Powerful Insights.
Proven Delivery.®

Cloud Computing:

Background, Risks and Audit Recommendations

October 30, 2014

protiviti®
Risk & Business Consulting.
Internal Audit.

Table of Contents

protiviti®

Cloud Computing: Overview

Cloud Computing - Definition

Cloud Computing describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources

These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption

Key Features

- On demand self service
- Standardized IT based capability
- Rapid Elasticity
- Web based accessibility & flexibility
- Location independent resource pooling
- Scalability & resilience as key design components
- Prices on a consumption based model
- Ubiquitous network access

Gmail
2,626,252 followers on Google+

protiviti®

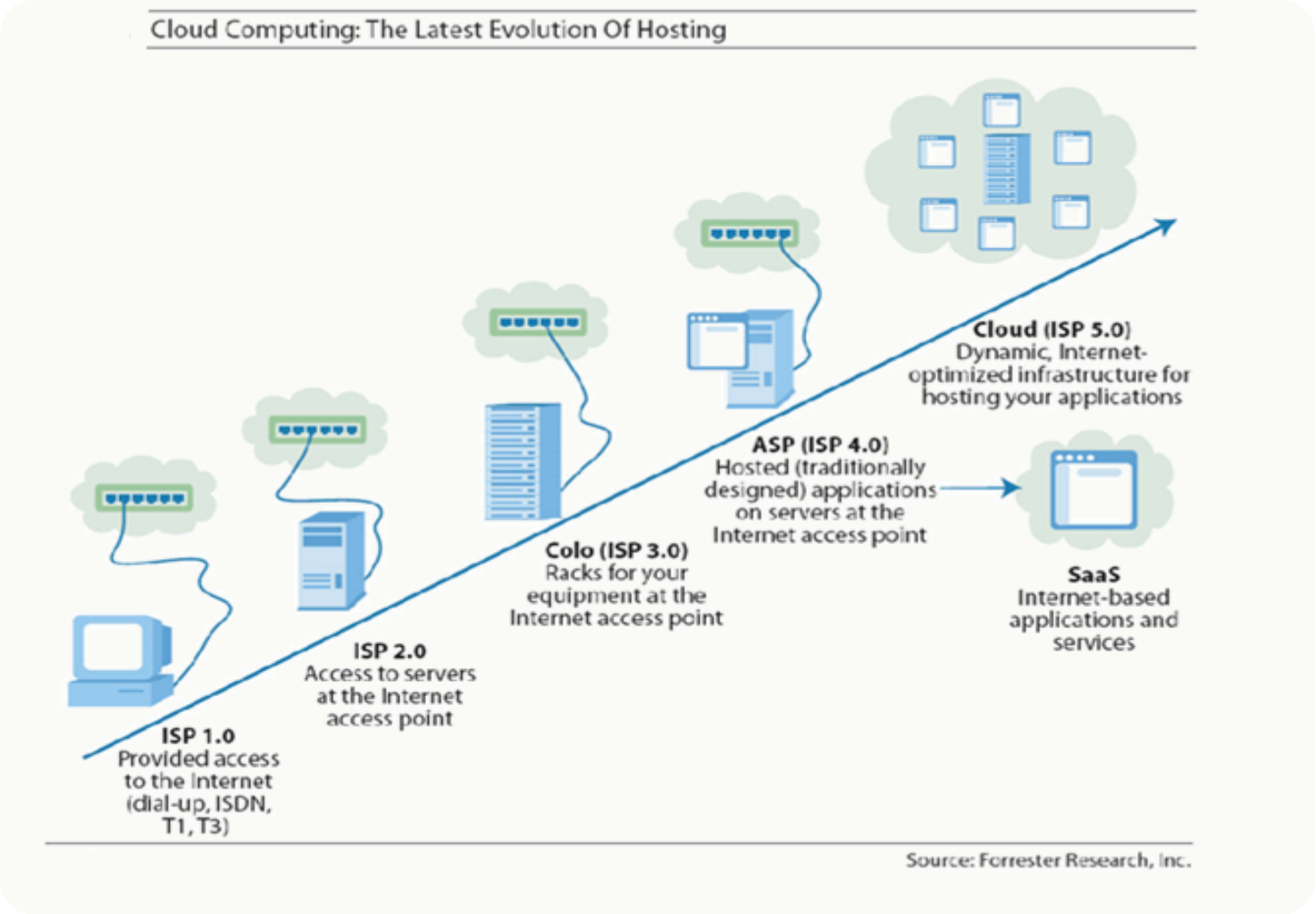
Essential Characteristics Of Cloud Computing

According to National Institute of Standards and Technology (NIST), the five essential characteristics of cloud computing are:

On-Demand Self Service	Authorized agencies must be able to provide and release capabilities, as needed, automatically, without requiring human interaction with each services provider.
Broad Network Access	Once provisioned, the software, platform, or infrastructure maintained by the cloud provider should be available over a network using thin or thick clients.
Resource Pooling	The resources provisioned from the cloud provider should be pooled to serve multiple agencies or programs using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the agency's self-service demand
Rapid Elasticity	Elasticity is defined as the ability to scale resources both up and down as needed. Cloud Computing capabilities should be rapidly and elastically provisioned and released.
Measured Service	Cloud resource usage should be monitored, controlled, and reported providing transparency for both the provider and consumer of the service.

protiviti®

The Latest Evolution Of Hosting



Source: http://blog.karmona.com/wp-content/uploads/2009/01/cloud-computing-the-latest-evolution-of-hosting.jpg

protiviti®

Cloud Computing Drivers and Inhibitors

Pay-as-you-go

Immediately scalable

Cloud characteristics

Multi-tenant

Highly abstracted

Drivers

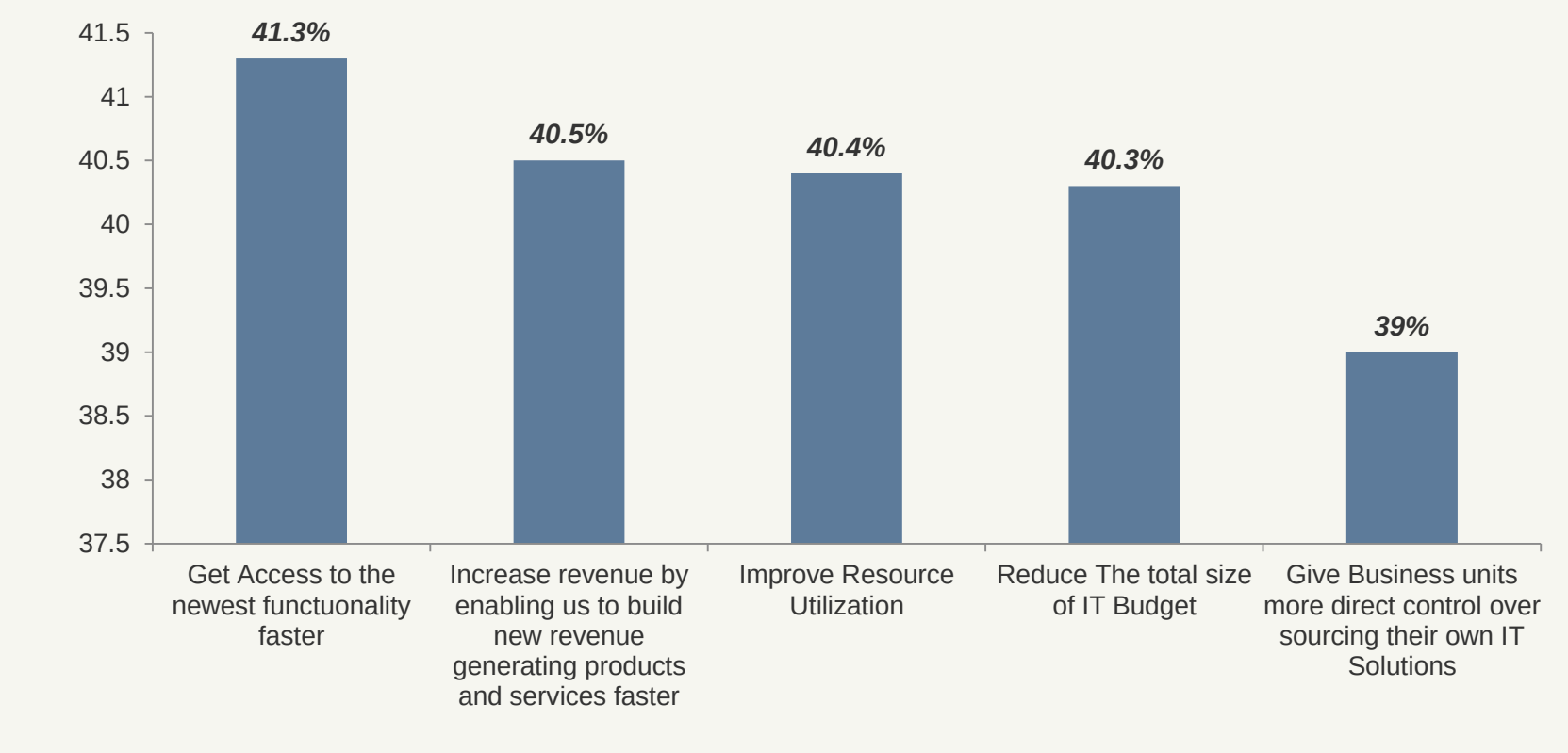
Inhibitors

- Increased ROI
  Quicker payback
  Lower upfront investment
- Accelerated deployment
- Greater flexibility and scalability
- Focus on core competencies

- Security, control and compliance concerns
- Resistance to IT change
- One size fits all approach

protiviti®

Top 5 Reasons For Moving To The Cloud

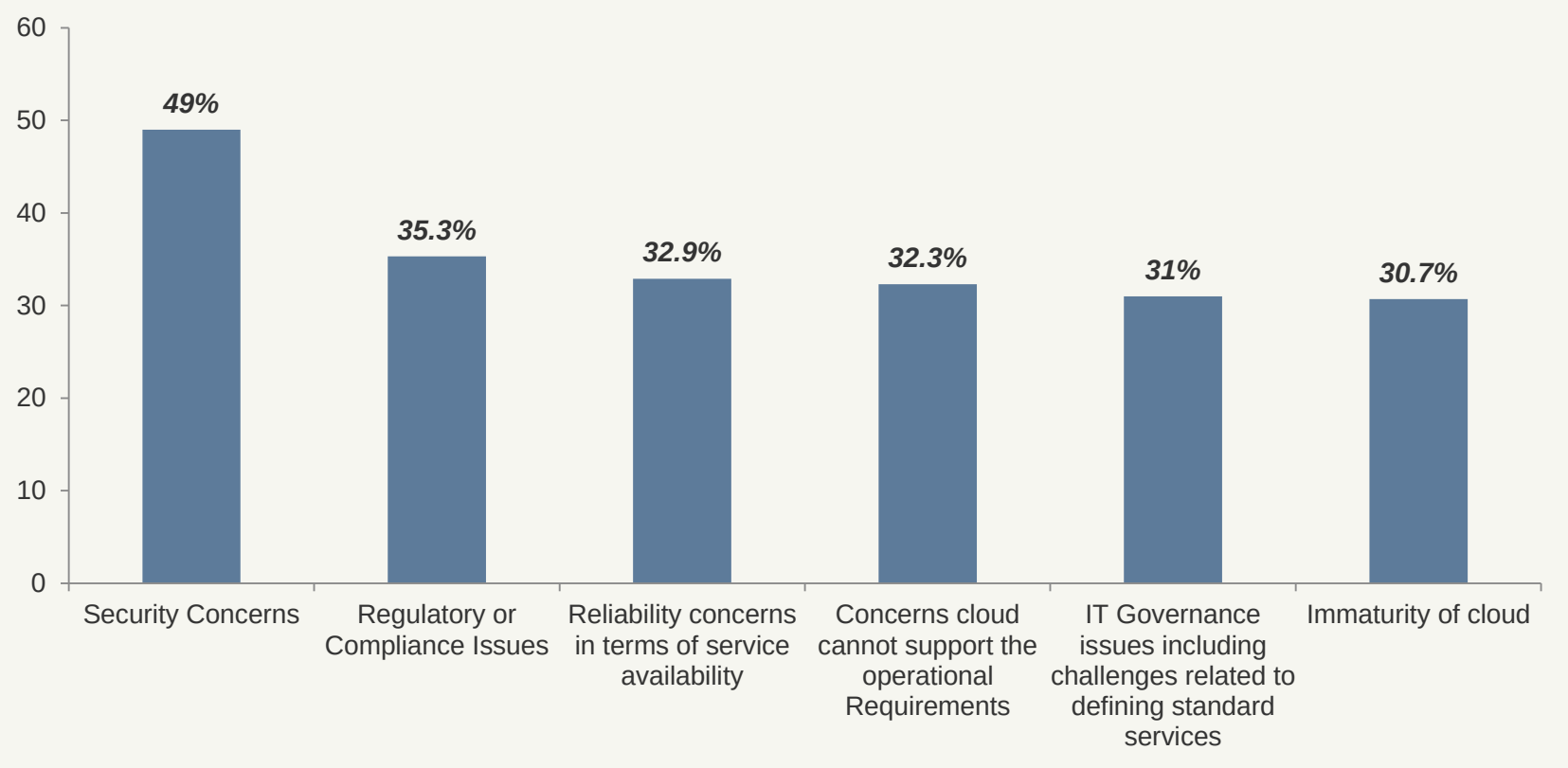


- *Percentage Respondents*
- *n = 1,109*
- *Source: IDC's CloudTrack Survey, October 2013*

protiviti®

Top 6 Inhibitors for Considering Public Cloud Services

Moving to cloud–based systems not only has many benefits but also is accompanied by some challenges that need to be addressed.



- ***Percentage Respondents***
- ***n = 1,109***
- ***Source: IDC's CloudTrack Survey, October 2013***

protiviti®

Multiple Models of Cloud Computing

Multiple Models of Cloud Computing

Cloud computing is a model for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. OR more simply,

"IT runs over the Internet instead of installing hardware and software yourself."

Characteristics

On demand self-service

Pay as you use

Rapid elasticity (expand / contract)

Multi tenancy (shared pool)

Broad network access

Service Models

Business Process as a Service
(emerging)
Entire business process as a service in the cloud

Software as a Service
Finished applications that you rent and customize

Platform as a Service
Developer platform that abstracts the infrastructure, OS, and middleware for developer productivity

Infrastructure as a Service
Deployment platform that abstracts the infrastructure

Deployment Models

Public Cloud

Community Cloud

Hybrid Cloud

Private Cloud

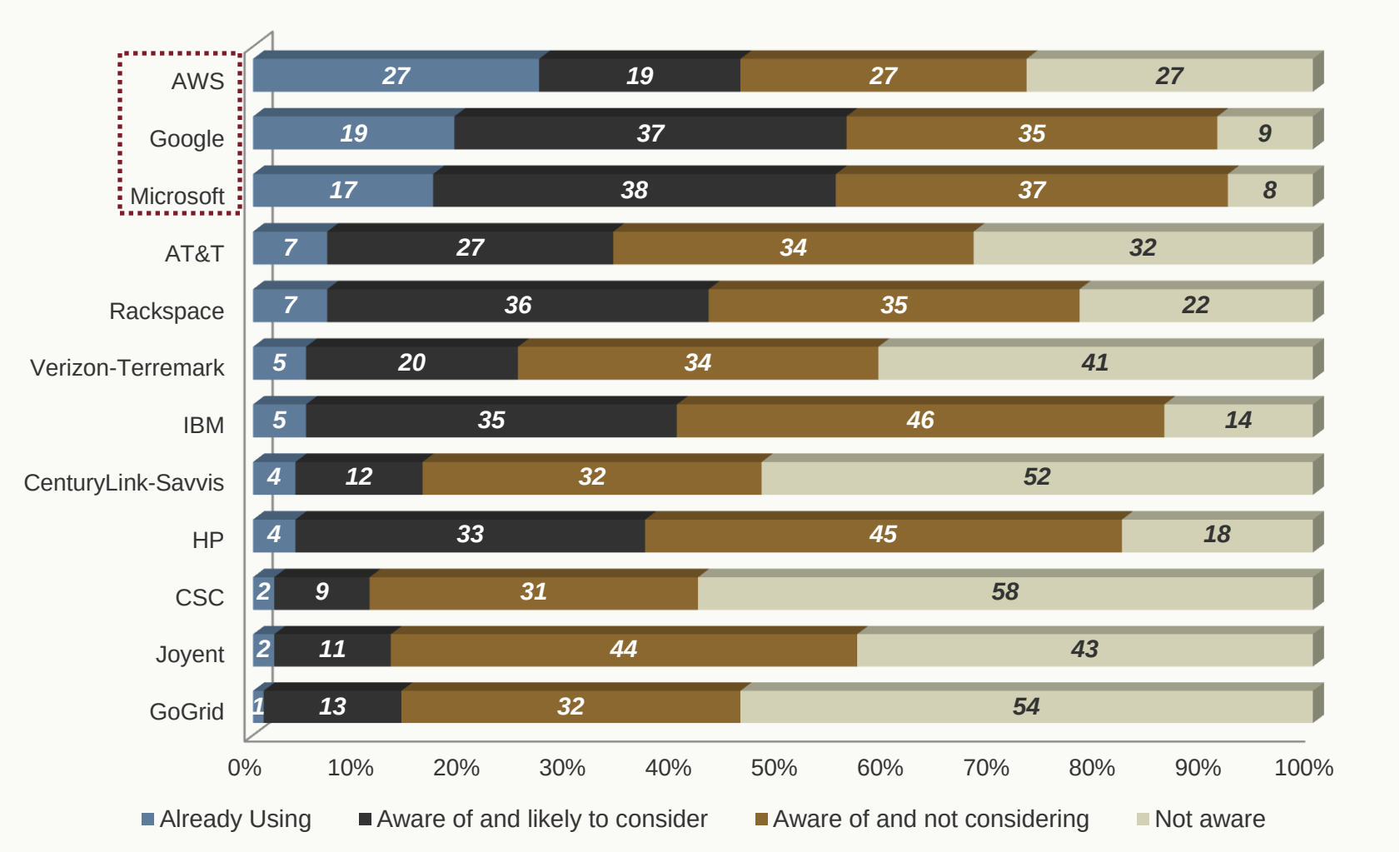
protiviti®

Cloud Computing Offerings

**** A sample list only. There are many more players.***

protiviti®

Public Cloud – Buyer Preference by Providers



- *Percentage Respondents*
- *n = 101*
- *Source: Everest Group, Enterprise Cloud Adoption Survey 2013*

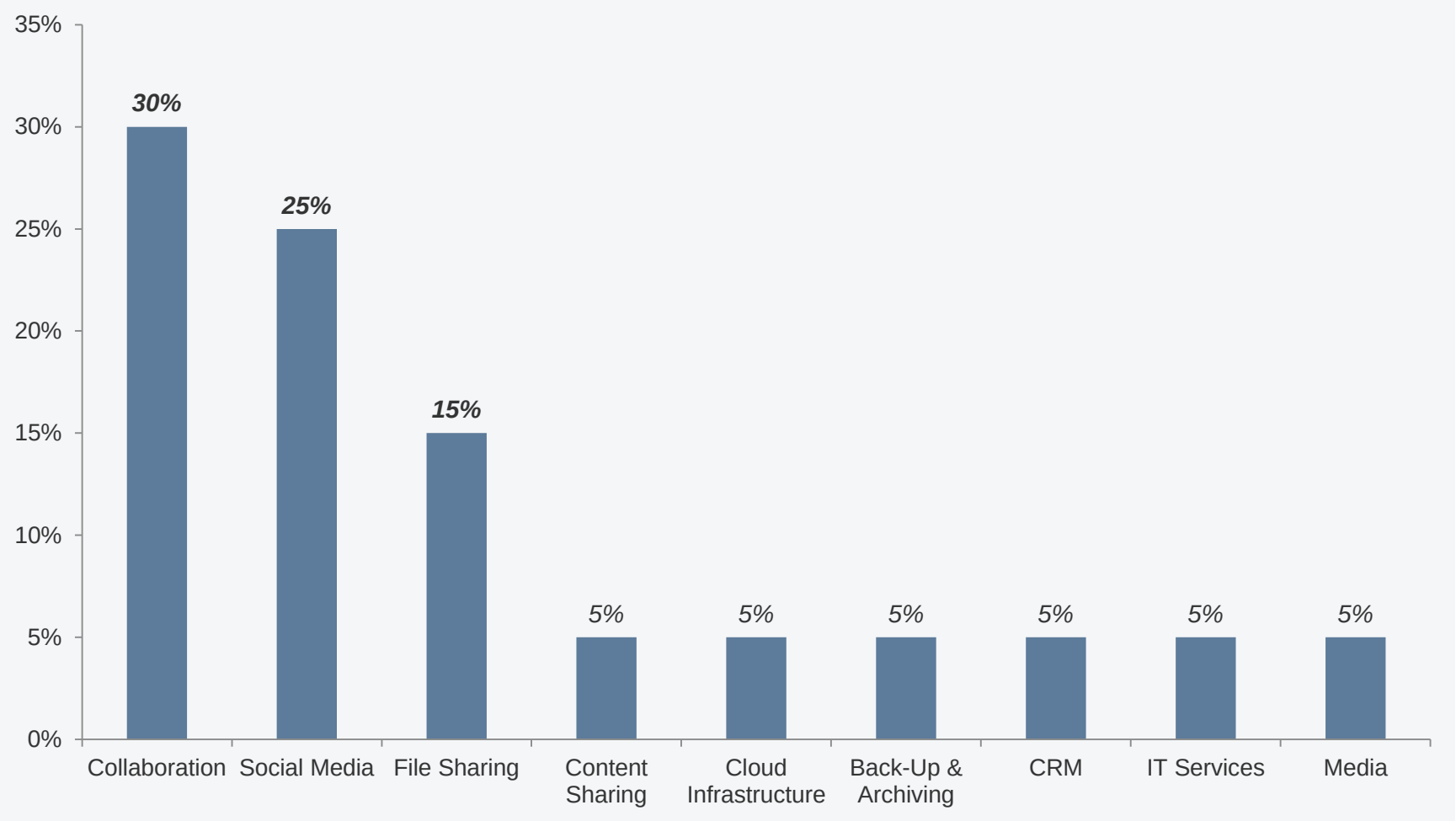
protiviti®

Cloud Usage – How Can It Help Businesses Operationally?

- Allowing High Variable Demand - Elastic nature of the infrastructure to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis
- Reaching Geographically Dispersed Users
- Consolidating Company IT
- Planning for Disaster Recovery
- Decoupling and separation of the business service from the infrastructure needed to run it (virtualization)
- Flexibility to choose multiple vendors that provide reliable and scalable business services, development environments, and infrastructure that can be leveraged out of the box and billed on a metered basis—with no long term contracts
- Cost allocation flexibility for customers wanting to move CapEx into OpEx
- Reduced costs due to operational efficiencies, and more rapid deployment of new business services
- Operational Expertise – Patch Management, Version Updates, Data Security Management

protiviti®

Cloud Usage – How The Cloud Is Being Utilized?



Source: Skyhigh Cloud Adoption Risk Report Q1 2014

protiviti®

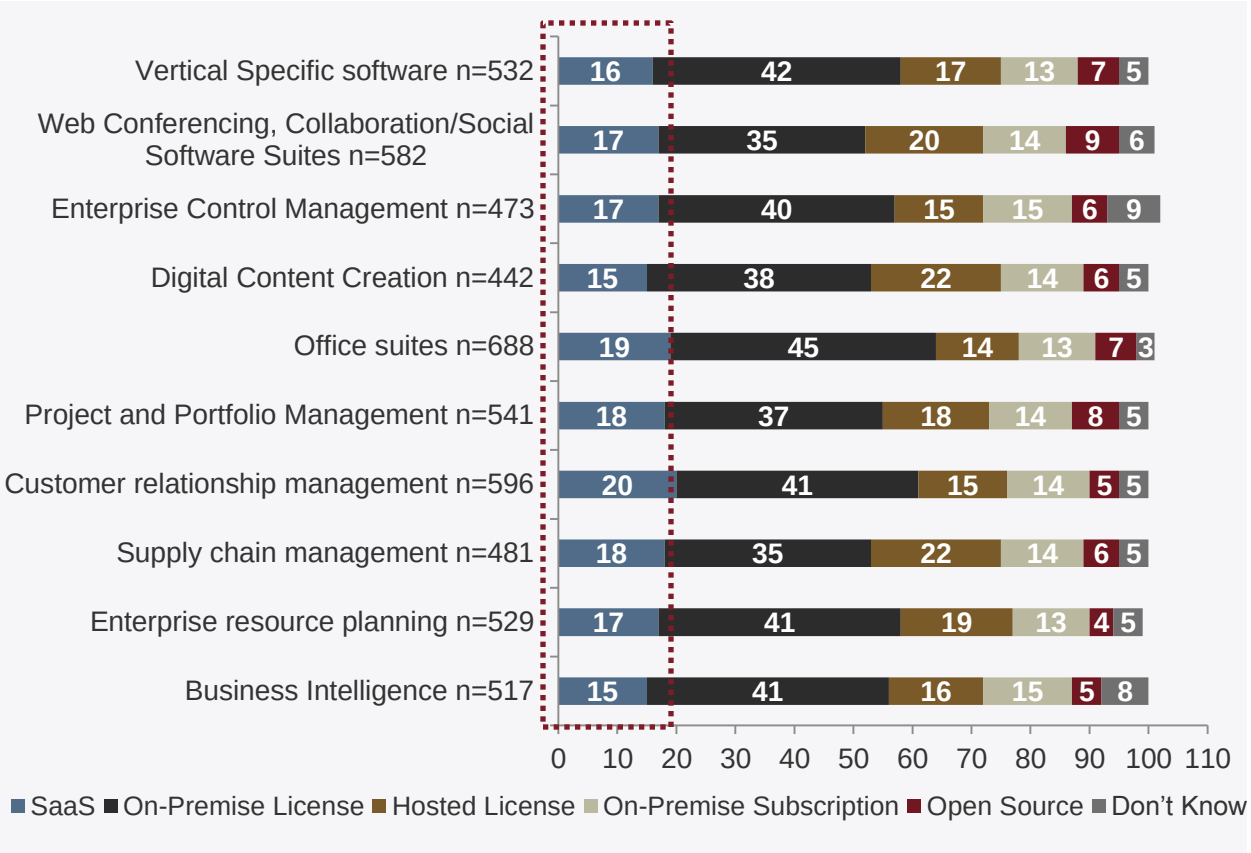
A Shift Toward Decentralized, Vertical, Subscription-Based Buying

The broader software implementation trends illustrate how enterprises are already changing their approach to purchasing applications and IT.

Question Asked: *What was the chosen approach for the implementation of those software applications?*

Base: *Respondents are piloting or have deployed the software application enterprise wide and/or in some business units. Percentages may not add up to 100% because of rounding.*

Approach to Software Implementation

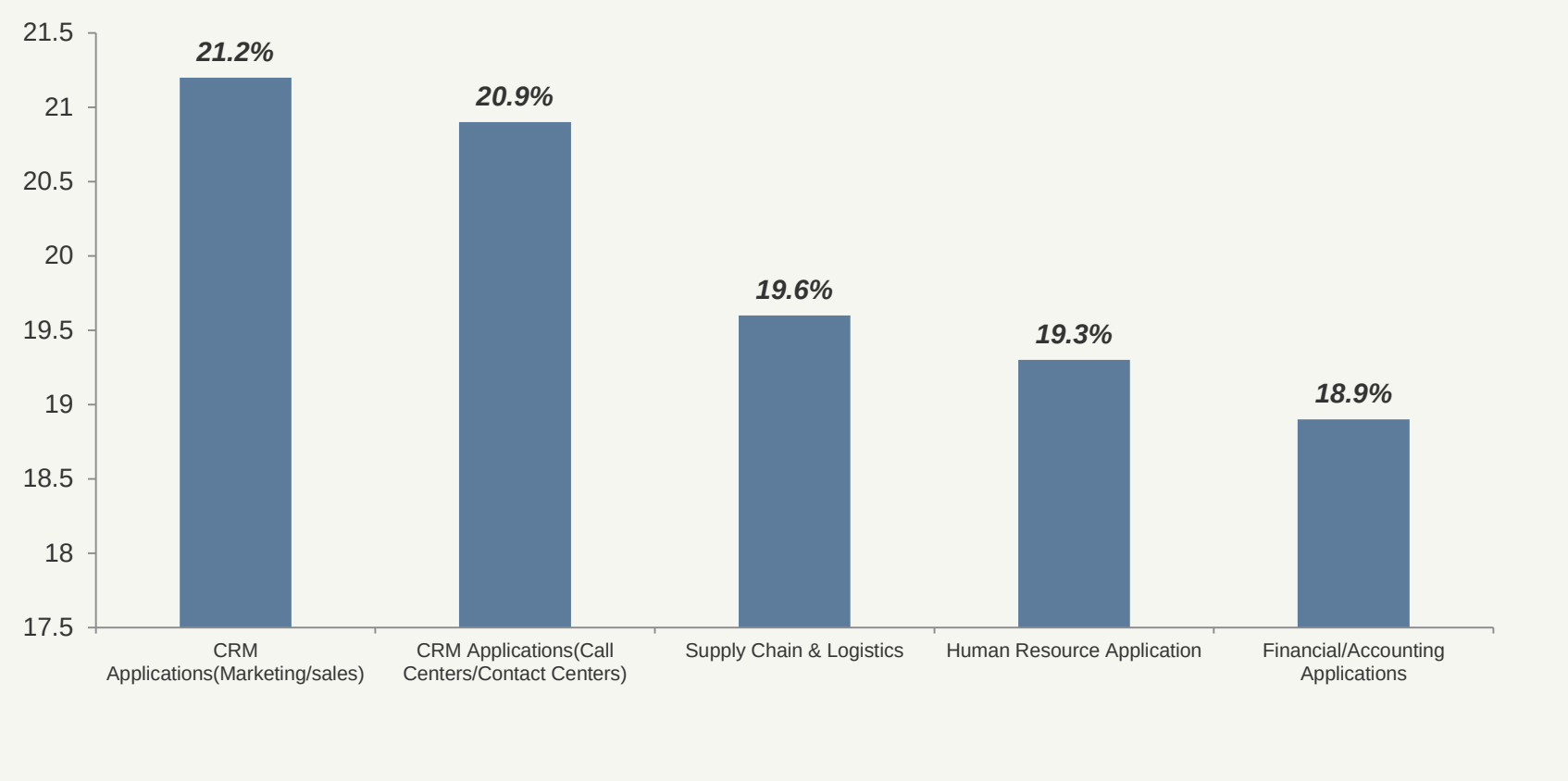


Source: Market Trends Application

protiviti®

Most Used Applications In The Public Cloud

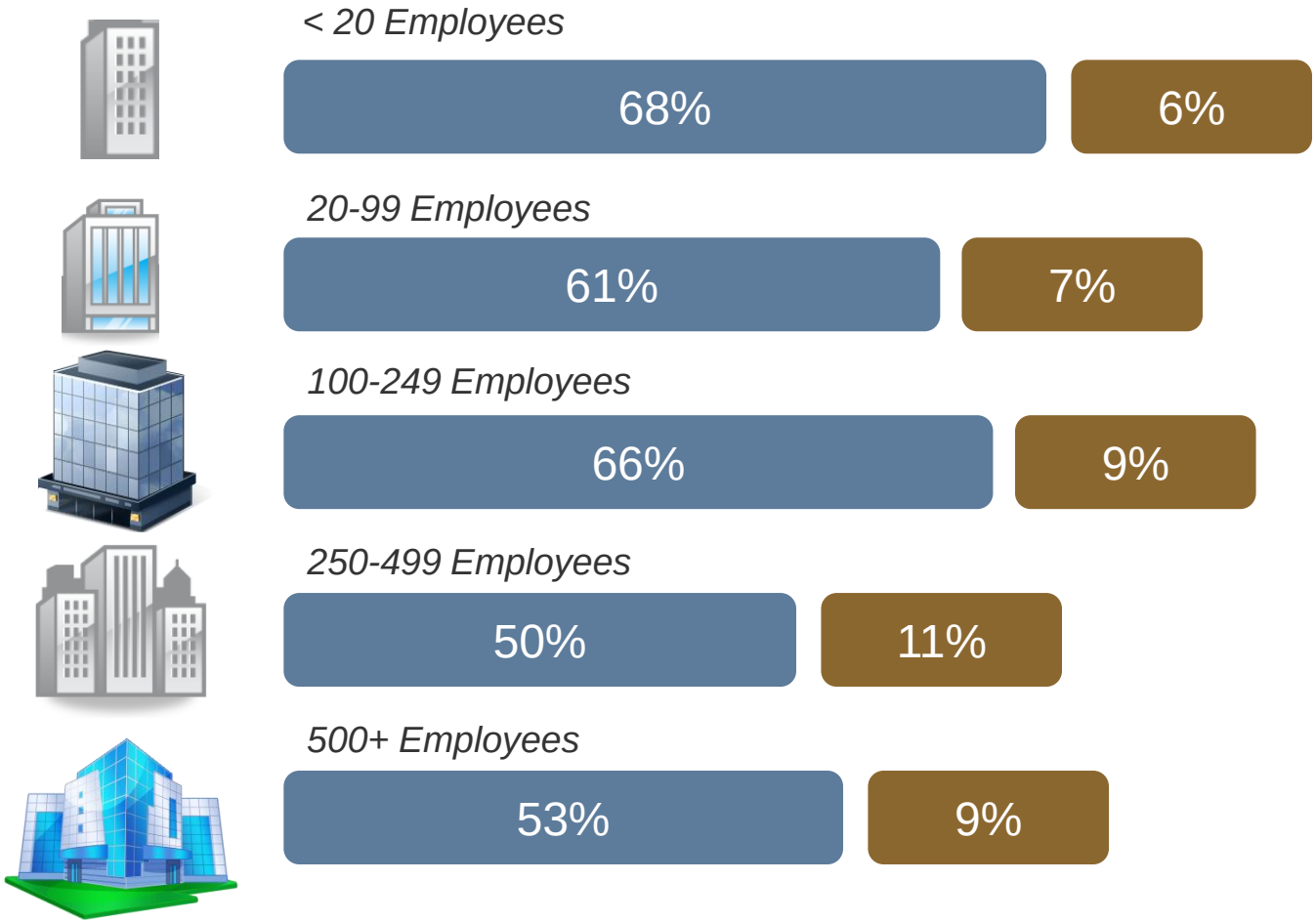
SaaS is a turnkey service, with application, presentation, and data tiers and all associated services in a single service that can be accessed and provisioned over the Internet .



- ***Percentage Respondents***
- ***n = 1,109***
- ***Source: IDC's CloudTrack Survey, October 2013***

protiviti®

Cloud Adoption by Company Size



Source: *Infographic: SMB Cloud Adoption Trends in 2014*

protiviti®

Cloud Maturity SMB vs Enterprise

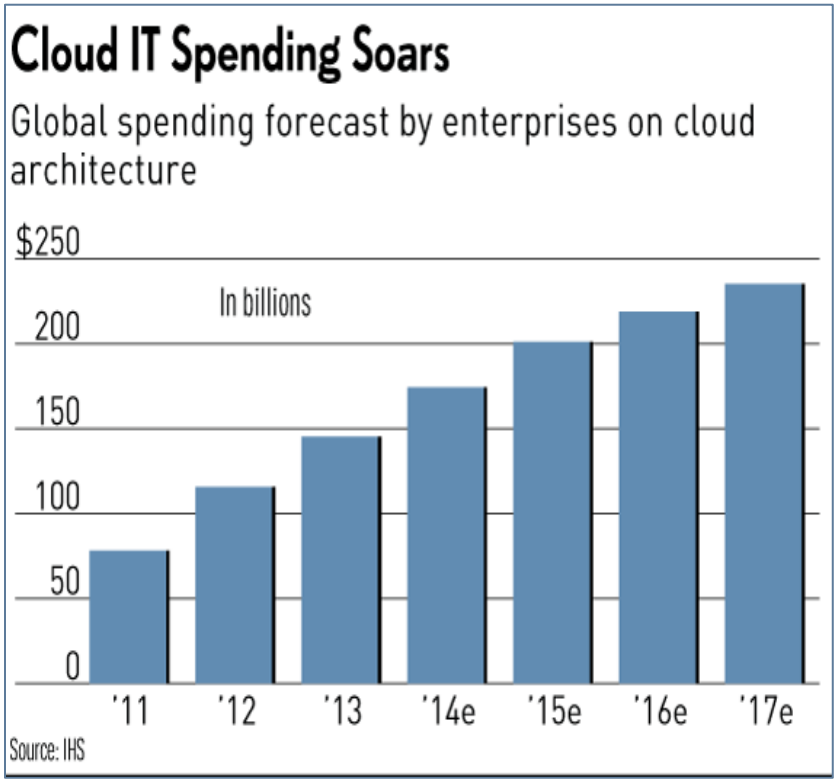
SMB		Enterprise
20%	***Developing a cloud strategy***	16%
29%	***Working on first cloud project***	35%
25%	***Multiple projects & developing apps in the cloud***	31%
26%	***Heavily using cloud infrastructure***	18%

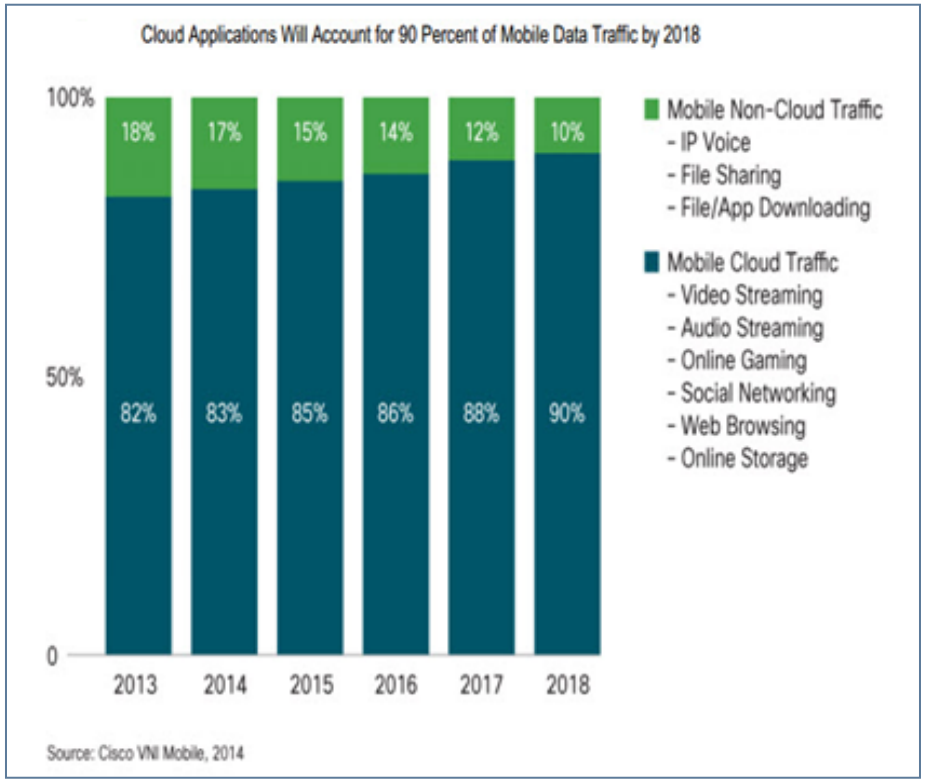
Source: *Infographic: SMB Cloud Adoption Trends in 2014*

protiviti®

Market Forecast

Cloud Services Market Outlook





Source: *Investors' Business Daily*

protiviti®

Cloud Services Market Outlook

Cloud service revenue is expected to be USD 220bn by 2015, and USD 480bn by 2019

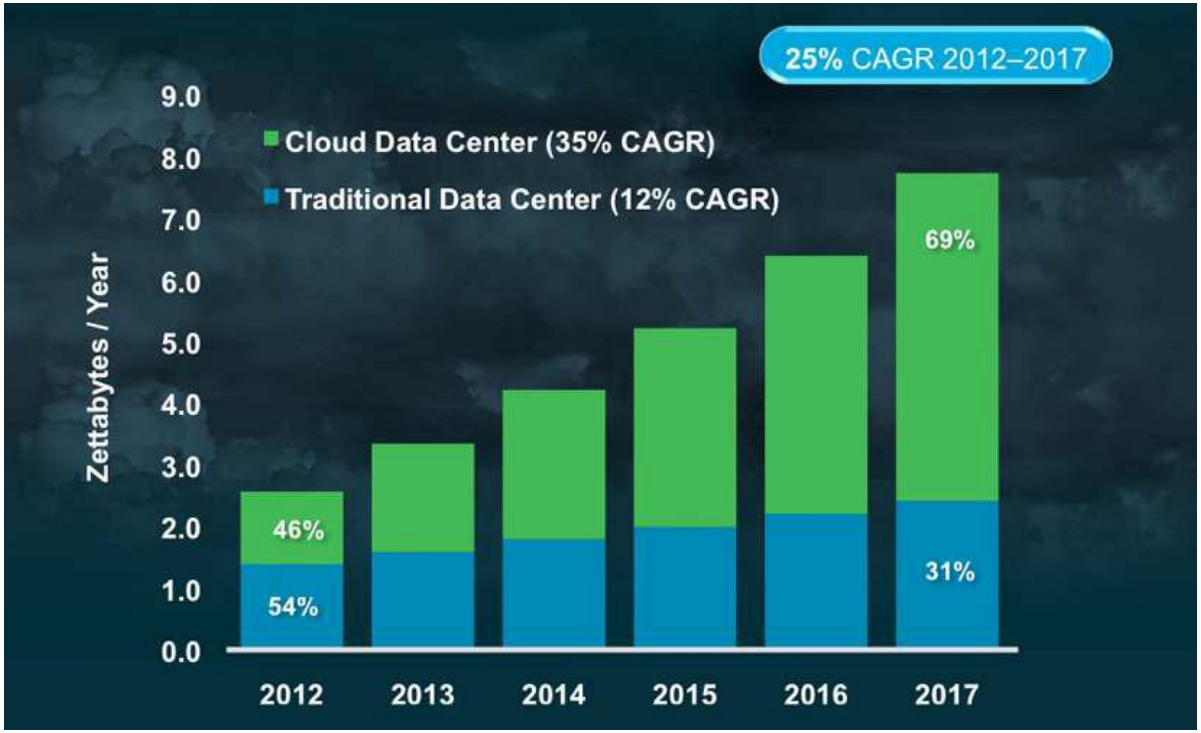
Business processes (cloud-based advertising, e-commerce, human resources, payment processing and other business processes) cloud services market is expected to be USD 370bn by 2019

Data from Intuit and Emergent Research reveals that by 2020, 78 percent of small businesses will be “fully adapted” to cloud computing. That’s more than double the current 37 percent adoption rate as of 2014.

Source: Research Pedia; Small Business Trends

protiviti®

Cloud Services Market Outlook



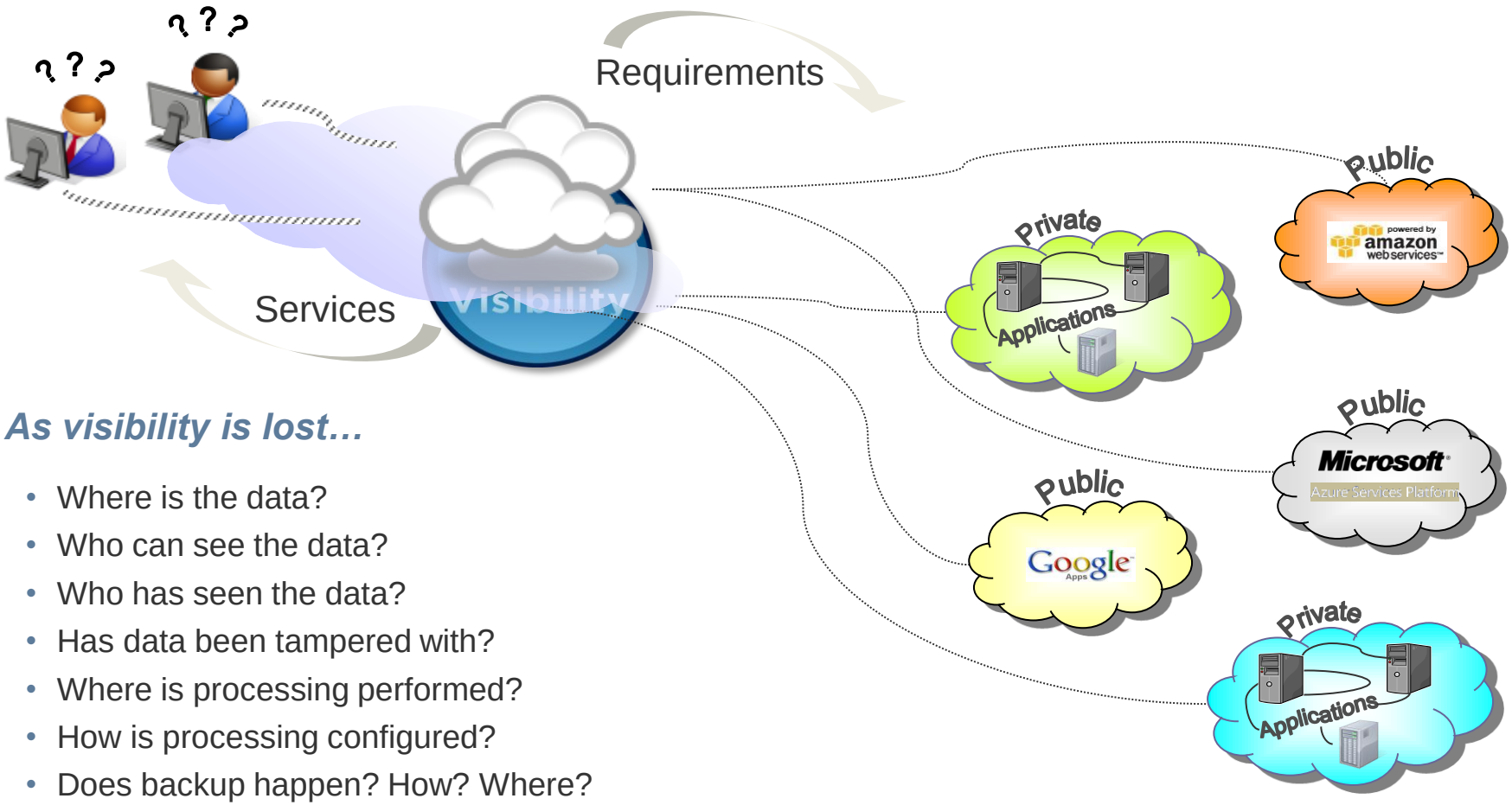
Cisco predicts Cloud Data Center traffic to grow at 35% CAGR. By 2017, over two-thirds of all data center traffic is expected to be based in the cloud.

Source: *http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf*

protiviti®

Risks

Clouds Are Cloudy



As visibility is lost…

- Where is the data?
- Who can see the data?
- Who has seen the data?
- Has data been tampered with?
- Where is processing performed?
- How is processing configured?
- Does backup happen? How? Where?

… security, compliance, and value are lost as well.

protiviti®

Top Risks

- Loss of Governance
- Lock-In
- Management Interface Compromise
- Incomplete or Insecure Data Deletion
- Data Protection
- Malicious Insider / Investigative Support
- Isolation Failure
- Compliance Risks

protiviti®

Categories of Control Objectives

- Compliance
- Data Governance
- Facility Security
- Human Resources
- Information Security
- Legal
- Operations Management
- Risk Management
- Release Management
- Resiliency

protiviti®

Control Objectives

Compliance	Independent Regulatory Audits
	Vendor Management
	Information System Regulatory Mapping
	Intellectual Property
Data Governance	Classification
	Handling / Labeling / Security Policy
	Retention Policy
	Risk Assessments
Facility	Policy
	User Access
	Asset Management
Human Resources	Background Screening
	Employment Agreements
	Employment Termination

protiviti®

Control Objectives

Information Security	Management Program
	Policy, Reviews, Enforcement
	User Access Restriction / Authorization / Reviews
	Awareness Training
	Roles / Responsibilities
	Management Oversight
	User Access Policy
	Workspace Cleanliness
	Anti-Virus / Malicious Software
	Incident Management – Identification, Reporting and Monitoring
	Incident Response Legal Preparation

protiviti®

Control Objectives

Legal	Non-Disclosure Agreements
	Third Party Agreements
	Service Level Agreements
Operations Management	Capacity / Resource Planning
Risk Management	Program
	Assessments
	Mitigation / Acceptance
	Business / Policy Change Impacts
	Third Party Access
Release Management	Production Changes
	Outsourced Development
Resiliency	Management Program
	Impact Analysis
	Business Continuity Planning
	Business Continuity Testing

protiviti®

Cloud Computing Audit Approach

Involvement of Internal Audit in Cloud Computing

Vendor Selection & Contract Negotiation

- Validation of business case
- Right to Audit Clause and/or SSAE16
- Compliance Scope
- Impact of Regulations on Data Security
- Stability of Partners and Services Providers
- Contractual Data Protection Responsibilities and Related Clauses
- Impact of Regulations on Provider Infrastructure
- Prepare Evidence of How Each Requirement Is Being Met

Pre-Implementation Review

- Project management - roles and responsibilities
- Data migration strategy
- Inherent and residual risk assessment

Post-Implementation Review

- Accuracy of data
- Policies and procedures pertaining to data security, privacy of data
- Regulatory changes - HIPAA, PCI, etc.

protiviti®

Audit/Projects Around Cloud Computing

- Cloud computing platform evaluation / due diligence
- Data migration review to the new platform
- Management of the cloud computing function
- Security reviews
  - Security of data
  - Network accessibility
  - User administration
- Regular review of SOC Type 1/provider sponsored audit reports
- Cost/Savings impact
- Realignment of controls for regulatory reporting
- SLA/KPI review to ensure the provider is living up to their end of the bargain
- Impacts to Disaster Recovery/Business Continuity

protiviti®

Scoping

Define the audit objectives and scope. Understand the core business process and its alignment with IT, in its non-cloud form and current or future cloud implementation.

- Obtain a description of all cloud computing environments in use and under consideration.
- Obtain a description of all cloud computing applications in use and under consideration.
- Identify the types of cloud services (IaaS, PaaS, SaaS) in use and under consideration, and determine the services and business solutions to be included in the review.
- Obtain and review any previous audit reports with remediation plans. Identify open issues, and assess updates to the documents with respect to these issues.

Since the areas under review rely heavily on the effectiveness of core IT general controls, it is recommended that audit/assurance reviews of the following areas be performed prior to the execution of the cloud computing review, so that appropriate reliance can be placed on these assessments:

- Identity management (if the organization's identity management system is integrated with the cloud computing system)
- Security incident management (to interface with and manage cloud computing incidents)
- Network perimeter security (as an access point to the Internet)
- Systems development (in which the cloud is part of the application infrastructure)
- Project management
- IT risk management
- Data management (for data transmitted and stored on cloud systems)
- Vulnerability management

Audit Approach

The ISACA approach breaks down an audit into two categories

- Governing the Cloud
- Operating in the Cloud

Each area has Control Objectives that are subsequently reviewed.

Audit Approach

Governing the Cloud includes the following processes. The controls associated with these processes are then evaluated.

Governance

- Audit/Assurance Objective: 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.

Enterprise Risk Management

- Audit/Assurance Objective: 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.

Information Risk Management

- Audit/Assurance Objective: 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.

protiviti®

Audit Approach

Governing the Cloud includes the following processes.

Third-party Management

- Audit/Assurance Objective: 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.

Contractual Obligations

- Audit/Assurance Objective: 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 Compliance

- Audit/Assurance Objective: Legal issues relating to functional, jurisdictional and contractual requirements are addressed to protect both parties, and these issues are documented, approved and monitored.

Right to Audit

- Audit/Assurance Objective: 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.

protiviti®

Audit Approach

Governing the Cloud includes the following processes.

Auditability

- Audit/Assurance Objective: 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.

Compliance Scope

- Audit/Assurance Objective: The use of cloud computing does not invalidate or violate any customer compliance agreement.

ISO 27001 Certification

- Audit/Assurance Objective: Service provider security assurance is provided through ISO27001 Certification.

Service Transition Planning

- Audit/Assurance Objective: 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.

protiviti®

Audit Approach

Operating in the Cloud includes the following processes. The controls associated with these processes are then evaluated.

Incident Response, Notification and Remediation

- Audit/Assurance Objective: Incident notifications, responses, and remediation are documented, timely, address the risk of the incident, escalated as necessary and are formally closed.

Application Security Architecture

- Audit/Assurance Objective: 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.

Compliance

- Audit/Assurance Objective: Compliance requirements are an integral component of the design and implementation of the application security architecture.

protiviti®

Audit Approach

Operating in the Cloud includes the following processes.

Tools and Services

- Audit/Assurance Objective: Use of development tools, application management libraries and other software are evaluated to ensure their use will not negatively impact the security of applications.

Application Functionality

- Audit/Assurance Objective: For SaaS implementations, the application outsourced to the cloud contains the appropriate functionality and processing controls required by the customer's control policies within the processing scope (financial, operational, etc.).

Encryption

- Audit/Assurance Objective: Data are securely transmitted and maintained to prevent unauthorized access and modification.

protiviti®

Audit Approach

Operating in the Cloud includes the following processes.

Key Management

- Audit/Assurance Objective: Encryption keys are securely protected against unauthorized access, separation of duties exists between the key managers and the hosting organization, and the keys are recoverable.

Identity and Access Management

- Audit/Assurance Objective: 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.

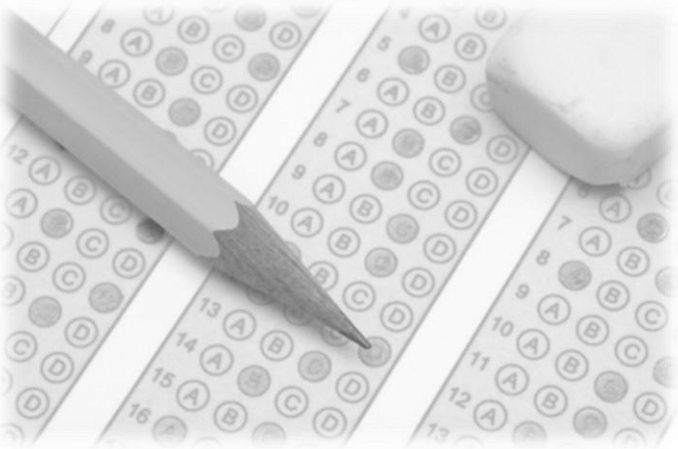
Virtualization

- Audit/Assurance Objective: Virtualization operating systems are hardened to prevent cross-contamination with other customer environments.

protiviti®

At A Minimum: Execute A Cloud Service Provider Questionnaire

- ***Ask the basic questions…***
  - Where do you store our data?
  - Who can access and retrieve the data?
  - Do you have auditing enabled? Is it available to us?
  - How do you determine if our data has been tampered with?
  - What are your configuration standards?
  - Does backup happen? How? Where?
  - Have you attained any external/independent security certifications?
- ***Follow-up with a detailed information security questionnaire***



protiviti®

Ensure Basic Mitigation Techniques Are In Place

Intellectual Property Loss

- Monitoring controls
- Encryption design and requirements
- Data backup management

Compliance Reporting

- Specify a breach notification process
- Ask for independent reviews and certifications
- Use your own “Golden Rule” – Treat my data like I treat my own

Security Administration

- Analyze the cloud service provider (CSP) security model
- Ensure strong authentication and access controls
- Require the CSP to be completely transparent

protiviti®

Q & A

Thank You

Cal Slemp
Managing Director
New York, NY
+1.203.905.2926
cal.slemp@protiviti.com

protiviti®

Powerful Insights.
Proven Delivery.®