

《云计算信息安全管理——CSAC-ST》

图书基本信息

书名：《云计算信息安全管理——CSAC-STAR实施指南》

13位ISBN编号：9787121272679

出版时间：2015-10

作者：赵国祥,刘小茵,李尧

页数：332

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

内容概要

本书包括理论篇和实践篇两部分，详细介绍了云计算环境下的信息安全管理指南。理论篇从梳理Gartner、云计算安全联盟（CSA）、欧洲网络与信息安全局（ENISA）等知名研究组织提出的云计算环境下所面临的安全问题着手，分析总结了现阶段常见的云计算环境下的信息安全风险；同时，对现有的国内外成熟的云计算信息安全管理标准及常见的云计算信息安全管理方法和模型进行了分析，有针对性地提出了C-STAR分级模型及评估方法。实践篇从应用和接口安全，审计保证与合规性，业务连续性管理和操作弹性，变更控制和配置管理，数据安全和信息生命周期管理，数据中心安全，加密和密钥管理，治理和风险管理，人力资源，身份识别和访问管理，基础设施和虚拟化安全，互操作性和可移植性，移动安全，安全事件管理、电子证据及云端调查取证，供应链管理、透明性及责任，威胁和脆弱性管理等16个方面详细解读了C-STAR体系规范中各项条款的内容和含义，同时给出了企业实施落地的实践参考，使C-STAR管理体系的建立者能深入理解各项条款的要求，并正确应用相关参考内容建设云计算环境的信息安全管理体系，有针对性地开展云计算安全管理。

书籍目录

理论篇

第1章 云计算发展历程

(2)

1.1 云计算的出现和发展

(2)

1.2 云计算与传统IT的联系

(3)

1.2.1 云计算与网格计算的关系

(3)

1.2.2 云计算与对等计算的关系

(5)

1.2.3 云计算与集群计算的关系

(5)

1.2.4 云计算与资源虚拟化的关系

(6)

1.2.5 云计算与Web服务技术的关系

(8)

1.2.6 云计算与传统IT的区别

(8)

1.3 云计算的特点

(10)

1.3.1 泛在网络访问

(11)

1.3.2 服务可度量

(11)

1.3.3 多租户

(11)

1.3.4 按需自助服务

(11)

1.3.5 快速弹性伸缩

(12)

1.3.6 资源池化

(13)

1.4 本章小结

(14)

第2章 云计算所面临的安全问题

(15)

2.1 案例分析

(16)

2.1.1 Google安全问题及事件分析

(16)

2.1.2 Amazon宕机事件及应对措施分析

(16)

2.1.3 Apple服务安全事件及应对措施分析

(17)

2.1.4 微软云服务安全事件及应对措施分析

(17)

2.2 云计算所面临的安全问题总结	(18)
2.2.1 云安全问题的研究分析	(18)
2.2.2 安全问题分类	(23)
2.3 本章小结	(31)
第3章 云计算信息安全管理标准介绍	(32)
3.1 云计算信息安全管理标准化工作概述	(32)
3.1.1 国外标准化概况	(32)
3.1.2 国内标准概况	(37)
3.2 云计算信息安全管理标准化主要成果分析	(42)
3.2.1 CSA云安全控制矩阵	(42)
3.2.2 国标云服务安全标准	(44)
3.2.3 美国联邦政府风险与授权管理项目FedRAMP	(47)
3.2.4 ENISA《云计算信息安全保障框架》	(51)
3.2.5 ISO/IEC 27018《信息技术—安全技术—公有云中作为个人信息（PII） 处理者的个人信息保护实用规则》	(54)
3.2.6 ISO/IEC 27001：2013《信息技术—安全技术—信息安全管理体系要求》	(56)
3.3 本章小结	(58)
第4章 云计算信息安全管理方法和模型	(60)
4.1 常见的信息安全管理方法	(60)
4.1.1 信息安全管理体系	(60)
4.1.2 信息安全等级保护	(65)
4.1.3 CERT-RMM模型	(68)
4.1.4 其他ISMS成熟度模型	(73)
4.1.5 专业领域的信息安全管理方法	(76)
4.2 云计算安全管理方法	(78)

4.2.1 云计算安全管理体系	(79)
4.2.2 云计算安全管理的实施	(81)
4.3 云计算信息安全评估模型	(84)
4.3.1 SSE-CMM模型	(84)
4.3.2 C-STAR模型	(87)
4.4 本章小结	(90)
实践篇	
第5章 应用和接口安全 (AIS)	(94)
5.1 应用和接口安全要求	(94)
5.1.1 应用和接口安全概述	(95)
5.1.2 控制条款解读	(96)
5.2 落地实施建议	(100)
第6章 审计保证与合规性 (AAC)	(102)
6.1 审计保证与合规性要求	(102)
6.1.1 审计保证与合规性概述	(103)
6.1.2 控制条款解读	(103)
6.2 落地实施建议	(113)
第7章 业务连续性管理和操作弹性 (BCR)	(116)
7.1 业务连续性管理和操作弹性要求	(116)
7.1.1 业务连续性管理和操作弹性概述	(117)
7.1.2 控制条款解读	(117)
7.2 落地实施建议	(126)
第8章 变更控制和配置管理 (CCC)	(133)
8.1 变更控制和配置管理要求	(133)
8.1.1 变更控制和配置管理概述	(134)

8.1.2 控制条款解读	(135)
8.2 落地实施建议	(138)
第9章 数据安全和信息生命周期管理 (DSI)	(150)
9.1 数据安全和信息生命周期管理要求	(150)
9.1.1 数据安全和信息生命周期管理概述	(151)
9.1.2 控制条款解读	(151)
9.2 落地实施建议	(157)
第10章 数据中心安全 (DCS)	(161)
10.1 数据中心安全要求	(161)
10.1.1 数据中心安全概述	(162)
10.1.2 控制条款详解	(162)
10.2 落地实施建议	(167)
第11章 加密和密钥管理 (EKM)	(170)
11.1 加密和密钥管理要求	(170)
11.1.1 加密和密钥管理概述	(171)
11.1.2 控制条款解读	(172)
11.2 落地实施建议	(176)
第12章 治理和风险管理 (GRM)	(178)
12.1 治理和风险管理要求	(178)
12.1.1 治理和风险管理概述	(179)
12.1.2 控制条款解读	(179)
12.2 落地实施建议	(189)
第13章 人力资源 (HRS)	(197)
13.1 人力资源安全要求	(197)
13.1.1 人力资源安全概述	

- (198)
- 13.1.2 控制条款解读
- (199)
- 13.2 落地实施建议
- (208)
- 第14章 身份识别和访问管理 (IAM)
- (210)
- 14.1 身份识别和访问管理要求
- (210)
- 14.1.1 身份识别和访问管理概述
- (211)
- 14.1.2 控制条款解读
- (212)
- 14.2 落地实施建议
- (221)
- 第15章 基础设施和虚拟化安全 (IVS)
- (225)
- 15.1 基础设施和虚拟化安全要求
- (225)
- 15.1.1 基础设施和虚拟化安全概述
- (226)
- 15.1.2 控制条款解读
- (227)
- 15.2 落地实施建议
- (241)
- 第16章 互操作性和可移植性 (IPY)
- (243)
- 16.1 互操作性和可移植性要求
- (243)
- 16.1.1 互操作性和可移植性概述
- (244)
- 16.1.2 控制条款解读
- (245)
- 16.2 落地实施建议
- (248)
- 第17章 移动安全 (MOS)
- (250)
- 17.1 移动安全要求
- (250)
- 17.1.1 移动安全概述
- (251)
- 17.1.2 控制条款解读
- (252)
- 17.2 落地实施建议
- (269)
- 第18章 安全事件管理、电子证据及云端调查取证 (SEF)
- (271)
- 18.1 安全事件管理、电子证据及云端调查取证要求
- (271)

18.1.1 安全事件管理、电子证据及云端调查取证概述	(272)
18.1.2 控制条款解读	(273)
18.2 落地实施建议	(278)
第19章 供应链管理、透明性及责任 (STA)	(283)
19.1 供应链管理、透明性及责任要求	(283)
19.1.1 供应链管理、透明性及责任概述	(284)
19.1.2 控制条款解读	(286)
19.2 落地实施建议	(292)
第20章 威胁和脆弱性管理 (TVM)	(295)
20.1 威胁和脆弱性管理要求	(295)
20.1.1 威胁和脆弱性管理概述	(296)
20.1.2 控制条款解读	(297)
20.2 落地实施建议	(300)
附录A CSA云安全控制矩阵ISO/IEC 27001 : 2013对照条款	(302)
参考文献	(317)

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com