云安全审计的现状和展望

CSA上海分会，联席主席
CISSP CISA CCSK CCSSP
shen@shanghai.chapters.cloudsecurityalliance.org

The global mandate to secure the cloud

Copyright © 2017 Cloud Security Alliance

法律要求在变

http://www.cac.gov.cn

互联网信息内容管理行政执法程序规定

网络产品和服务安全审查办法（试行）
网络关键设备和网络安全专用产品目录（第一批）

个人信息和重要数据出境安全评估办法（征求意见稿）

互联网新闻信息服务管理规定
互联网新闻信息服务许可管理实施细则

CSA cloud security alliance
Copyright © 2017 Cloud Security Alliance
www.cloudsecurityalliance.org

议题

1. 挑战
2. 现状
3. 展望

Copyright © 2017 Cloud Security Alliance

计算模式在变

- 系统和数据在哪儿？
- 设备谁拥有, 谁管理？
- 谁能访问？
- ....

Copyright © 2017 Cloud Security Alliance

不同

位置	IaaS	PaaS	SaaS
主机是那台	一台特定的主机（往往是VM），大概地理位置	N/A	N/A
在哪台网络设备上	确定，但对用户不可见	N/A	N/A
在哪台防火墙之后	虚拟防火墙	N/A	N/A
数据所在目录/文件	清晰可见	一个链接能见、格式能见、物理位置不详	能访问程序中数据，实际格式、位置不详

Copyright © 2017 Cloud Security Alliance

议题

1. 挑战
2. 现状
3. 展望

Copyright © 2017 Cloud Security Alliance

现状

云审计现状从哪儿看起？

Copyright © 2017 Cloud Security Alliance

AWS

CSA
云安全联盟控制体系

ISO 9001
全球质量标准

ISO 27001
安全管理标准

ISO 27017
专门针对云的控制体系

ISO 27018
个人数据保护

PCI DSS 第 1 级
支付卡标准

SOC 1
审计控制报告

SOC 2
合规性控制报告

SOC 3
一般控制报告

Copyright © 2017 Cloud Security Alliance

AWS

Copyright © 2017 Cloud Security Alliance

AWS

FISC [日本]
金融业信息系统

IRAP [澳大利亚]
澳大利亚安全标准

MLPS 第 3 级 [中国]
多层保护

MTCS 3 层 [新加坡]
多层云安全标准

My Number Act [日本]
个人信息保护

DNB [荷兰]
荷兰金融条例

UK Cyber Essentials Plus
网络威胁防护

G-Cloud [英国]
英国政府标准

IT-Grundschutz [德国]
基准保护方法

AWS

Copyright © 2017 Cloud Security Alliance

Azure

Certifications

CDSA	FERPA	IT Grundschutz Compliance Workbook
CJIS	FIPS 140-2	ITAR
CSA CCM	FISC	MARS-E
CS Mark	HIPAA/HITECH	MPAA
DISA	IRAP (CCSL)	MTCS
EU Model Clauses	IRS 1075	NZ CC Framework
FACT	ISO 22301	PCI-DSS
FDA	ISO/IEC 27001	Section 508 VPATs
FedRAMP	ISO/IEC 27017	SOC 1, 2, and 3
	ISO/IEC 27018	Spain ENS
		UK G-Cloud

Copyright © 2017 Cloud Security Alliance

阿里云

Copyright © 2017 Cloud Security Alliance

交集

- ISO 27001 多个机构的审计师，使用ISO27001审核
- CSA 多个机构的审计师，使用CSA标准
- SOC 美国注册会计师，使用CSA标准
- PCI DSS 支付. 行业标准
- MPLS 中国. 地方标准
- MTCS T3 新加坡. 地方标准

Copyright © 2017 Cloud Security Alliance

现状分析

- 谁审谁
- 请谁审
- 标准
- 频率
- 谁出钱

Copyright © 2017 Cloud Security Alliance

云计算安全审计

	ISO 27001	CSA	SOC	备注
发起方	云服务商	云服务商	云服务商	大玩家
被审计方	云服务商	云服务商	云服务商	大玩家
审计成本承担	云服务商	云服务商	云服务商	大玩家
审计工作承担方	认证公司	认证公司	会计师事务所	审计人员缺乏*
采用标准	ISO 27001	CSA CMM	CSA CMM	
审计频率	每年	每年	6个月	Docker支持持续发布

Copyright © 2017 Cloud Security Alliance

问题

生态

云服务商是大玩家

工具

审计方法耗时耗力、频率过低

人

云飞速发展，审计人员缺乏

Copyright © 2017 Cloud Security Alliance

议题

1. 挑战
2. 现状
3. 展望

Copyright © 2017 Cloud Security Alliance

展望

Certified Public Accountant

CISA
Certified Information Systems Auditor

CCSP

CCSK
Certificate of Cloud Security Knowledge

openstack.

cloudstack

OvS

kibana
elasticsearch

KVM

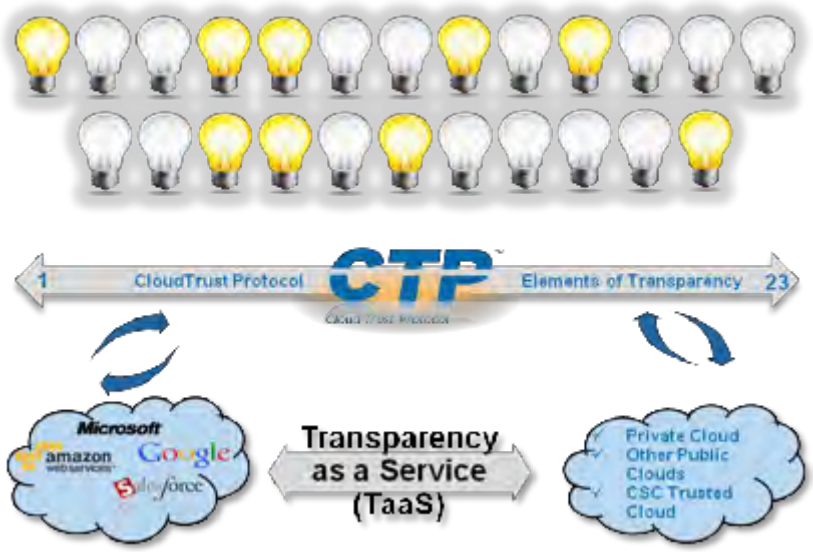
Xen

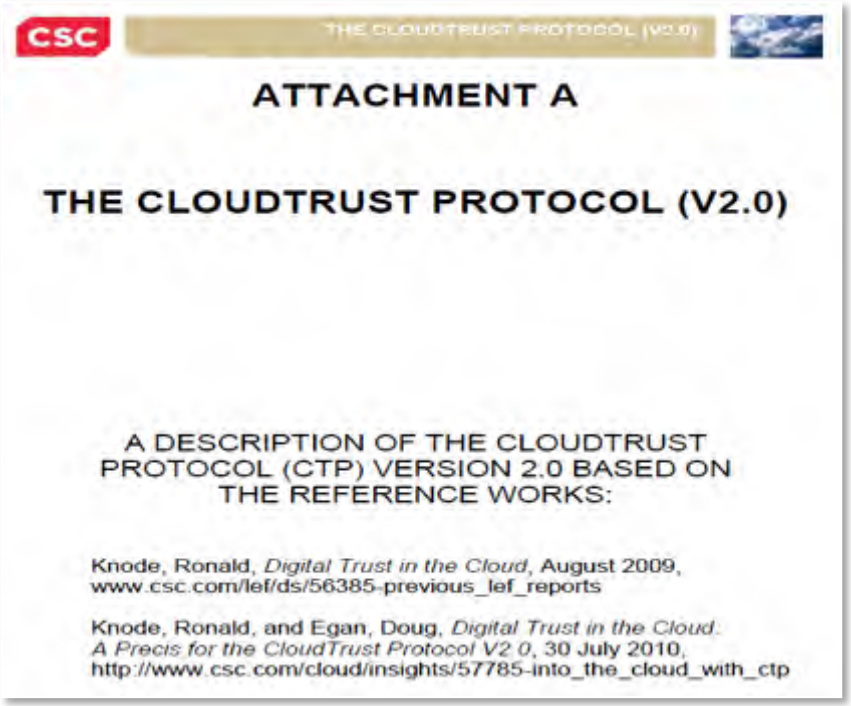
• • • • • •

Copyright © 2017 Cloud Security Alliance

展望

CTP V2.0




CSC

THE CLOUDTRUST PROTOCOL (V2.0)

ATTACHMENT A

THE CLOUDTRUST PROTOCOL (V2.0)

A DESCRIPTION OF THE CLOUDTRUST PROTOCOL (CTP) VERSION 2.0 BASED ON THE REFERENCE WORKS:

Knode, Ronald, *Digital Trust in the Cloud*, August 2009, www.csc.com/lef/ds/56385-previous_lef_reports

Knode, Ronald, and Egan, Doug, *Digital Trust in the Cloud. A Precis for the CloudTrust Protocol V2.0*, 30 July 2010, http://www.csc.com/cloud/insights/57785-into_the_cloud_with_ctp

Copyright © 2017 Cloud Security Alliance

展望

IIHS HLDI
Insurance Institute for Highway Safety
Highway Loss Data Institute

独立*
非盈利
科研
教育机构

* 保险公司和保险协会提供全部**资金支持**

Copyright © 2017 Cloud Security Alliance

JOIN US

Copyright © 2017 Cloud Security Alliance

CSA上海企业会员

Copyright © 2017 Cloud Security Alliance

作为个人会员加入

Copyright © 2017 Cloud Security Alliance