Let’s talk about cloud audit.

an independent member of
BAKER TILLY
INTERNATIONAL

BAKER TILLY

Candor. Insight. Results.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP,
an independently owned and managed member of Baker Tilly International.

HELLO.
My name is:

Chris Tait
Tom Wojcinski

About Baker Tilly

BAKER TILLY

Candor. Insight. Results.

Firm facts

- Established in **1931**
- **Offices located in 11 cities** throughout Illinois, Michigan, Minnesota, New York, Washington DC and Wisconsin
- Over **1300 total staff**
- Baker Tilly is ranked as the **16th largest accounting and advisory firm in the United States** according to *Accounting Today's* 2011 list of "Top 100 firms."
- Largest independent member of Baker Tilly International in the United States

Just a few of our 11 offices across the US.

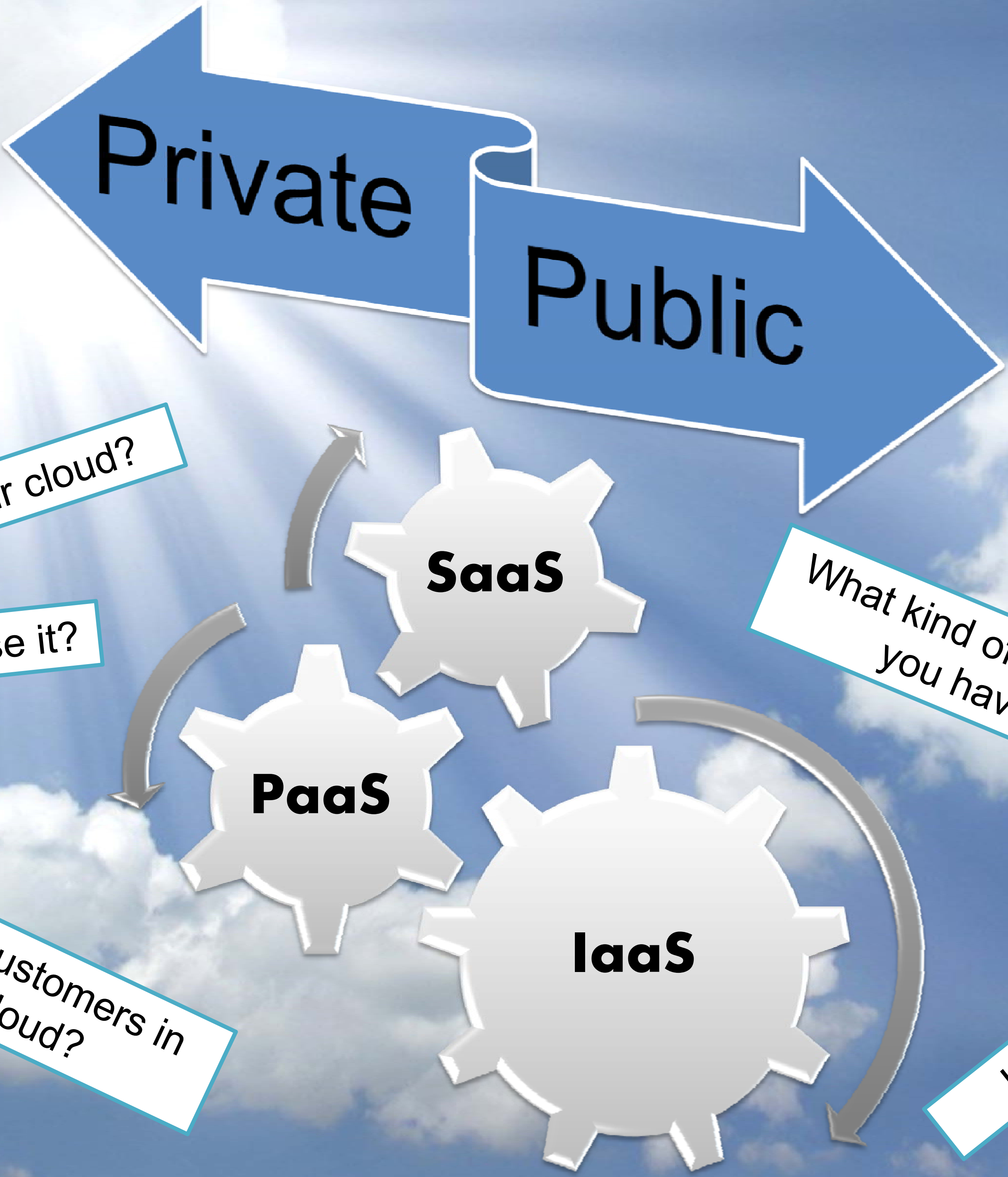
Agenda

BAKER TILLY

Candor. Insight. Results.

- Cloud overview
- Cloud risks and challenges
- Emerging cloud control frameworks
- Assurance reporting
- Key take aways

Cloud Overview



Private

Public

SaaS

PaaS

IaaS

Where's your cloud?

How do I use it?

Are my customers in the cloud?

What kind of cloud do you have?

Is it safe?

How do you define the Cloud?

BAKER TILLY

Candor. Insight. Results.

> “I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. **But I know it when I see it**…”
>
> —Justice Potter Stewart, *concurring opinion in Jacobellis v. Ohio 378 U.S. 184 (1964)*

Oracle CEO Larry Ellison Bashes 'Cloud Computing' Hype

http://www.youtube.com/watch?v=UOEFXaWHppE&feature=player_detailpage

1:55

What is Cloud Computing

Baker Tilly

Candor. Insight. Results.

Simply defined, SaaS is an application delivery model in which the user accesses software over the Internet, from anywhere, at any time. (Often called “On-Demand”.)

Five Key Elements:

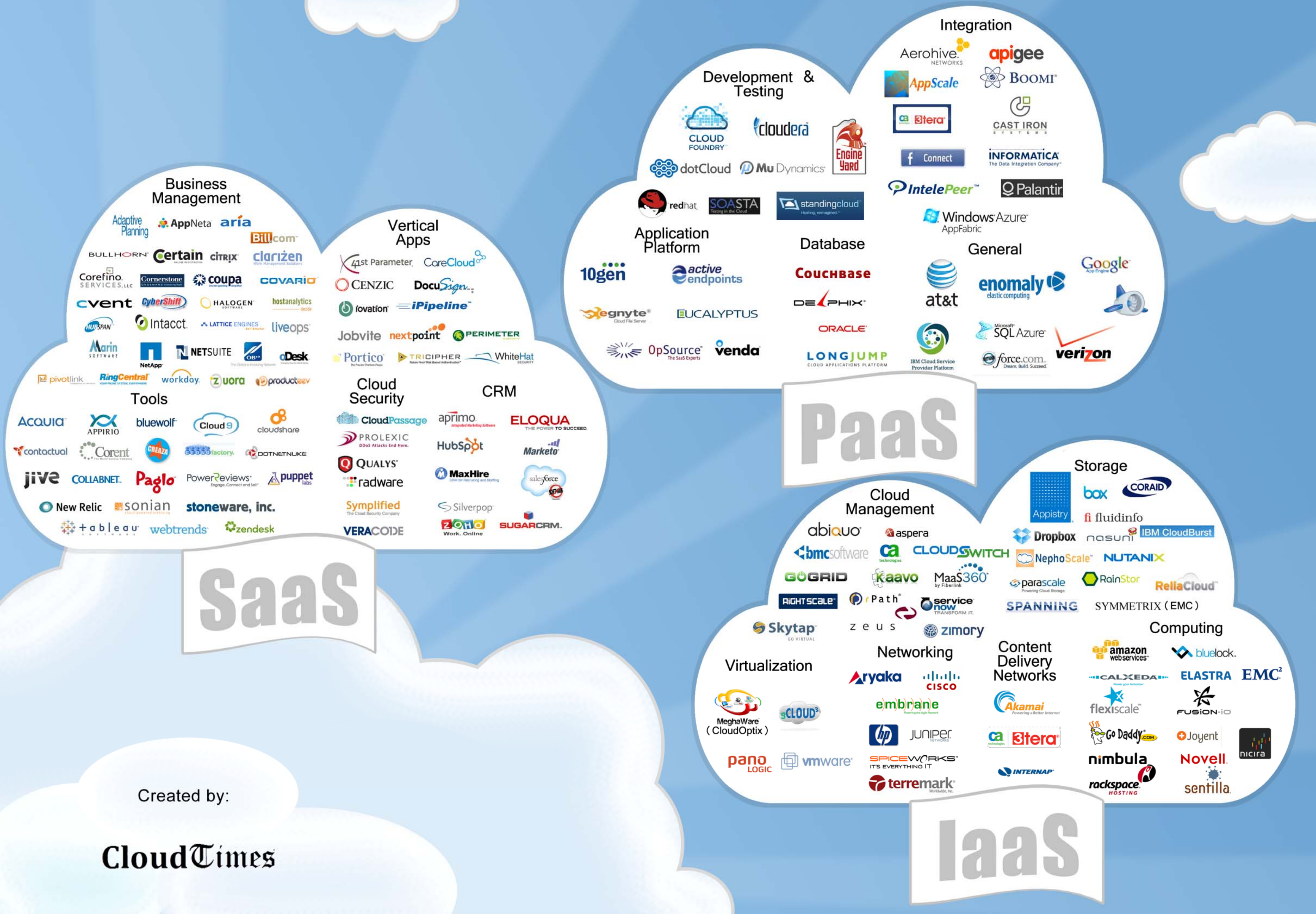
- On-demand self-service: Get it when you need it
- Measured service: Pay for what you use
- Rapid elasticity: Increase and decrease capacity quickly
- Broad network access: Access it from any Internet connection
- Resource pooling: Share fixed costs, which lowers individual costs

Source: **The NIST Definition of Cloud Computing**

One more for the auditors:

- Multitenant architecture: Common code set and database for all customers

Cloud Companies



SaaS

Business Management

Adaptive Planning, AppNeta, aria, Bill.com, BULLHORN, Certain, CITRIX, clarizen, Corefino SERVICES, LLC, Cornerstone, coupa, COVARIO, cvent, CyberShift, HALOGEN SOFTWARE, hostanalytics, HUBSPAN, Intacct, LATTICE ENGINES, liveops, Marin SOFTWARE, NetApp, NETSUITE, OB10, oDesk, pivotlink, RingCentral, workday, zuora, productEev

Tools

ACQUIA, APPIRIO, bluewolf, Cloud 9, cloudshare, contactual, Corent, CREAZA, factory, DOTNETNUKE, jive, COLLABNET, Paglo, PowerReviews, puppet labs, New Relic, sonian, stoneware, inc., tableau, webtrends, zendesk

Vertical Apps

41st Parameter, CareCloud, CENZIC, DocuSign, iovation, iPipeline, Jobvite, nextpoint, PERIMETER, Portico, TRICIPHER, WhiteHat SECURITY

Cloud Security

CloudPassage, PROLEXIC, QUALYS, radware, Symplified, VERACODE

CRM

aprimo, ELOQUA, HubSpot, Marketo, MaxHire, salesforce, Silverpop, ZOHO Work. Online, SUGARCRM.

PaaS

Development & Testing

CLOUD FOUNDRY, cloudera, Engine Yard, dotCloud, Mu Dynamics, redhat, SOASTA, standingcloud

Integration

Aerohive NETWORKS, apigee, AppScale, BOOMI, ca 3tera, CAST IRON SYSTEMS, f Connect, INFORMATICA The Data Integration Company, IntelePeer, Palantir, Windows Azure AppFabric

Application Platform

10gen, active endpoints, egnyte, EUCALYPTUS, OpSource The SaaS Experts, venda

Database

COUCHBASE, DELPHIX, ORACLE, LONGJUMP CLOUD APPLICATIONS PLATFORM

General

at&t, enomaly elastic computing, Google App Engine, IBM Cloud Service Provider Platform, SQL Azure, force.com Dream. Build. Succeed., verizon

IaaS

Storage

Appistry, box, CORAID, fluidinfo, Dropbox, nasuni, IBM CloudBurst, NephoScale, NUTANIX, parascale, RainStor, RelliaCloud, SPANNING, SYMMETRIX (EMC)

Cloud Management

abiquo, aspera, bmcsoftware, ca technologies, CLOUDSWITCH, GOGRID, Kaavo, MaaS360 by Fiberlink, RIGHTSCALE, rPath, service now, zeus, Skytap, zimory

Virtualization

MeghaWare (CloudOptix), sCLOUD, pano LOGIC, vmware

Networking

Aryaka, CISCO, embrane, hp, JUNIPER NETWORKS, SPICEWORKS IT'S EVERYTHING IT, terremark

Content Delivery Networks

Akamai, ca 3tera, INTERNAP

Computing

amazon webservices, bluelock, CALXEDA, ELASTRA, EMC2, flexiscale, FUSION-io, Go Daddy.com, Joyent, nicira, nimbula, Novell, rackspace HOSTING, sentilla

Created by:

CloudTimes

The Benefits

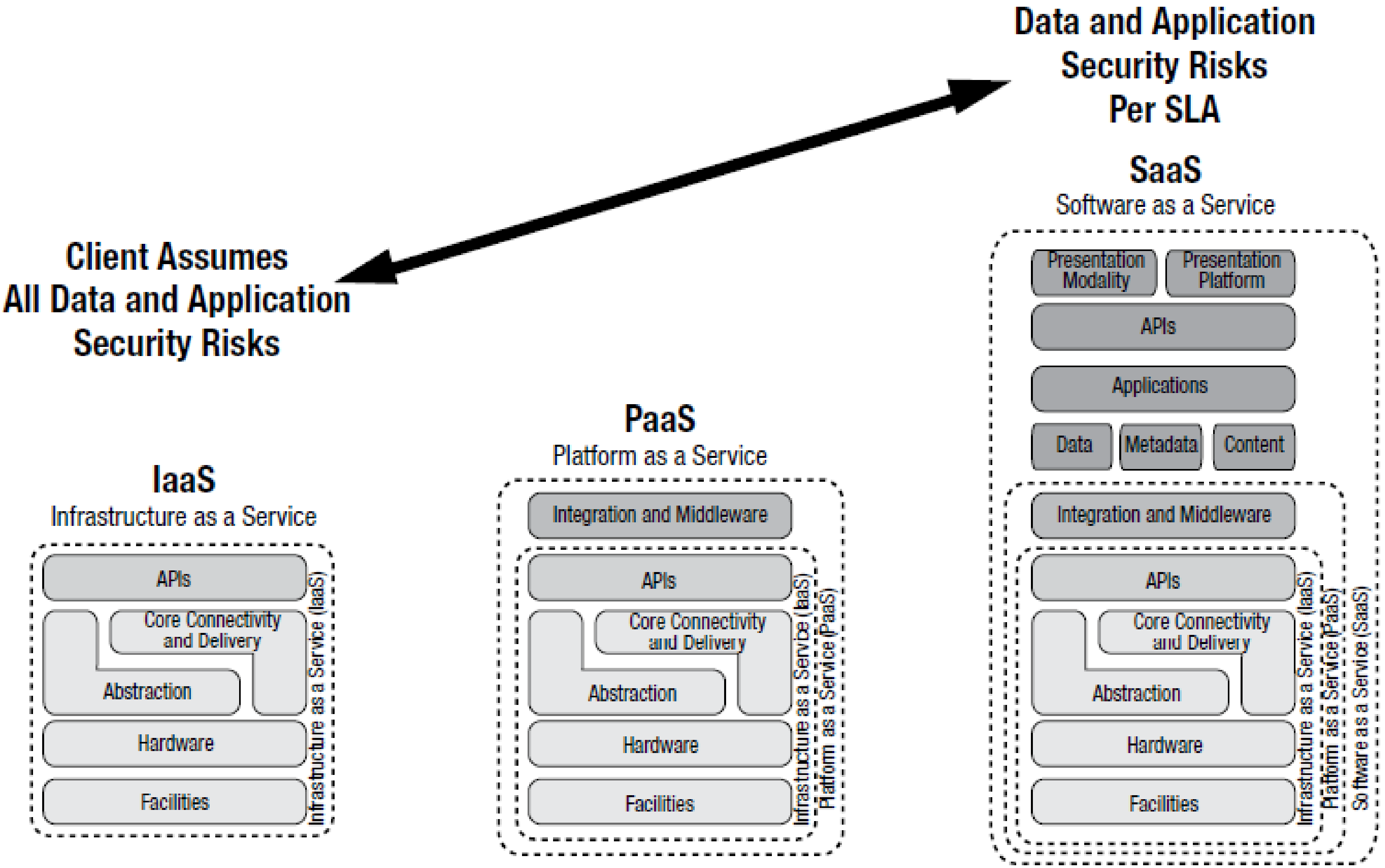
BAKER TILLY

Candor. Insight. Results.

- Pay-as-you-go model
- Scalable solution that supports rapid business growth
- Cost transparency to the end-user/business
- Quicker time to market for IT solutions
- Outsourcing competencies that are not core to the business
- Ease of licensing

Cloud Risks and Challenges

Cloud Risks at each layer


Data and Application Security Risks Per SLA
Client Assumes All Data and Application Security Risks
IaaS
Infrastructure as a Service
APIs
Core Connectivity and Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
PaaS
Platform as a Service
Integration and Middleware
APIs
Core Connectivity and Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
SaaS
Software as a Service
Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Content
Integration and Middleware
APIs
Core Connectivity and Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)

- Configuration options / standards
- VM security

- Proprietary development platforms
- Encryption

- Data portability
- Password management

Security: Two Perspectives

BAKER TILLY

Candor. Insight. Results.

The Good:

- In 2010 and 2011, there were 1,161 security breaches made public per the Privacy Rights Clearinghouse
- 43 million records were compromised
- Of those, 20 were from hacking or malware
- One of those was due in part to a cloud partner

PRC

Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

The Bad:

- Cloud provider security doesn't enhance competitive edge
- Providers believe it is the customer's responsibility
- Customers purchase cloud for lower costs and faster deployment (Not improved security or compliance)
- Majority of providers don't have dedicated security teams

Ponemon INSTITUTE

Security of Cloud Computing Providers Study

Sponsored by CA Technologies

Independently conducted by Ponemon Institute LLC

Publication Date: April 2011

Cloud Challenges - Plan for the worst?

BAKER TILLY

Candor. Insight. Results.

- Geographic location of data
- Data recoverability / export
- Security breaches
- Confidentiality
- Provider use of data
- Subpoenaed data
- SLA Development / Monitoring
- Change-in-control provisions
- Internal control verification

What should we be asking?

BAKER TILLY

Candor. Insight. Results.

To our company:

- Do we understand our implementation and the key risks associated with our use of cloud technologies

To our cloud providers:

- How can you provide assurance and transparency into your control environment

Emerging Cloud Control Frameworks

Cloud Security Alliance – Cloud Controls Matrix

Cloud Controls Matrix	
What is it?	• Part of CSA GRC stack • Self assessment framework for cloud service providers to disclose fundamental security controls • Aligned with delivery models and supplier relationship • Intended to create transparency / be shared publicly • Draws from ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP
How to use it?	• See if cloud provider has published • Encourage completion of the self assessment • Evaluate responses in relation to your organization's objectives
Challenges to IA	• Adoption is still low
Publisher	Cloud Security Alliance (https://cloudsecurityalliance.org/research/ccm/)

Cloud Security Alliance –
Cloud Controls Matrix

10 primary categories

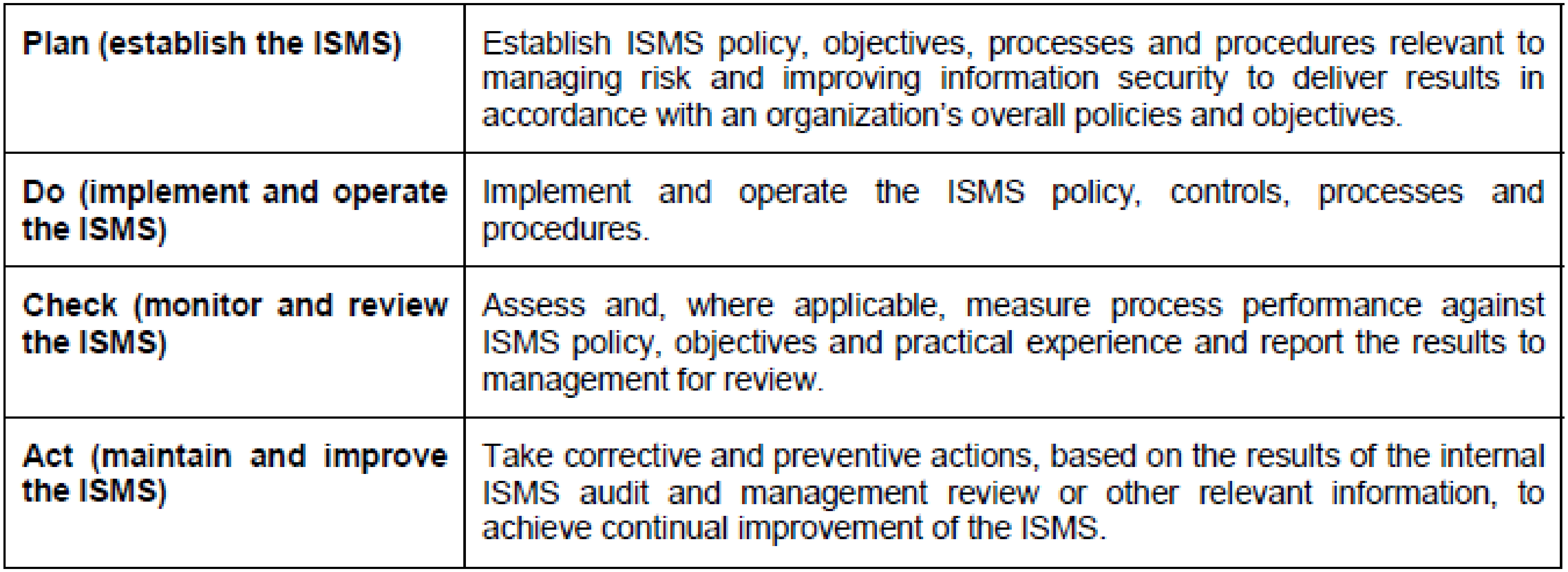
- Compliance
- Data governance
- Facility security
- Human resources security
- Information security
- Legal
- Operations Management
- Risk Management
- Resiliency
- Security Architecture

ISO 27001

ISO 27001	
What is it?	• Requirements for information security management system • PDCA process based model – Establish, Implement, Monitor, Improve • It aims toward the “preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved” • Management standard, so organizations can be certified
How to use it?	• Understand the process requirements contained within the standard and map to your organization’s requirements for incident management
Challenges to IA	• It doesn’t guarantee that a company is secure • Limited applicability to application changes • Not to be confused with ISO 27002
Publisher	International Organization for Standardization (http://www.iso.org/iso/home.htm)

ISO 27001

International Organization for Standardization



Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

- **ISO/IEC 27001:2005**

ISACA Cloud Audit

ISACA®

Trust in, and value from, information systems

IT CONTROL OBJECTIVES *for* CLOUD COMPUTING:

CONTROLS AND ASSURANCE IN THE CLOUD

Cloud Audit	
What is it?	• Work program to execute a controls review of a cloud provider • Focused in three areas: planning and scoping, governing the cloud, and operating in the cloud • Also includes a framework for control maturity assessment
How to use it?	• Use as a base work program to conduct a controls review of your cloud provider(s)
Challenges to IA	• Access to data… cloud provider may not be a willing participant • Limited applicability to direct data modifications and application changes
Publisher	ISACA (http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Management-Audit-Assurance-Program.aspx)

Alignment to Cloud Audit

1. Planning and scoping the audit	CCM	ISO 27001
1.1 Define the audit/assurance objectives. The audit/assurance objectives are high level and describe the overall audit goals.	◔	◔
1.2 Define the boundaries of review. The review must have a defined scope. Understand the core business process and its alignment with IT, in its noncloud form and current or future cloud implementation.	◔	◔
1.3 Identify and document risks. The risk assessment is necessary to evaluate where audit resources should be focused. In most enterprises, audit resources are not available for all processes. The risk-based approach assures utilization of audit resources in the most effective manner.	◑	◔
1.4 Define the change process. The initial audit approach is based on the reviewer’s understanding of the operating environment and associated risks. As further research and analysis are performed, changes to the scope and approach may result.	◔	◔
1.5 Define assignment success. The success factors need to be identified. Communication among the IT audit/assurance team, other assurance teams and the enterprise is essential.	○	◔
1.6 Define the audit/assurance resources required. The audit/assurance resources required for a successful review need to be defined.	◔	◔
1.7 Define deliverables. The deliverable is not limited to the final report. Communication between the audit/assurance teams and the process owner about the number, format, timing and nature of deliverables is essential to assignment success.	○	○
1.8 Communications The audit/assurance process must be clearly communicated to the customer/client.	○	◔

Alignment to Cloud Audit

2. Governing the cloud	CCM	ISO 27001
2.1 Governance and Enterprise Risk Management (ERM) • Governance functions are established to ensure effective and sustainable management processes that result in transparency of business decisions, clear lines of responsibility, information security in alignment with regulatory and customer organization standards, and accountability. • Risk management practices are implemented to evaluate inherent risks within the cloud computing model, identify appropriate control mechanisms, and ensure that residual risk is within acceptable levels. • A process to manage information risk exists and is integrated into the organization’s overall ERM framework. Information risk management information and metrics are available for the information security function to manage risks within the risk tolerance of the data owner. • The customer recognizes the outsourced relationship with the service provider. The customer understands its responsibilities for controls, and the service provider has provided assurances of sustainability of those controls.	◑	◑
2.2 Legal and Electronic Discovery • The service provider and customer establish bilateral agreements and procedures to ensure contractual obligations are satisfied, and these obligations address the compliance requirements of both the customer and service provider. • Legal issues relating to functional, jurisdictional and contractual requirements are addressed to protect both parties, and these issues are documented, approved and monitored.	◔	◑

Alignment to Cloud Audit

BAKER TILLY

Candor. Insight. Results.

2. Governing the cloud	CCM	ISO 27001
2.3 Compliance and Audit • The right to audit is clearly defined and satisfies the assurance requirements of the customer's board of directors, audit charter, external auditors and any regulators having jurisdiction over the customer. • The service provider's operating environment should be subject to audit to satisfy the customer's audit charter, compliance requirements and good practice controls without restriction. • The use of cloud computing does not invalidate or violate any customer compliance agreement. • Service provider security assurance is provided through ISO27001 Certification.	◔	◑
2.4 Portability and Interoperability • Planning for the migration of data, such as formats and access, is essential to reducing operational and financial risks at the end of the contract. The transition of services should be considered at the beginning of contract negotiations.	○	○

Alignment to Cloud Audit

3. Operating in the cloud	CCM	ISO 27001
3.1 Incident Response, Notification and Remediation • Incident notifications, responses, and remediation are documented, timely, address the risk of the incident, escalated as necessary and are formally closed.	◕	◕
3.2 Application Security • Applications are developed with an understanding of the interdependencies inherent in cloud applications, requiring a risk analysis and design of configuration management and provisioning process that will withstand changing application architectures.	◑	○
3.3 Data Security and Integrity • Data are securely transmitted and maintained to prevent unauthorized access and modification.	◑	○
3.4 Identity and Access Management • Identity processes assure only authorized users have access to the data and resources, user activities can be audited and analyzed, and the customer has control over access management.	◕	◔
3.5 Virtualization • Virtualization operating systems are hardened to prevent cross-contamination with other customer environments.	◑	○

Other Control Assurance Reporting Frameworks

SOC1

BAKER TILLY

Candor. Insight. Results.

Service Organization Control 1	
What is it?	Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
How to use it?	These reports are important components of user entities' evaluation of their internal controls over financial reporting for purposes of comply with laws and regulations such as the Sarbanes-Oxley Act and the user entities' auditors as they plan and perform audits of the user entities' financial statements
Challenges to IA	• Focus on financial reporting controls - it may not cover all the controls you care about. Typical controls may include: • Logical Security • Physical Security & Environmental Security • User Access • Change Management • Restricted to customers
Publisher	AICPA (http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx)

SOC 2/3

BAKER TILLY

Candor. Insight. Results.

Service Organization Control 2/3	
What is it?	Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. (Trust Services Principles – Including WebTrust & SysTrust)
How to use it?	These reports are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization to form an important part of stakeholders: • Understanding of operations • Oversight of the organization • Vendor management program • Internal corporate governance and risk management processes • Regulatory oversight
Challenges to IA	• Some objectives require significant auditor judgment • Restricted to those familiar with subject matter(SOC2) • Limited Info (SOC3) – General Use Report
Publisher	AICPA (http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx)

AWS Example

AWS Certifications and Third-party Attestations

- SOC 1 (SSAE 16/ISAE 3402)
- FISMA Moderate
- PCI DSS Level 1
- ISO 27001
- International Traffic in Arms Regulations
- FIPS 140-2Key Compliance Issues and AWS

amazon web services™

Amazon Web Services: Risk and Compliance

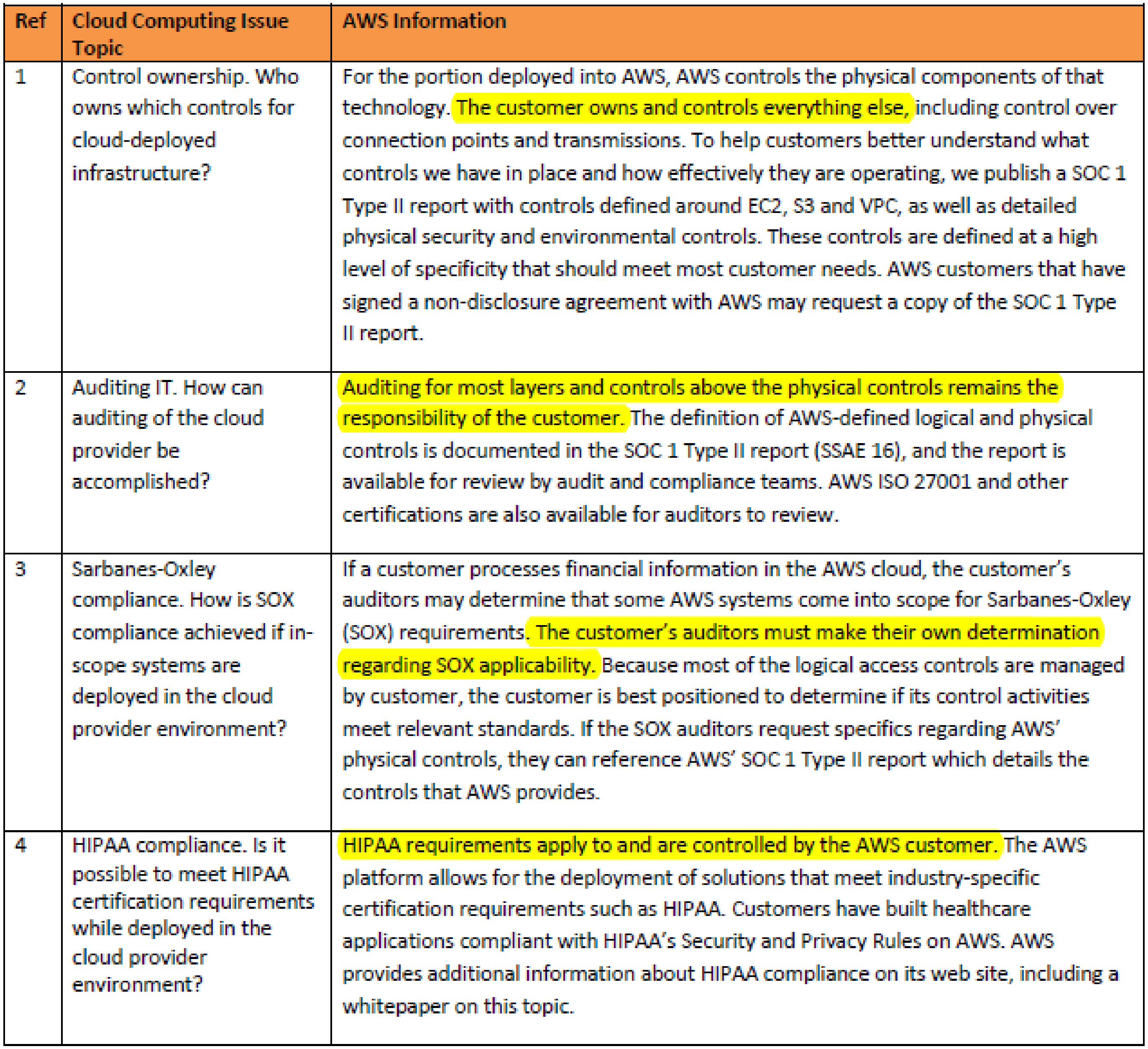
January 2012

(Please consult http://aws.amazon.com/security **for the latest version of this paper)**

Strong customer compliance and governance might include the following basic approach:

1. Review information available from AWS together with other information to understand as much of the entire IT environment as possible, and then document all compliance requirements.
2. Design and implement control objectives to meet the enterprise compliance requirements.
3. Identify and document controls owned by outside parties.
4. Verify that all control objectives are met and all key controls are designed and operating effectively.

AWS Example continued



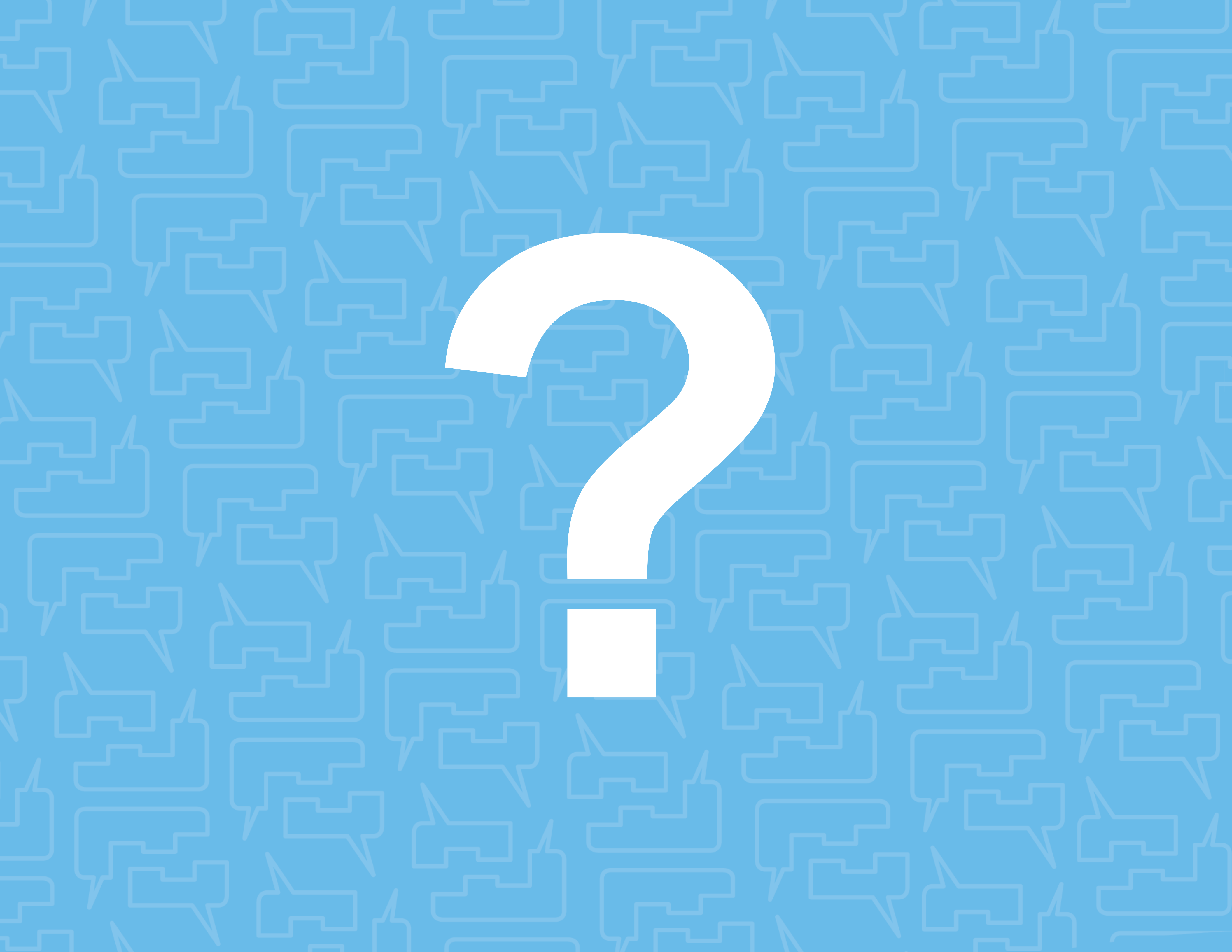
Ref	Cloud Computing Issue Topic	AWS Information
1	Control ownership. Who owns which controls for cloud-deployed infrastructure?	For the portion deployed into AWS, AWS controls the physical components of that technology. The customer owns and controls everything else, including control over connection points and transmissions. To help customers better understand what controls we have in place and how effectively they are operating, we publish a SOC 1 Type II report with controls defined around EC2, S3 and VPC, as well as detailed physical security and environmental controls. These controls are defined at a high level of specificity that should meet most customer needs. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report.
2	Auditing IT. How can auditing of the cloud provider be accomplished?	Auditing for most layers and controls above the physical controls remains the responsibility of the customer. The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report (SSAE 16), and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review.
3	Sarbanes-Oxley compliance. How is SOX compliance achieved if in-scope systems are deployed in the cloud provider environment?	If a customer processes financial information in the AWS cloud, the customer's auditors may determine that some AWS systems come into scope for Sarbanes-Oxley (SOX) requirements. The customer's auditors must make their own determination regarding SOX applicability. Because most of the logical access controls are managed by customer, the customer is best positioned to determine if its control activities meet relevant standards. If the SOX auditors request specifics regarding AWS' physical controls, they can reference AWS' SOC 1 Type II report which details the controls that AWS provides.
4	HIPAA compliance. Is it possible to meet HIPAA certification requirements while deployed in the cloud provider environment?	HIPAA requirements apply to and are controlled by the AWS customer. The AWS platform allows for the deployment of solutions that meet industry-specific certification requirements such as HIPAA. Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides additional information about HIPAA compliance on its web site, including a whitepaper on this topic.

Key Take Aways

BAKER TILLY

Candor. Insight. Results.

- Evolving reporting landscape combines self assessment and independent assurance reports
- Still need to understand how contract addresses operational risks
- Work with cloud providers to exercise right-to-audit clause or complete CCM self assessment



Thank you

BAKER TILLY

Candor. Insight. Results.

Tom Wojcinski

414.777.5536

tom.wojcinski@bakertilly.com

Chris Tait

414.777.5515

christopher.tait@bakertilly.com