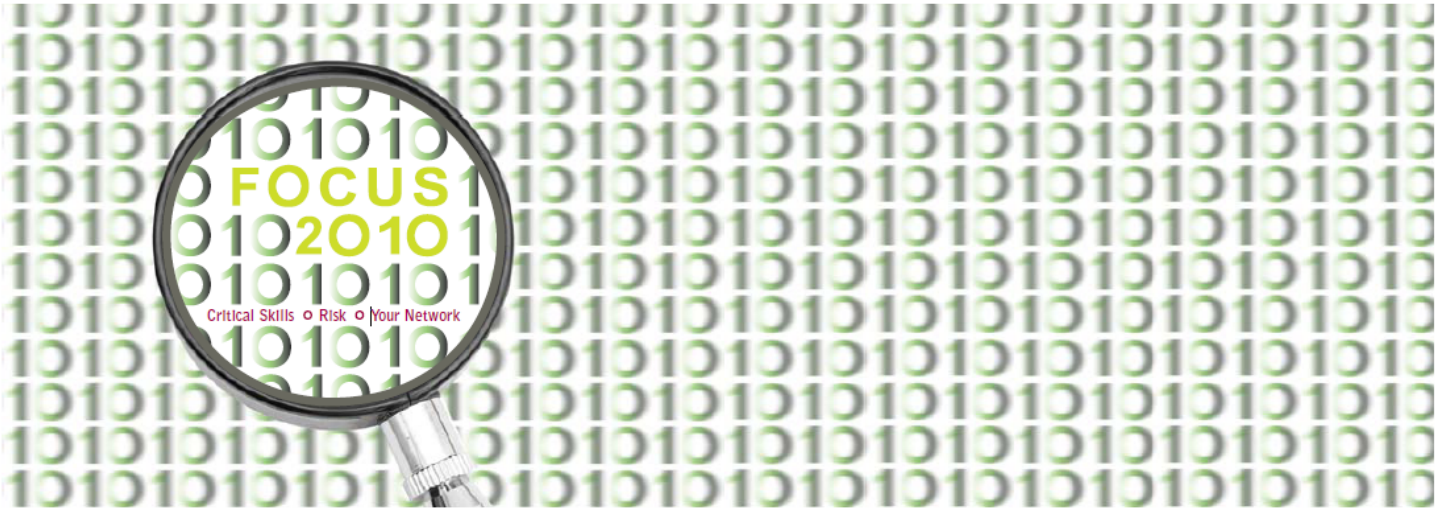
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



T13: Compliance in the Cloud

Davi Ottenheimer, flyingpenguin, LLC

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Compliance in the Cloud

Managing Risks and Addressing Concerns

Davi Ottenheimer

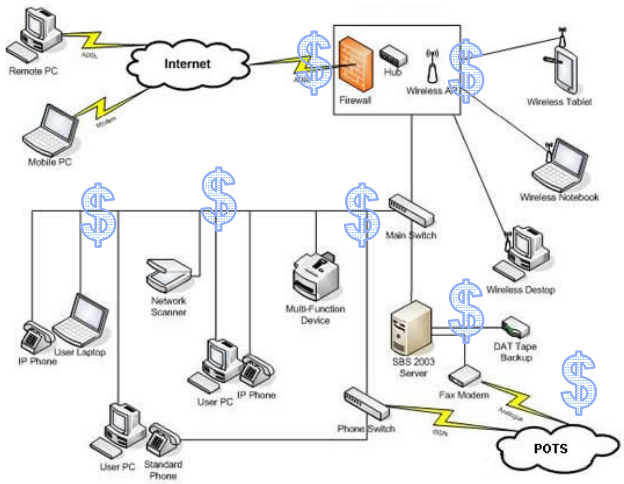
Introduction

- 16th Year in Information Security
- ISACA Member Since 1997
- Former CRM Manager, Arthur Andersen
- Former ISACA Silicon Valley Board
- CISM, CISSP, QSA, PA-QSA, ITIL
- President, flyingpenguin

Agenda

- Overview
- Managing Risk
- Addressing Concerns
- Conclusions

Life Before Cloud



The Cloud Model

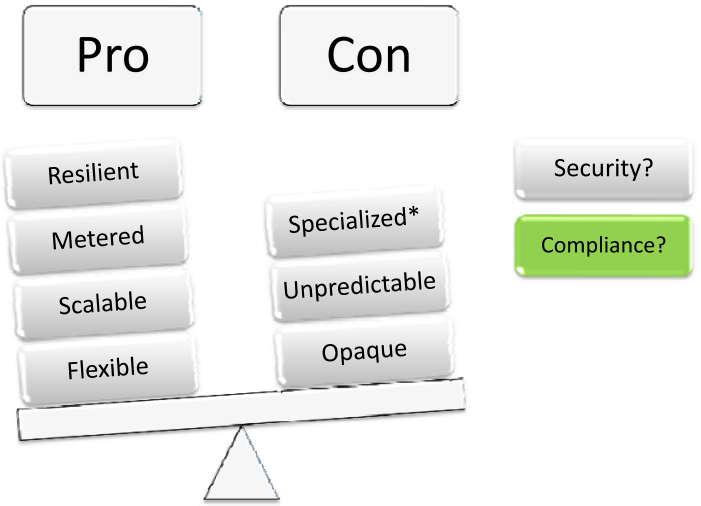
Cloud Definition

Cloud Computing according to vendors

- Lightweight entry/exit service acquisition model
- Consumption based pricing
- Accessible using standard internet protocols
- Elastic
- Improved economics due to shared infrastructure
- Massively more efficient to manage

> **Cloud computing comes into focus only when you think about… a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time… extends IT's existing capabilities.**
>
> InfoWorld

Cloud Attributes



Why Trust This Stuff?

Cloud Provider Trust Marketing

- Commodity?

"…who is likely to be better at security? You or the cloud provider whose business depends on it?"

- Size?

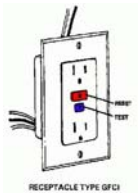
"Too big to fail"

Commodity != Safety

"In the long run, everything is a toaster." – Bruce Greenwald

Still has risks...

54 Years to safe toast (1964)



1905 Filament Wire

1909 Commercial Electric Toaster

1913 Automatic Bread Turner

1919 Pop-up Timer Mechanism

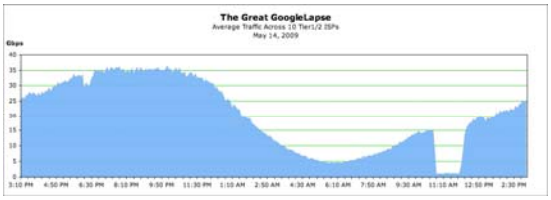
1928 Mechanical Sliced Bread

1929 Home-use Pop-up Toaster

1930 Standardized Sliced Bread

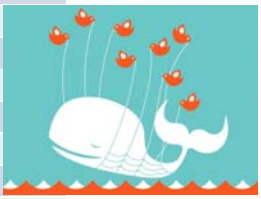
"The Myth of Commoditization" – Michael Schrage

Size != Safety



http://asert.arbornetworks.com/2009/05/the-great-googlelapse/

Provider	Date	Impact
Google Gmail, Apps	August 15, 2008	24 Hours
Google Gmail	October 16, 2008	30 Hours
Microsoft Sidekick	March 13, 2009	6 Days
Microsoft Azure	March 13, 2009	22 Hours
Terremark	March 17, 2010	7 Hours
Sage	June 1, 2010	22 Hours
Twitter	June 11, 2010	3 Days+
Intuit	June 15, 2010	300K users



Size != Safety

- Data spans jurisdictions of privacy and property
- Audit, e-discovery, subpoena variations by region
- Data "environment" and segmentation gaps
  - Eavesdropping
  - Hypervisor "hopping"
- Evidence of compliance (like painting the GGB)
- Limitations on liability by management

How to assess a cloud as "safe"?

Zen and the Art of…IT Quality

Classical Approach

- Focus on Details
- Emphasis on Analysis
- Problem Solving Skills

Romantic Approach

- Focus Elsewhere
- Emphasis on "Moment"
- Service Center Relationship

Classical Approach

1. Where is the Data?
   - Age
   - Location
2. Control Test Documentation
3. Audit Trails and Archives
4. Reports

Romantic Approach

Risk = (Asset x Vulnerability x Threat) / ***Countermeasures***

Either Way, Verify

ISO 27002 Best Practice	NIST	PCI DSS	SOX	HIPAA
4. Risk Assessment and Treatment	✓	✓	✓	✓
5. Security Policy	✓	✓	✓	✓
6. Organization of Information Security	✓			✓
7. Asset Management	✓		✓	✓
8. Human Resources Management	✓			✓
9. Physical and Environmental Security	✓	✓	✓	✓
10. Communications and Operations Management	✓	✓	✓	✓
11. Access Control	✓	✓	✓	✓
12. Information Systems Acquisition, Development and Maintenance	✓	✓	✓	✓
13. Information Security Incident Management	✓	✓	✓	✓
14. Business Continuity Management	✓		✓	✓
15. Compliance	✓		✓	✓

Agenda

- Overview
- **Managing Risk (R=…)**
- Addressing Concerns
- Conclusions

Cloud Vulnerability

$$R = (V \times T \times A) / C$$

Vulnerability Tests – Firewall

Pre-Cloud

Rule Name	Direction	Event Name	Protocol	Src 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 Igmp In	Inbound	allow igmp in	IGMP	*
Allow Ike In	Inbound	allow udp in	UDP	500
Allow Ip In	Inbound	allow ip in	IP	*
Allow Ipsec Nat-t 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	*
AOL Instant Messenger Allow IN	Inbound	allow aim in	TCP	5190

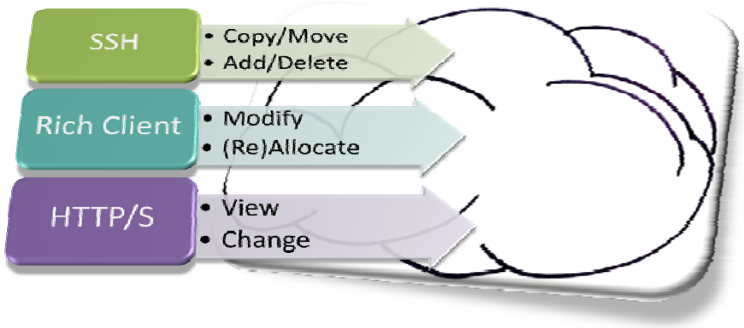
Post-Cloud

Rule Name	Direction	Event Name	Protocol	Src 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 Nat-t In	Inbound	allow udp in	UDP	10000
Allow Ping In	Inbound	allow ping in	ICMP	*
[redacted]				

Your rules

Unknown rules

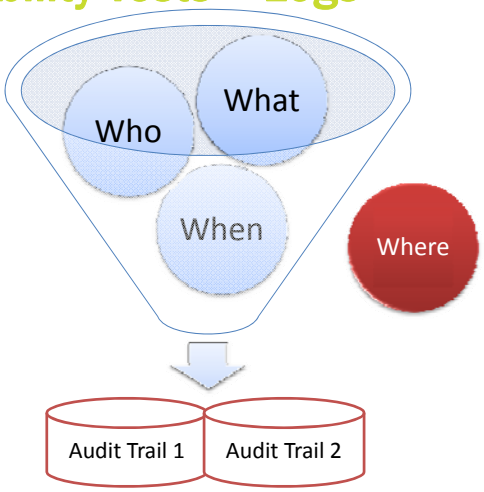
Vulnerability Tests – Remote Access



…same as it ever was
but different

Vulnerability Tests – Logs

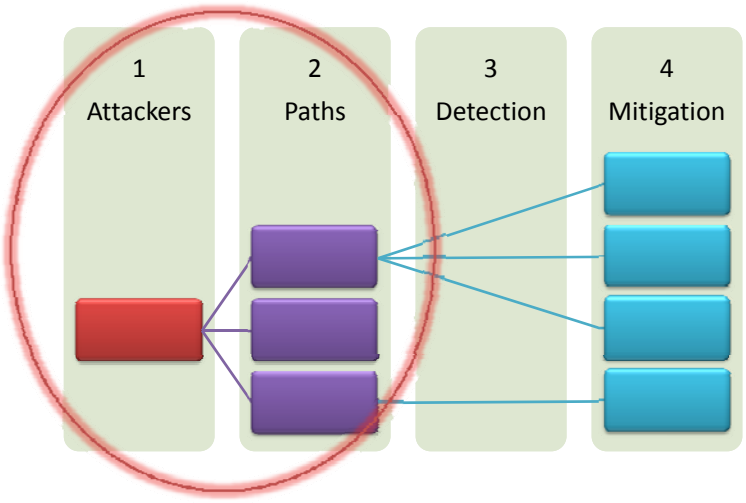
- Retention
- Access
- Detail
- Integrity
- Confidentiality



Threat

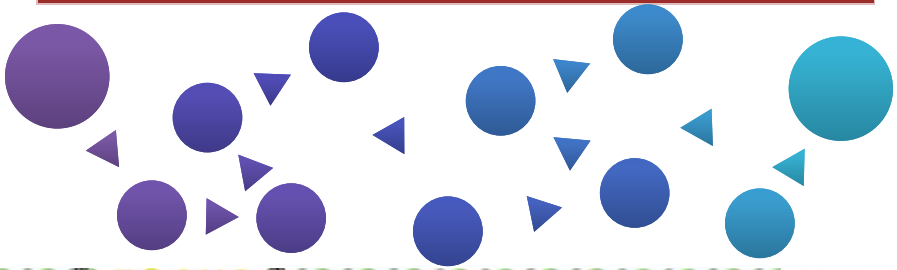
$$R = (V \times T \times A) / C$$

Threat Modeling



Attacker Profiles and Paths

Level	Commitment			Resources		
	Intensity	Stealth	Time	Power	Ability	Opportunity
1	H	H	Long	Organized	H	H
2	M	M	Varied	Grouped	M	M
3	L	L	Short	Isolated	L	L



ENISA (Euro Network and InfoSec Agency) Risk Map

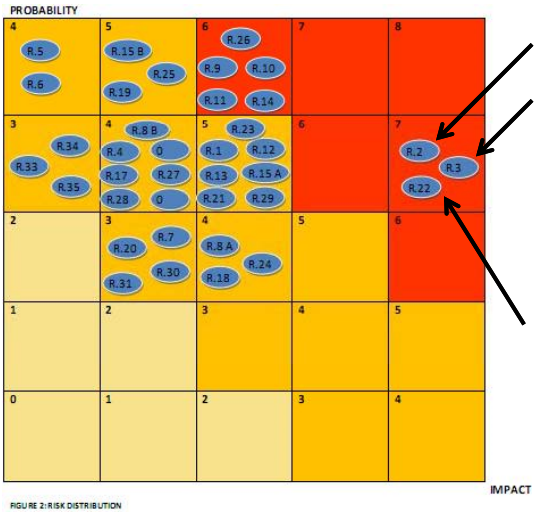


FIGURE 2: RISK DISTRIBUTION

- **R.2 Loss of Governance**
- **R.3 Lock-in**
- R.9 Isolation Failure
- R.10 Compliance Risks
- R.11 Management Interface Compromise
- R.14 Data Protection
- **R.22 Insecure or Incomplete Data Deletion**
- R.26 Malicious Insider

Agenda

- Overview
- Managing Risk
- Addressing Concerns
- Conclusions

Three Audit Pillars (in the cloud)

Pre-Cloud	Post-Cloud
1. Where is the data?	1. Where is the data?
2. Is it protected?	2. Is it protected?
3. Can you prove it?	3. Can you prove it?

Will it Deliver This?

Or Will it Deliver This?

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

Security and Compliance

ANSI American National Standards Institute 11 West 42nd Street, New York, NY 10036

BHMA CERTIFIED

c UL us

UL Listed for both Canada and the US.

Security Checklist for a Cloud

- Management
- Network Security
- Storage Security
- Application/DB Security
- Backups
- Physical Security

- Certifications and Accreditations?

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

SAS 70 (ISAE3402/SSAE16) Example

You want to know

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

SAS 70 provides

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

Has an organization described its own controls accurately?

- International Standard on Assurance Engagements No. 3402 (ISAE 3402), Assurance Reports on Controls at a Service Organization
- Statement on Standards for Attestation Engagements No. 16 (SSAE 16), Reporting on Controls at a Service Organization

HIPAA Example

Control	Description
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	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	Implement hardware, software, and/or procedural mechanisms that **record and examine activity** in information systems that contain or use ePHI.

PCI DSS 1.2 Example

Requirement	Description
2.4	Shared hosting providers must **protect each entity's hosted environment and data**.
8.3	Incorporate **two-factor authentication for remote access** (network-level access originating from outside the network) to the network by employees, administrators, and third parties.
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.

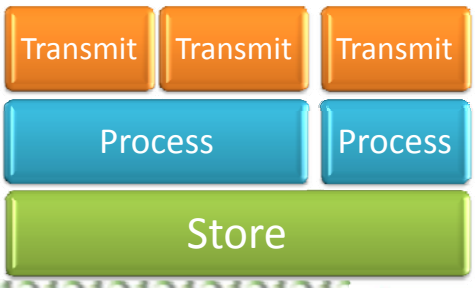
Threat Map versus Compliance

ENSIA Top Threats	ISO 27002
R2 Loss of Governance	A06 Organization of Information Security A15 Compliance
R3 Lock-in	A07 Asset Management
R9 Isolation Failure	A11 Access Control
R10 Compliance Risks	A15 Compliance
R11 Management Interface Compromise	A10 Communications and Operations Management
R14 Data Protection	A12 Information Systems Acquisition, Development and Maintenance
R22 Insecure or Incomplete Data Deletion	A10.07 Media Handling
R26 Malicious Insider	A08 Human Resources Security

ENISA R2 Loss of Governance

Cloud Provider May…

- Prohibit Independent Security Assessments
- Not Provide Full or Even Detailed Logs
- Restrict Access to Incident Information
- Have no Forensic Capabilities
- Fail to Disclose Location(s) of Data
- Outsource, Sub, Off-shore…
- Hide Behind SLA Trickery



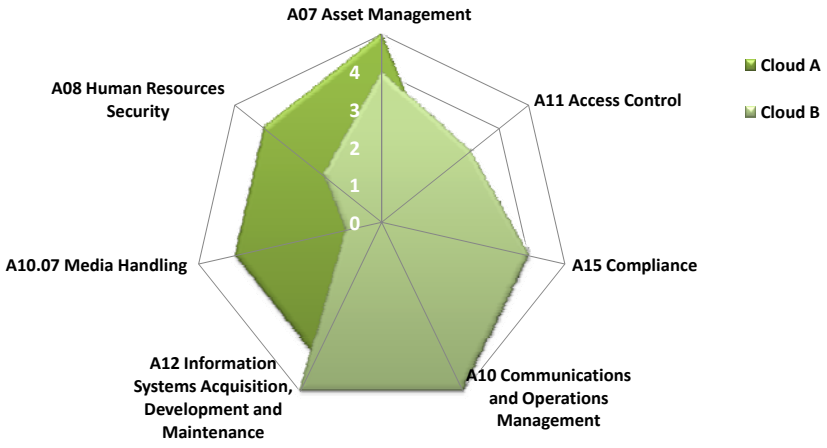
ENISA R3 Lock in → ISO A07 Asset Management

7.1.1 Inventory of Assets
7.1.2 Ownership of Assets
7.1.3 Acceptable Use of Assets
7.2.1 Classification Guidelines
7.2.2 Information Labeling and Handling

ENISA R9 Isolation Failure → ISO A11 Access Control

1. Control Access to Information
2. Manage User Access Rights
3. Access Practices
4. Access to Network Services
5. Access to OS
6. Access to Applications and Information
7. Protect Mobile and Teleworking Services

Cloud Provider Compliance Rating

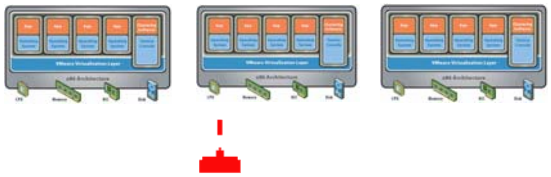


Agenda

- Overview
- Managing Risk
- Addressing Concerns
- **Conclusions**

Cloud Compliance Conclusions

- Extension of "Insiders"
  - Size of provider
  - Sub-contracts
- Obfuscated location (data transit and storage)
- Management Interface Importance
  - Access
  - Administration
  - Logs
  - Forensics
- Hypervisors



Cloud Compliance Conclusions

Liability and Transfer

- Terms of Service - Contract
- Insurance

Countermeasures

- Data Sanitization (mask, wipe, hash, group)
- Data Encryption
- Segmented Architecture
  - Logical separation (even geographic)
  - Physical presence of data

Cloud Compliance Conclusions

- Cloud computing can provide improved security if…
- Cloud computing depends on management to deliver security
- Management depends on compliance for baselines
- Compliance requires audit = transparency

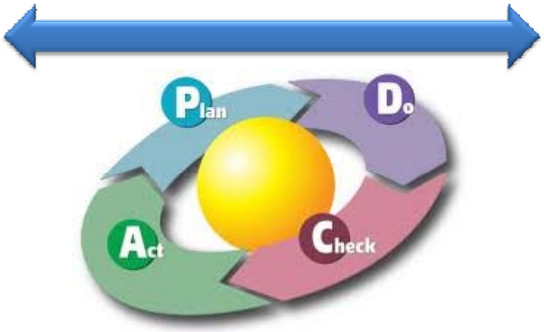
Compliance in the Cloud

Classical Approach

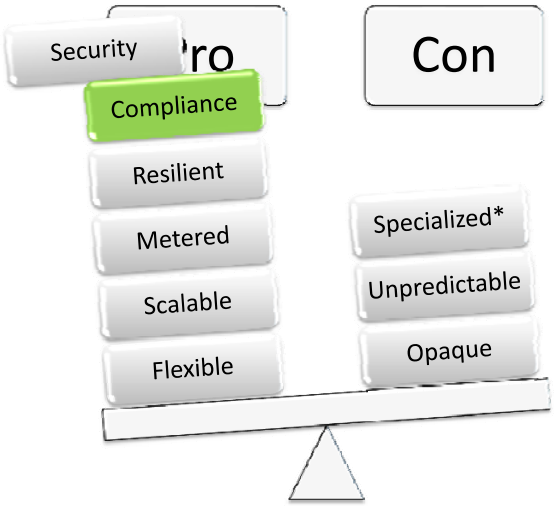
- Focus on Details
- Emphasis on Analysis
- Problem Solving Skills

Romantic Approach

- Focus Elsewhere
- Emphasis on "Moment"
- Service Center Relationship



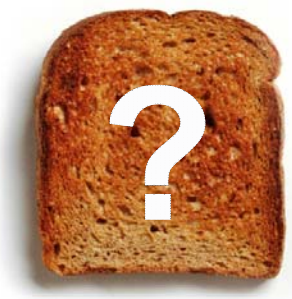
Compliance in the Cloud



FOCUS 2010

ISACA San Francisco Chapter

Compliance in the Cloud: Q and A



FOCUS 2010

Critical Skills ○ Risk ○ Your Network