评估，并充分运用GB/T 22080管理体系标准以及CSA云控制矩阵（CCM），帮助企业满足对安全性有特定要求的客户需求。

刘小茵

赛宝认证中心 总监

ISMS/ITSMS高级审核员

CISA、ITIL

TEL:18688899548

Email: LXY@CEPREI.ORG