

# Compliance in the Cloud

Davi Ottenheimer



September 21, 2009 – September 23, 2009



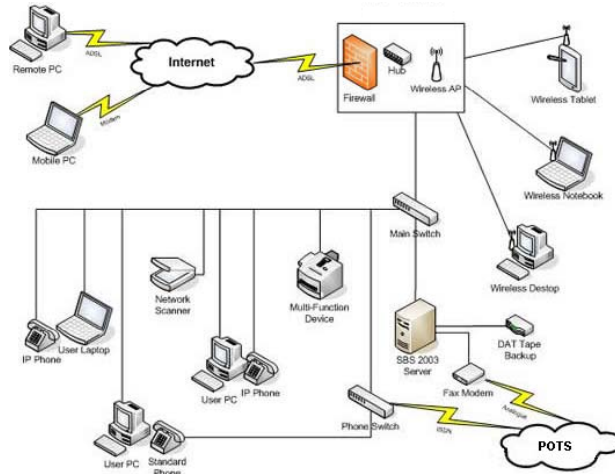
## Hello

- 15th Year in Information Security
- CISSP, CISM, QSA, PA-QSA, ITIL

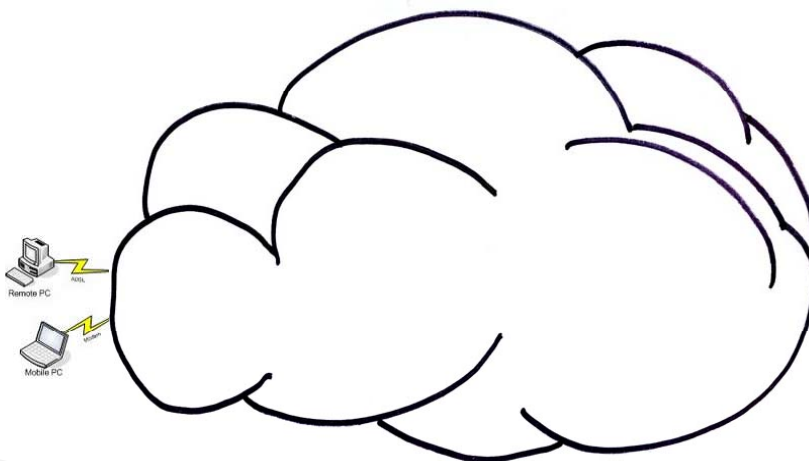
A smaller version of the CONVERGEMERGE logo, featuring the word in bold with a pink circular arrow and arrows pointing to various benefits.



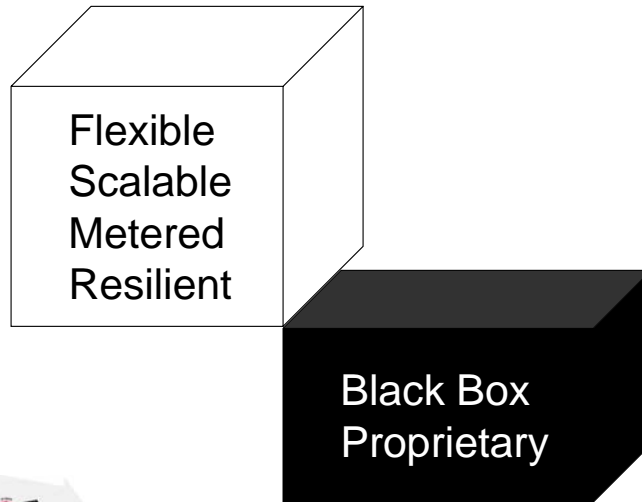
# Before the Cloud



# After the Cloud



## Cloud Attributes



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

## Who wants this risk?



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

# What if it was marketed like this?



NAIAS 2007 - The Audi Q7 V12 TDI

AudiWorld

Vroom, vroom. Powerful. What can it do?

Get in, hold on (and don't try to get out)!



# Has this model worked before?

How does liquid get into that box...what are we buying? Can we **rely** on it? Is it **safe**? I do not **trust** it.



The question is, are you **thirsty** and can you **afford** it?

Oh, *and* does the system **deliver**?



What about THIS delivery model?



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

The *old* Holy Grail of IT



CONVERGEMERGE

**25 Years to the Toaster**

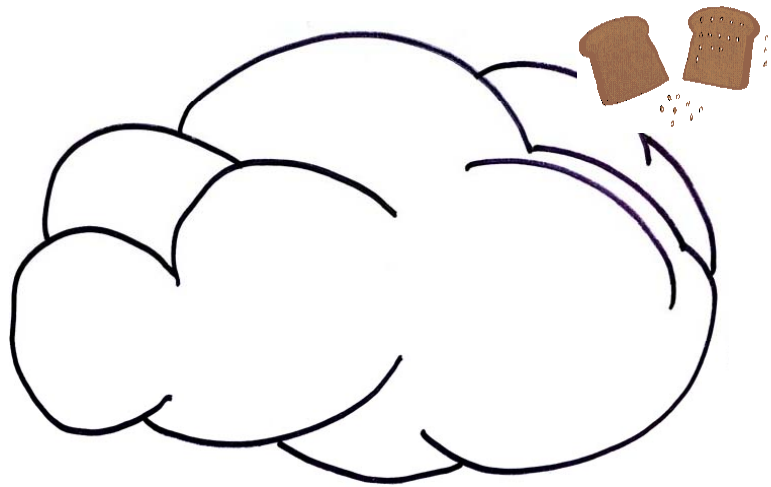
- 1905 Filament Wire
- 1909 Commercial Electric Toaster
- 1913 Automatic Bread Turner
- 1919 Pop-up Timer Mechanism
- 1928 Mechanical Sliced Bread
- 1929 Home-Use Pop-up Toaster
- 1930 Standardized Sliced Bread

**54 Years to *Safe* Toast**

- 1961 GFCI

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

# The *new* Holy Grail of IT



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

## Why worry?

CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

# Reality check: Ready for this?



## Warning: Needs actually may be Black and White

Pre-Cloud

Rule Name	Direction	Event Name	Protocol	Sic Port
Allow All In	Inbound	allow all in	*	*
Allow Arp In	Inbound	allow arp in	ARP	*
Allow HTTP In	Inbound	allow http in	TCP	80
Allow HTTPS In	Inbound	allow https-tcp in	TCP	443
Allow https in 444	Inbound	allow tcp in	TCP	444
Allow Icmp In	Inbound	allow icmp in	ICMP	*
Allow Icmp In	Inbound	allow icmp in	IGMP	*
Allow Iike In	Inbound	allow udp in	UDP	500
Allow Ip In	Inbound	allow ip in	IP	*
Allow Ipsec-Nak In	Inbound	allow udp in	UDP	10000
Allow Ping In	Inbound	allow ping in	ICMP	*
Allow POP3 In	Inbound	allow pop3 in	TCP	110
Allow SMTP In	Inbound	allow smtp in	TCP	25
Allow Tcp In	Inbound	allow tcp in	TCP	*
Allow Udp In	Inbound	allow udp in	UDP	*
ADL Instant Messenger Allow IN	Inbound	allow aim in	TCP	5190

Post-Cloud

Rule Name	Direction	Event Name	Protocol	Sic Port
Allow All In	Inbound	allow all in	*	*
Allow Arp In	Inbound	allow arp in	ARP	*
Allow HTTP In	Inbound	allow http in	TCP	80
[Redacted]				
Allow Icmp In	Inbound	allow icmp in	ICMP	*
[Redacted]				
Allow Ip In	Inbound	allow ip in	IP	*
Allow Ipsec-Nak In	Inbound	allow udp in	UDP	10000
Allow Ping In	Inbound	allow ping in	ICMP	*
[Redacted]				

Your rules

Unknown rules



Still thinking this?



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

Can a cloud have transparency?

1. Inventory of customer data
2. Proof that it is protected
3. Evidence of access to it



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter



## Can a cloud be trusted?



1. Tell us where our customer data is
2. Prove to us you are protecting it
3. Show us who is accessing it

CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

## Maybe



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

## Maybe Not

T-FAL Model 8781 Hi-Speed Toaster “presented a substantial risk of injury [from fire] to the public as defined by the Consumer Product Safety Act”



CONVERGENCE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

Where are the answers?

CONVERGENCE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

# Security versus Compliance



**ANSI**  
American National Standards Institute  
11 West 42nd Street, New York, NY 10018

**BHMA**  
CERTIFIED

**UL** **UL**  
UL Listed for both Canada and the US.

**CONVERGENCE**

**ISACA**  
Serving IT Governance Professionals  
San Francisco Chapter

# Is a Cloud Secure?



**CONVERGENCE**

**ISACA**  
Serving IT Governance Professionals  
San Francisco Chapter

## Who gets to decide?

CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

## Cloud Security Checklist

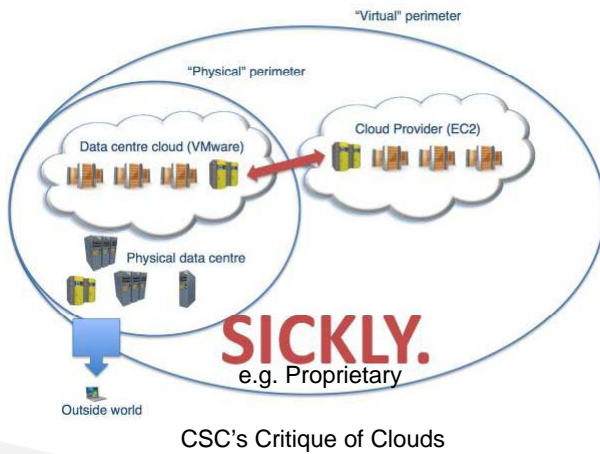
- Certifications and Accreditations
- Physical Security
- Backups
- Network Security
- Storage Security
- Application and DB Security



CONVERGEMERGE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

# Notice sudden health problems?



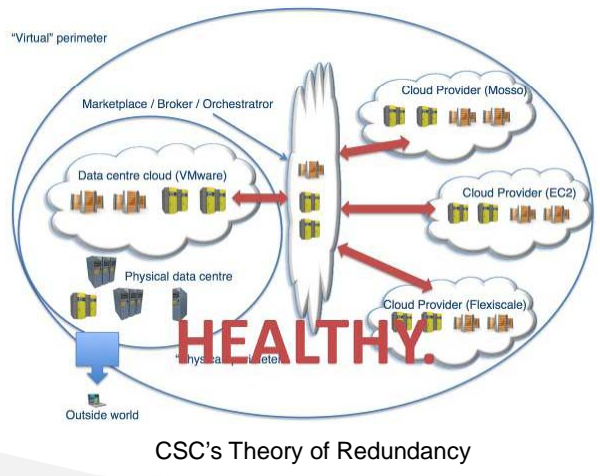
The question was, are you **thirsty** and can you **afford** it? Oh, *and* does the system **deliver**?



CSC's Critique of Clouds



# Maybe you saw this one coming



= Ivory Tower  
(RAID was Redundant Array of *Inexpensive* Disks for a reason: storage was *expensive*)  
How much for a Cloud Broker?

CSC's Theory of Redundancy



## Vroom vroom



CONVERGENCE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

## Can a cloud be compliant?

Compliance = meet or exceed the requirements of a clearly defined specification, policy, standard or law.

- Organization and Management
- Physical Security
- Network Security
- Storage Security
- Application and DB Security
- Response and Recovery

CONVERGENCE

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter

## SAS 70 Example

### You want to know:

- Where is the data?
- Who can access data?
- Who has accessed data?

### Cloud SAS 70 Report tells you:

- Control description (e.g. Physical security)
- Control objectives (Open to interpretation)

Has an organization described its own controls accurately?



29



## Something completely different

### PCI DSS 1.2 Requirements

- 2.4 - Shared hosting providers must protect each entity's hosted environment and data.
- 10.5.3 - Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
- 12.8 - Maintain a written agreement that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess.



# HIPAA Clouds

164.310(d)(2)(iii) Accountability - Implement procedures to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

164.312(a)(1) Access Control - Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec 164.308(a)(4)

164.312(b) Audit Controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.



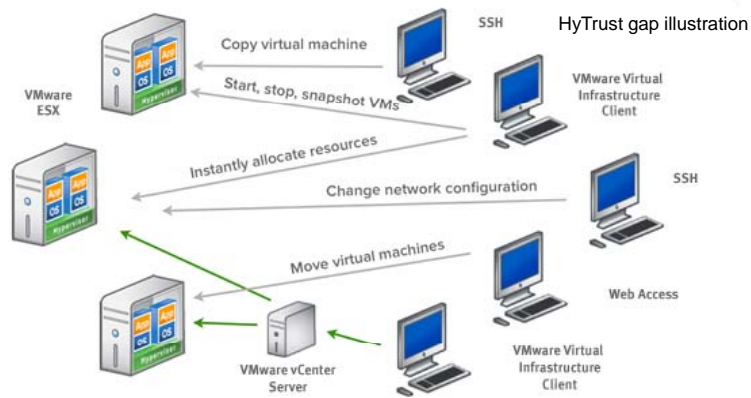
## What if the Cloud is internal only?

How did my data get into that *meta operating system*...? Can we **rely** on it? Is it **safe**? I do not **trust** it.





## The new model creates new risks...



...that we already know about.



## Conclusion: Accountability is Key

- Transfer liability to a *trusted* Service Provider (Cloud)  
or
- Remove risk
  - Sanitize data (mask, wipe, hash, group)
  - Encrypt data
  - Keep in-house and real-time control
  - Force separation (even geographic)



# Compliance in the Cloud: Q & A



Davi Ottenheimer  
davi@flyingpenguin.com



35

