KPMG

The Changing Internet Environment

ISACA SAN FRANCISCO CHAPTER

JUNE 2010

AUDIT ▪ TAX ▪ ADVISORY

Session Overview

- We are in the midst of a period of unprecedented change on the Internet.
- The rise of social networking and a new generation of advances in Web-based and mobile technology have spawned a new wave of innovation.
- Significant changes to the Internet infrastructure are underway to support new business models, an international user base, and additional security.
- Organizations are increasingly looking to innovative cloud computing services to solve business problems and accelerate time to market.
- This session is intended to help managers, technologists, and auditors prepare to address the risks and opportunities associated with the changing Internet environment.

Agenda

- Technology Business Climate
- Changing Internet Infrastructure
- Cloud Computing
- Q&A

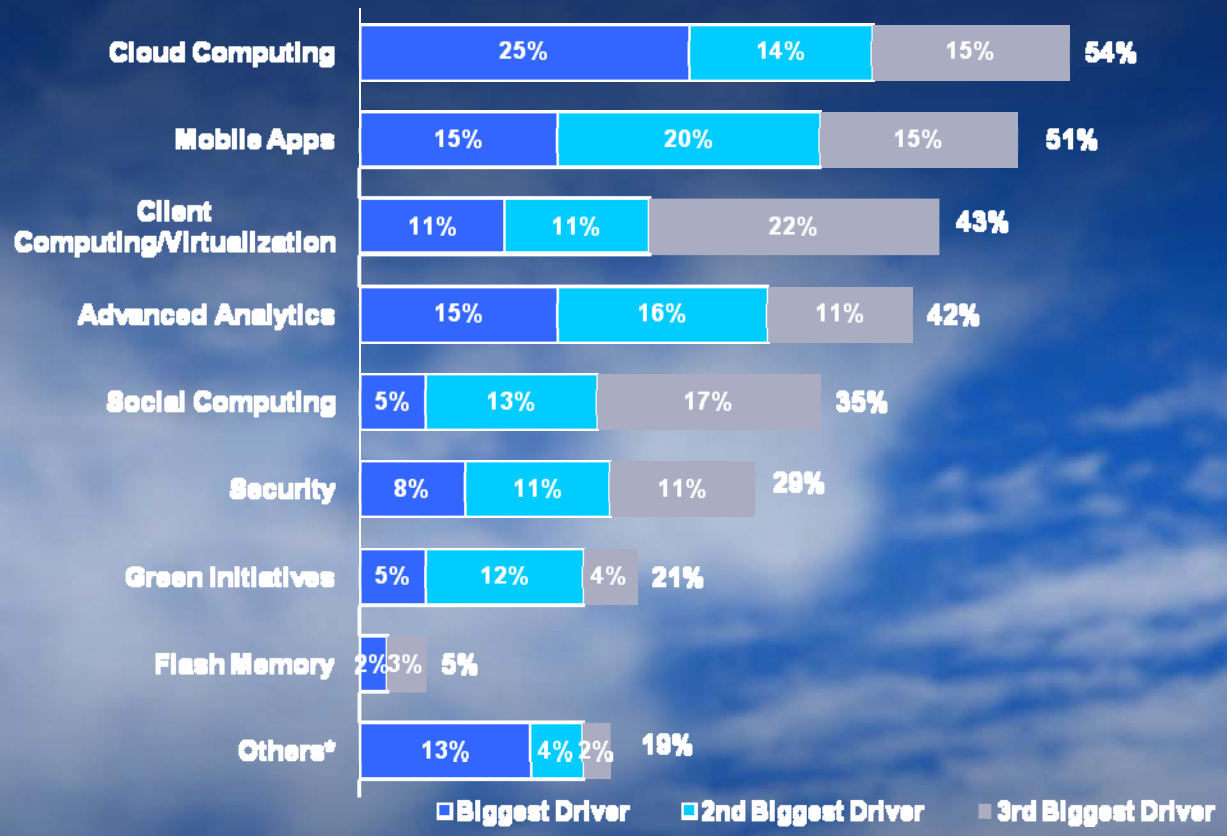
Highlights from KPMG's Business Climate Survey Technology Sector

June 2010

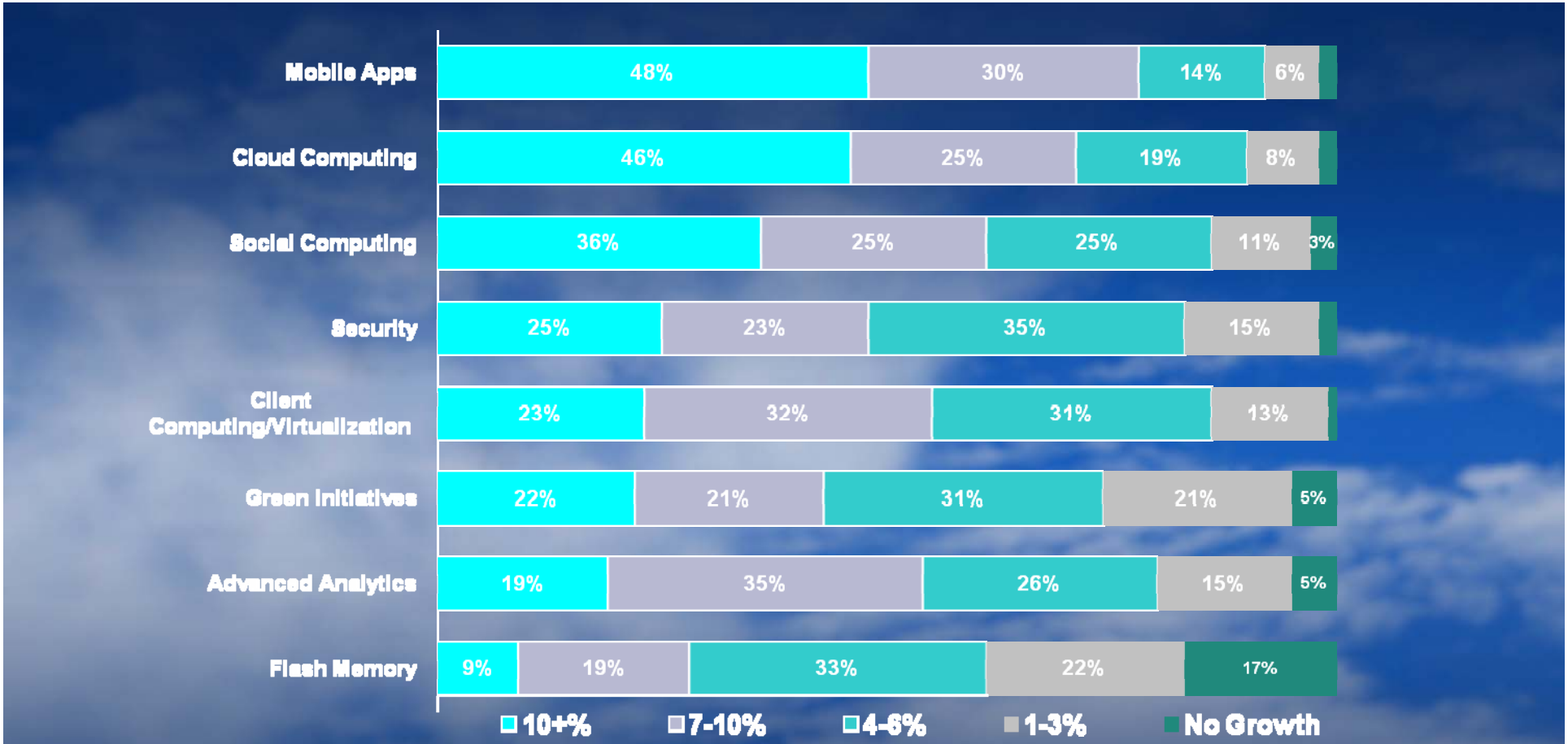
Key Findings from KPMG's Business Climate Survey Technology Sector – June 2010

- Executives in technology see stronger revenue and profitability in their sector resulting from increased spending on global information technology.
- About three-fourths of respondents expect their companies to add headcount in 2010, with more than a third projecting the increase to be seven percent or more. They expect most of the employment gains to come in China, India, and Brazil.
- Seven in ten respondents believe their sector will recover ahead of the U.S. economy. On average, the executives think the U.S. recovery will take hold in March 2012 almost a full year later than they projected in last summer's survey.
- Respondents named the following as the biggest drivers of revenue growth over the next three years: cloud computing and mobile applications.

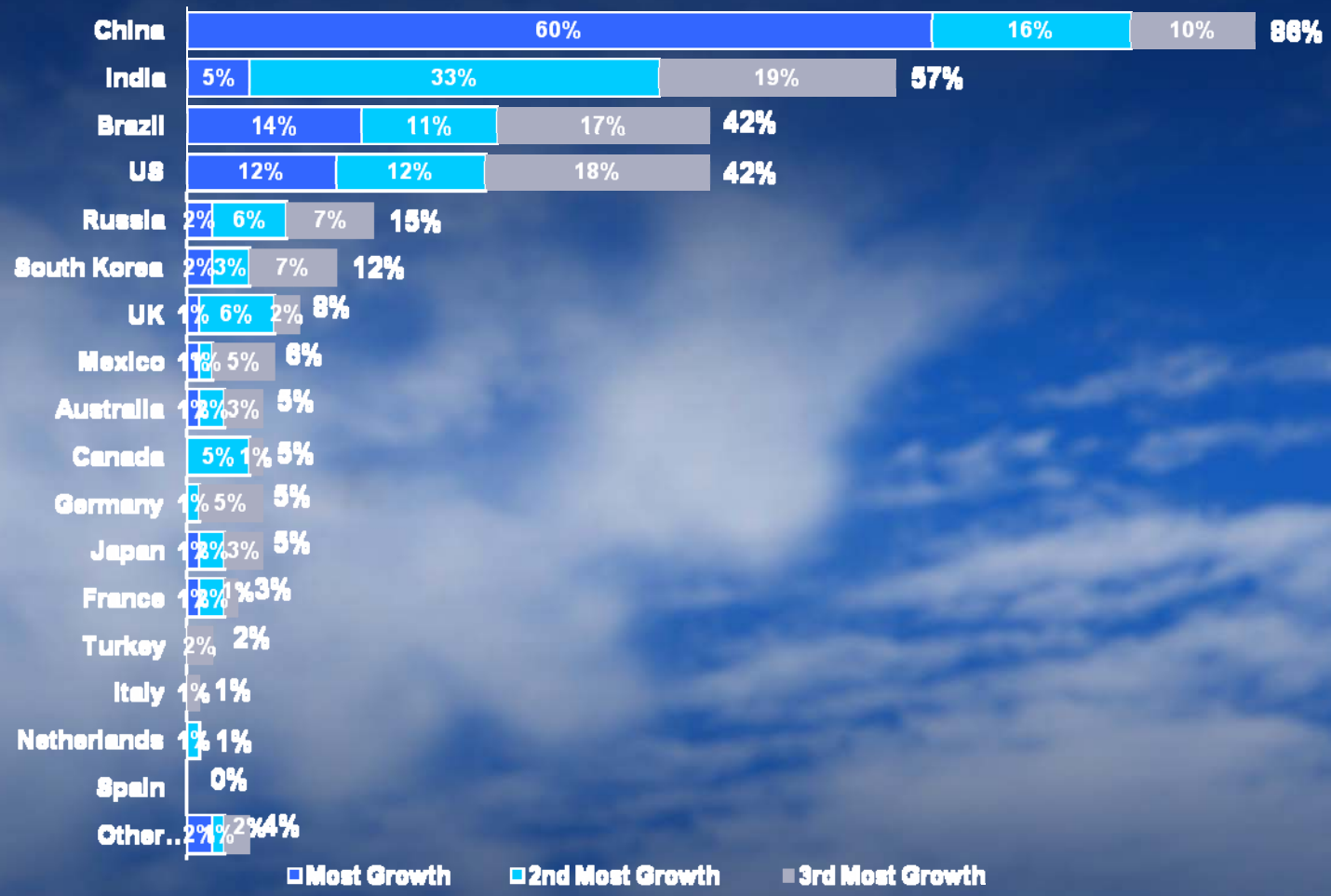
Biggest Drivers of Company's Revenue Growth: Next One to Three Years



Anticipated Total Growth Rate Over Next Two Years Related to Specific Areas



Countries with Highest Revenue Growth Over Next 12 Months



Changing Internet Infrastructure

Internet Infrastructure Changes

- Majority of global business networks are entirely reliant on Internet availability, stability, and integrity.
- Multiple large scale Internet infrastructure changes are anticipated to be deployed or are in process of being deployed over the next few years:
  - DNSSEC
  - New gTLDs
  - IDN TLDs
- Any one of these changes alone would constitute a significant architectural and operational challenge.

DNS Security Extensions Protocol (DNSSEC)

- **DNS Vulnerabilities**
  - DNS forms the building blocks of the Internet and was designed as a distributed database to enable it to scale across a range of operating conditions
  - Unfortunately, the Internet name resolution function is vulnerable to a variety of attacks such as DNS cache poisoning and man-in-the-middle attacks
- **DNSSEC Value Proposition**

  Involves modifications to the DNS protocol to introduce:
  - Origin authentication of DNS data
  - Data integrity
- **DNSSEC does not provide**
  - Confidentiality of data
  - Protection from DDOS attacks

How DNSSEC Works

- Cryptographic Signing of DNS Responses
  - DNSSEC works by digitally signing responses to DNS lookups using public key cryptography.
  - The protocol introduces additional DNS record types which include a signature of the lookup answer sent in response the query received.
  - In order to validate the source and integrity of the response received, DNS resolvers should have the capability to check these signatures thus demonstrating the authenticity of the information supplied.
  - Adoption requires an overhaul of the DNS system to include cryptographic key management capabilities and DNSSEC-aware infrastructure.

DNSSEC Deployment

- Deployment Progress
  - Deployment has been slow although the protocol has been under development for more than a decade.
  - Gained momentum in 2008 after discovery of the Dan Kaminsky bug.
  - DNSSEC identified as an effective protocol to prevent such attacks.
  - Effective only when fully deployed across the Internet to establish a chain of trust.
  - Until then, Web sites remain vulnerable to Kaminsky-style attacks.

DNSSEC Adoption

- A number of TLDs have already been signed
  - ccTLDs (i.e., bg, br, ch, cz, lk, na, nu, pm, pr, pt, se etc.)
  - gTLDs (i.e., arpa, gov, org)
- U.S. Office of Management and Budget has mandated that all federal agencies support DNSSEC
- Planned signings
  - Root zone (July 2010), currently operating in DURZ mode
  - .net (late 2010)
  - .com (early 2011)

DNSSEC Preparation

- Get DNSSEC on your radar now. DNSSEC management is different from DNS management.
- If DNS management is outsourced to a service provider:
  - Inquire about DNSSEC deployment plans and cryptographic key management practices.
- If DNS is hosted and managed in-house:
  - Does your DNS resolver support validation?
  - Do you have a plan to sign your zone?
  - Consider changes to infrastructure (DNSSEC aware hardware and software)
  - Consider impact on network and resources (i.e., firewalls, load balancers, capacity and bandwidth)
  - Identify signing/cryptographic key management best practices
  - Develop and test emergency roll-back procedures.

KPMG

New Generic Top-level Domains (gTLDs)

- gTLDs are part of the Internet's global addressing system
- Currently 21 gTLDs are in operation
- In 2008, ICANN approved the new gTLD program
  - Initiative that will enable the introduction of new gTLDs (including both ASCII and IDN) into the domain name space
  - Not expected to affect the way the Internet operates
  - May potentially change the way people find information on the Internet or how businesses plan and structure their online presence
  - Program is still under development and is expected to begin accepting applications by the end of 2010

New gTLDs – Opportunities and Challenges

- Opportunities
  - Enhanced brand recognition
  - Effective marketing vehicle
  - Enhanced control over brand use online
  - Enhanced protection with introduction of high-security TLDs that have more stringent application and compliance requirements
- Overarching issues identified by ICANN
  - Trademark protection
  - TLD demand and economic analysis
  - Security and stability
  - Potential for malicious conduct

New gTLDs – Program Application

- New gTLD Application Process
  - Any public or private organization worldwide may apply to create a new gTLD.
  - All applicants need to meet very specific operational and technical criteria.
  - New gTLD registries are expected to comply with ICANN's contract to preserve the security, stability and global interoperability of the Internet.
- Draft Applicant Guidebook
  - Developed by ICANN as reference roadmap for potential gTLD applicants.
  - Covers technical and operational criteria, financial criteria, evaluation fees, required documentation, evaluation processes, and objection procedures.
  - Applications to be assessed against published criteria.

Internationalized Domain Names (IDN) TLDs

- **Internet User Demographics**
  - **More than 70 percent of Internet users are non-English speakers, while the dominant language used on the internet is English** ***(Source: www.internetworldstats.com).***
  - **IDNs on the second and third levels exist in some generic top-level domains (gTLDs) and in some country code top-level domains (ccTLDs).**
- **IDN TLDs**
  - **Program to implement internationalized top-level domains represented by local language character in the root zone. Such domain names could contain letters or characters from non-ASCII scripts.**
  - **Internet users around the world can establish and use domains in native language and scripts.**

Internationalized Domain Names (IDN) TLDs

- **Provisioning of IDN TLDs**

  IDN TLDs will be made available by ICANN through two separate processes:

  - **New gTLD Program**
  - **IDN ccTLD Fast Track Process**

Internet Infrastructure Changes
Key Takeaways

- With the renewed emphasis on the importance of the Internet with regards to cloud-based applications and services, these impending changes are anticipated to have a significant impact on the availability of resources for operations once fully deployed.
- As a result, careful planning and preparation is necessary to ensure organization agility and robustness when responding to the demands of the changing Internet infrastructure.

Cloud Computing

Cloud Marketplace

- Many interpretations of “cloud”
- Evolution of cloud services
- State of adoption
- Mobile and social networking

Cloud Models

Service Delivery Models

- Software-as-a-Service (SaaS)
- Platform-as-a-Service (PaaS)
- Infrastructure-as-a-Service (IaaS)
- Security-as-a-Service

Cloud Deployment Models

- Public
- Hybrid
- Private

Key Challenges in Adopting the Cloud

Greatest Concerns Surrounding Cloud Adoption at Your Company	
Security	45%
Integration with existing systems	26%
Loss of control over data	26%
Availability concerns	25%
Performance issues	24%
IT governance issues	19%
Regulatory/compliance concerns	19%
Dissatisfaction with vendor offerings/pricing	12%
Ability to bring systems back in-house	11%
Lack of customization opportunities	11%
Measuring ROI	11%
Not sure	7%
Other	6%

*RESPONDENTS SELECTED UP TO THREE CRITERIA.
SOURCE: CIO RESEARCH

Security is the biggest challenge with the cloud

KPMG

Practical Approach

In designing their service offerings and supporting processes, Cloud Service Providers (CSPs) need to:

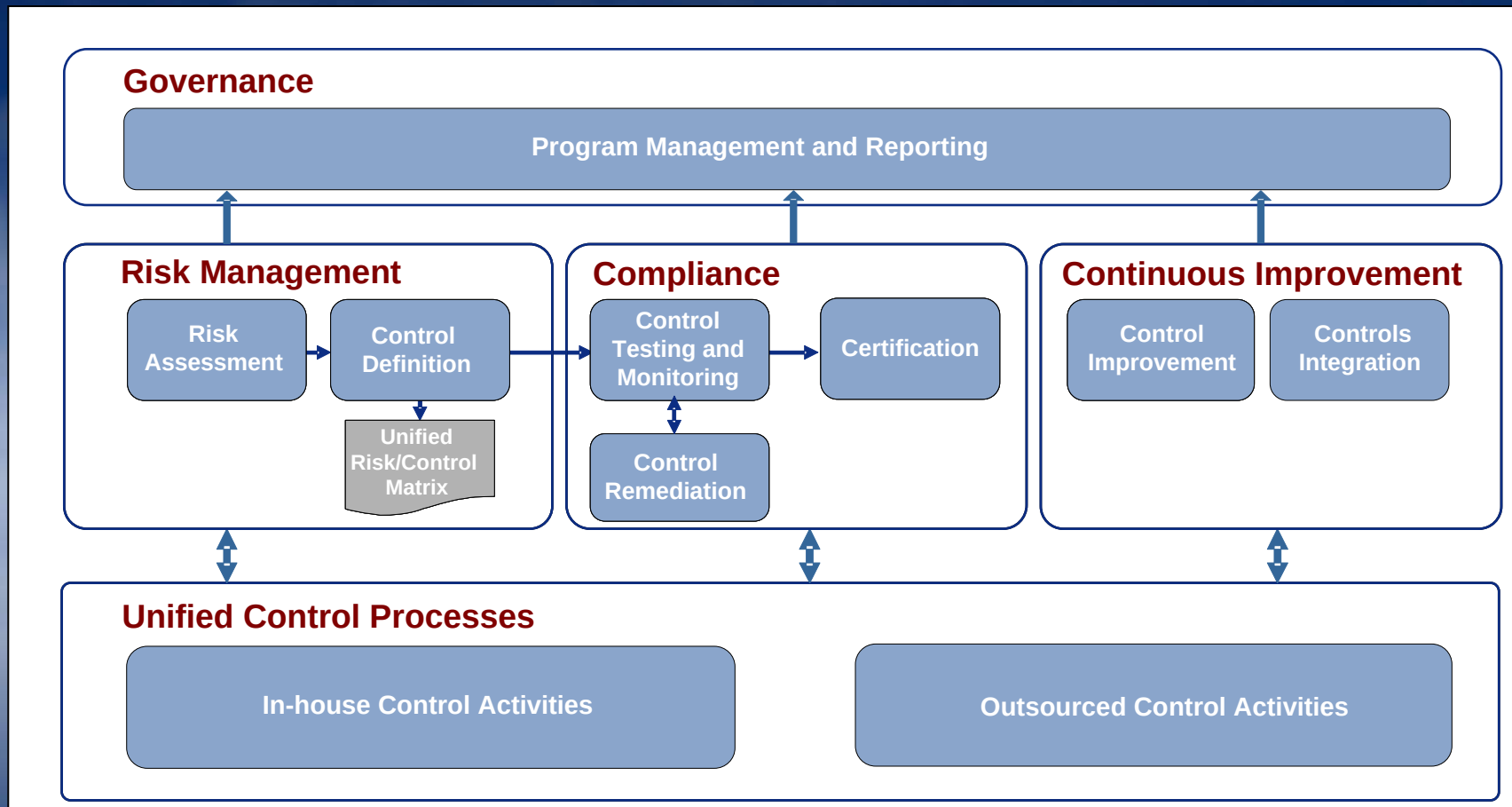
- Address the requirements of their current and planned customer base
- Establish a strong control foundation that will substantially meet customer requirements and minimize the need for infrastructure customization
- Set a standard that is high enough to address those requirements
- Define standardized processes to drive efficiencies
- Establish and implement an effective compliance monitoring program.

This can be achieved through a unified IT compliance approach.

Internal audit can play an important role.

KPMG

Unified IT Compliance Program



Baseline CSP Control Requirements – ISO 27001 Domains

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Areas of Added Emphasis for CSPs

- Data Protection/Segregation/Encryption
- Encryption Standards
- Logging
- Authentication to the Cloud
- Monitoring/Compliance Function
- Virtualization/Configuration Management

Focus Areas for CSP Users

- Managing Access to the Cloud
- Configuration Management
- Change Management
- Application Maintenance
- Vendor Management

Cloud Vendor Risk Mitigation Strategies

- Risk assessment
- Due diligence
- Contracting
- Auditing and ongoing monitoring

CSP External Audit Approaches – Today

Approach	Highlights
SAS 70	• Most applicable where the CSP plays a significant role in transaction processing or financial reporting for customers • Does not provide coverage of privacy or business continuity
Trust Services (SysTrust and WebTrust)	• Most applicable where the CSP needs to demonstrate to customers and prospects that its specific security, availability, confidentiality, processing integrity, and privacy controls are operating effectively over a period of time
ISO 27001	• Most applicable where global customers and prospects seek comfort with the CSP's overall security program

CSP External Audit Approaches – 2011

Approach	Highlights
Service Organization Report (Financial)	• Replaces SAS 70 for periods ending after 6/15/2011 • SSAE 16/ISAE 3402 attestation standards • Uses financial reporting focused criteria
Service Organization Report (Trust Services)	• Same structure/contents as service organization report (financial) • Uses security, availability, confidentiality, processing integrity, and privacy criteria
BITS AUP	• Cloud-focused “agreed-upon” test procedures • Builds upon the ISO 27001-based Financial Industry Shared Assessments Program (FISAP)

Interpreting External Audit Reports

- Type of report
- Period of coverage
- Audit opinion
- Auditor
- Scope
- Subservice organizations
- Description of controls
- User control considerations
- Control objectives and control activities
- Test procedures and test results

Cloud Computing
Key Takeaways

- The cloud services market covers a wide spectrum of innovation.
- Cloud service providers can benefit from a unified IT compliance approach to security and compliance.
- Users and potential users of cloud services should consider enhancing their vendor risk management programs to consider cloud services.
- There are a variety of standardization activities underway and external audit approaches available to provide assurance over cloud services.

Q&A

For More Information

Mark A. Lundin

KPMG LLP

Partner

415-963-5493

mlundin@kpmg.com

Reema Anand

KPMG LLP

Manager

650-404-4874

reemaanand@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.