Cloud Computing Overview

Benefits, Risks and Challenges

Agenda

- IT Challenges & Business Implications
- Cloud Definitions and Benefits
- Adoption Models
- Cloud Challenges
- Auditing the Cloud

IT Challenges & Business Implications

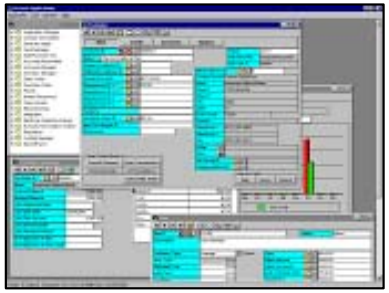
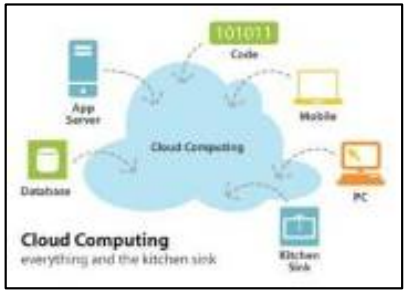
IT Challenges & Business Implications

IT organizations struggle to meet the exponential growth in applications and data with resources still characterized by infrastructure and organizational silos.

As a result, companies today are faced with a number of challenges, including:

Operational Challenges	Business Implications
Inability to provision services seamlessly across infrastructure domains (e.g. Network/Security, Servers, Storage)	• IT cannot keep up with business and application demands • Administration inefficiencies • Misalignment resulting in errors
Insufficient flexibility to keep pace with dynamic business requirements	• Inability to meet service levels • Inefficient, cost over provisioning • Limited business agility
Proliferation and low utilization of resource (e.g. servers, storage)	• High TCO • Power inefficiencies • High facilities (space) cost
Expense of traditional disaster recovery	• Inability to cost-effectively meet application recovery time / point objective (RTO/RPO) requirements

Evolving toward the cloud

	1960s Centralized computing	1980s Client-server computing	1990s Internet applications	2000s Cloud computing
				
Client	▸ Minimal processing power, display only	▸ Strong client processing ▸ Some data stored/processed on client	▸ Strong client, but not used for processing ▸ Unstructured data (photos, documents) stored on client	▸ Minimal processing power needed (smartphones, etc)
Server	▸ Strong central processing ▸ Data stored centrally	▸ Some data stored / processed on client	▸ Processing done centrally	▸ Processing and data storage takes place centrally

The cloud presents enormous opportunities & challenges to a company's IT investment.

Situation

- Internal and external customers are demanding better, faster, more scalable solutions that can be quickly customized and deployed to meet their unique needs.
- Cloud computing has shifted companies' continued investment in their own infrastructure to sourcing IT services externally.

Root Cause

- Legacy systems often cannot be integrated with new technologies; sometimes require total transformation.
- Skills set of the organization changes from "keeping the lights on" to managing SLAs and third party contracts.
- Speed to market and advanced functionality often trumps security, which presents risk to the organization

Complications

- The journey to the cloud can be difficult and can put the organization at risk if not planned correctly.
- Once adoption reaches a certain point within an organization, the CIO must fundamentally change the way she/he manages and governs the IT organization.
- Designing and implementing scalable and secure solutions in a vendor environment is complicated.

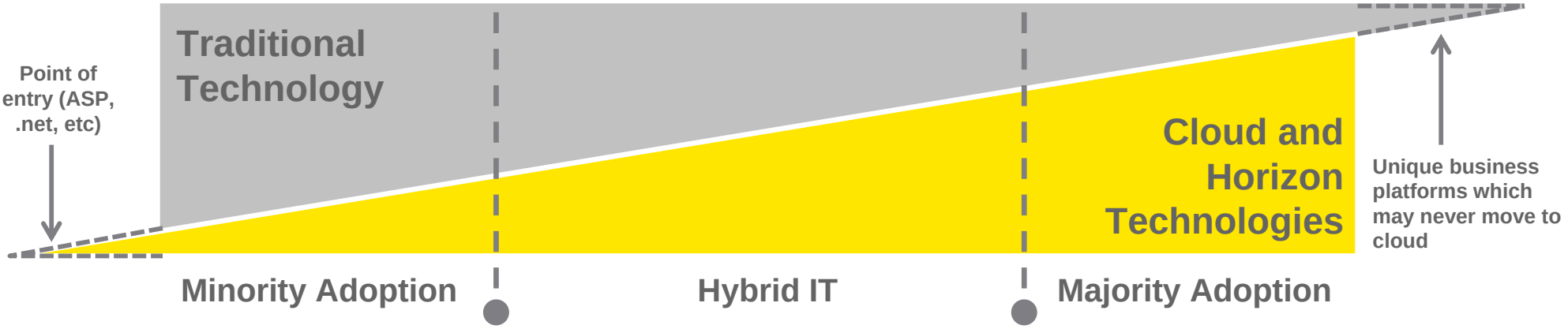
Problem

How can companies design tactical and implementable solutions that meet the ever-changing business needs on their journey into the cloud?

Solutions

- Cloud will allow you to adopt innovative new technologies while increasing transparency of IT spend and delivery to the business, while still addressing the fundament requirements around a stable, secure and audit ready environment.
- IT will be able to implement comprehensive solutions to address challenges faced through the journey to the cloud.

IT organizations are fundamentally changing from “operators” to “managers”.



- Cloud has not begun to dominate the IT budget and funding model of service delivery
- Data centers and operations remain focused on delivering traditional IT
- Systems of record and other major business specific processes have not even been considered as a candidate for cloud
- Skills for cloud based services are just starting to be realized and grown
- Commoditized applications are being reviewed for candidacy to migrate to the cloud

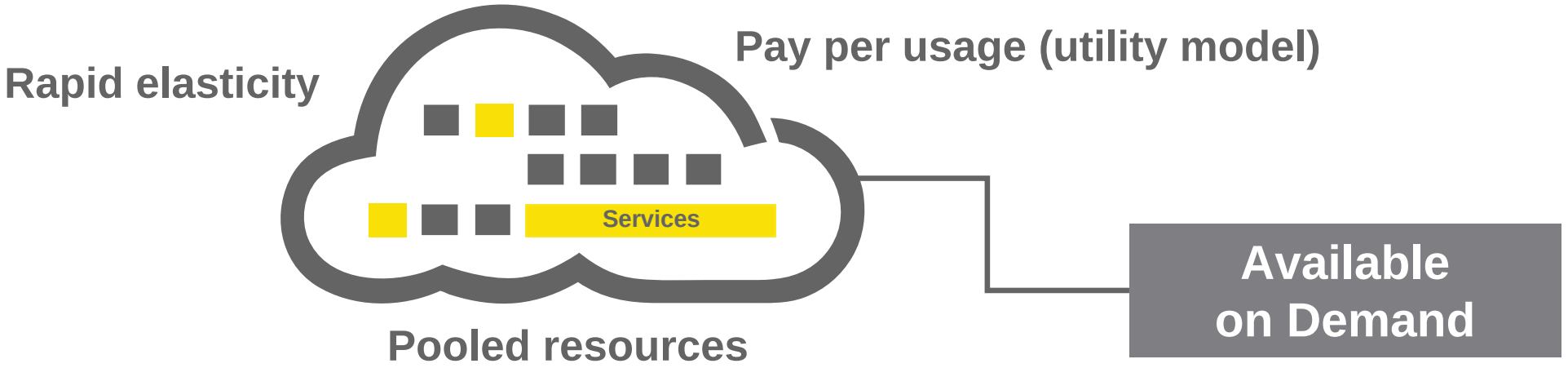
- A comprehensive Hybrid IT environment will become prevalent
- Two dominate funding models will be in place: “Capital expenditures” and “Transactions/As-a-service consumption”
- Integration challenges arise when integrating multiple SaaS solutions (including identity and access management)
- Vendor management and SLAs will be re-evaluated based on new and smaller vendors as well as different solutions being provided by the same vendor
- New skills will be needed to grow and manage cloud computing topology

- Cloud will dominate IT budget and funding model will be primarily “Transactions/As-a-service consumption”
- Data centers are repurposed at gateways to As-a-Service providers
- Systems of record begin the transition to Cloud / As-a-Service solutions in large, multi-national companies
- IT organization has been restructured as a service provider to the business units
- CIO focuses on contract management and SLA enforcement rather than managing own infrastructure

Cloud Definitions and Benefits

What is cloud computing?

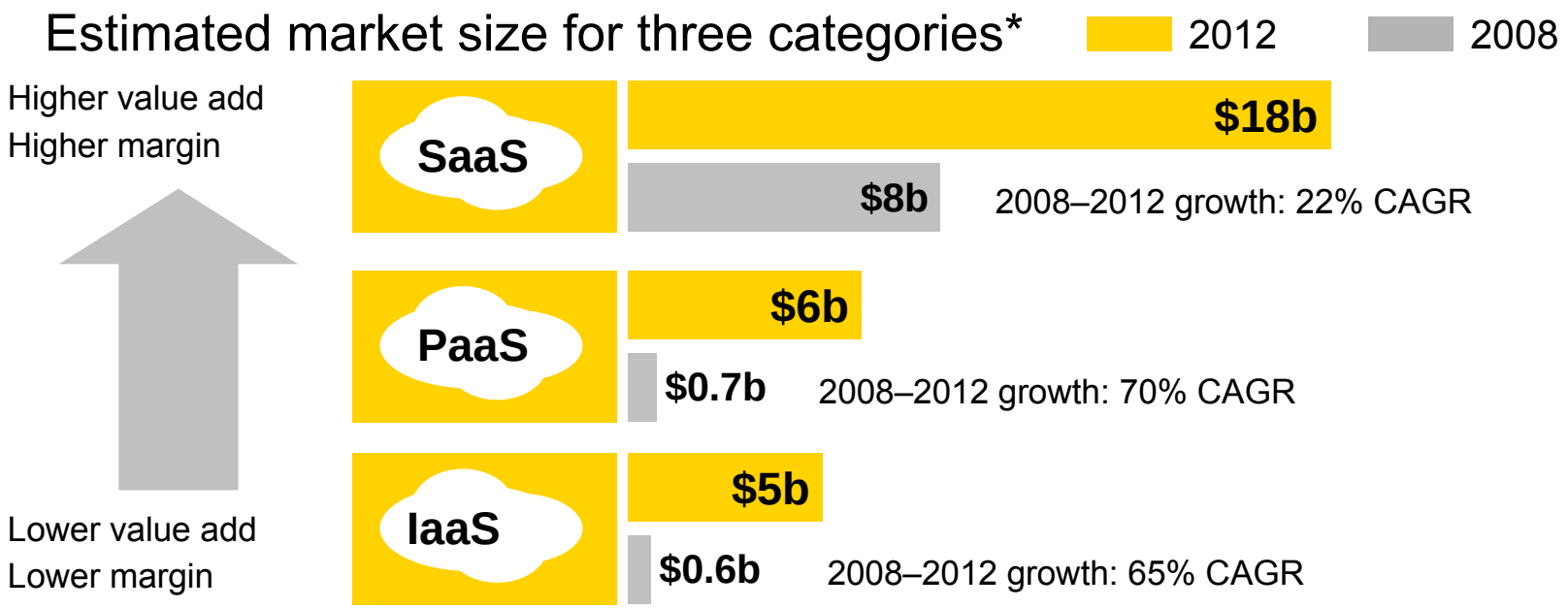
Cloud computing is a new paradigm where resources are available on-demand and on a pay-per-use basis to enterprises and users.



- Cloud computing uses the internet to access someone else's software running on someone else's hardware in someone else's data center.
- Industry swings between centralized computing models (mainframe of 1960s) to host-centric ones ("client-server" technology of 1980s). Cloud computing is a logical extension of the dot-com era web app - further enabled by advances in bandwidth, datacenter architecture, and large-scale storage.
- There are five defining characteristics of cloud computing: **on-demand, broadly accessible, pooled, elastic, and metered**.

Simply put…..computing over the internet

It’s more than just a buzzword

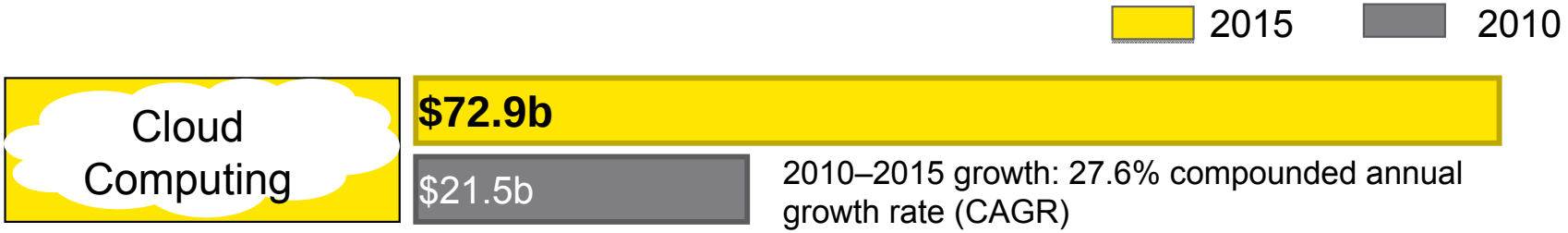


*Note: These are rough estimates. Total market size discrepancies are also due to rounding off.

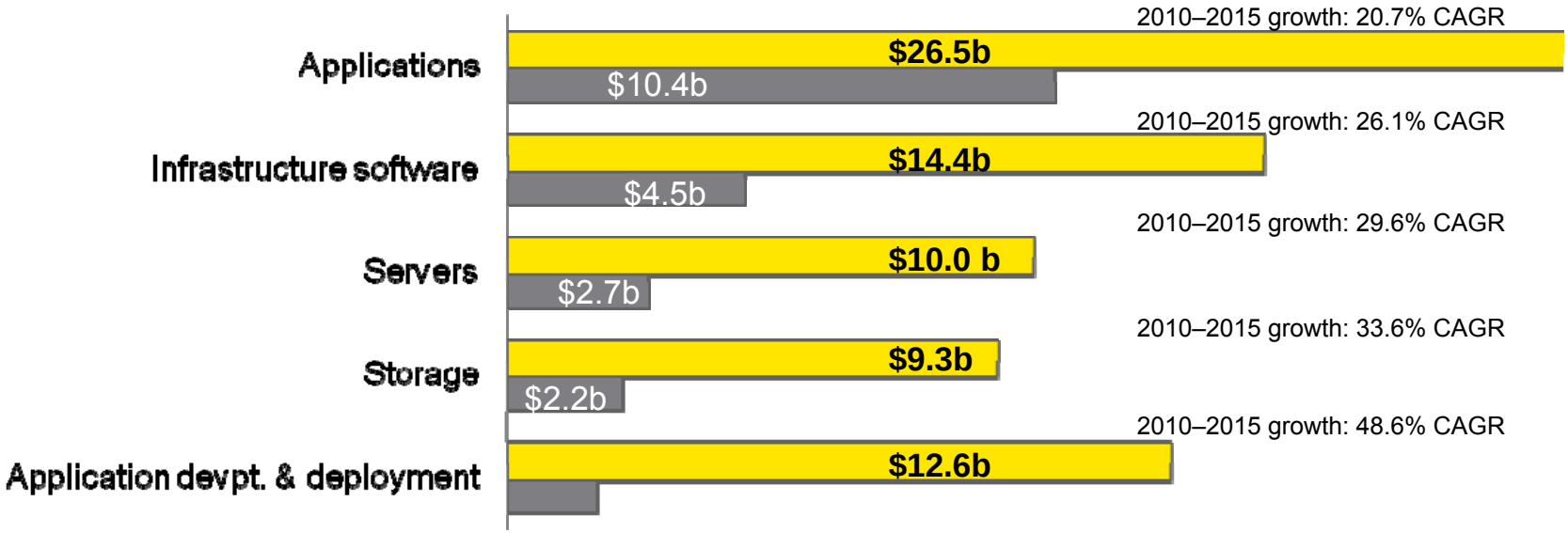
Sources: AMR, Gartner, International Data Corporation, William Blair & Company, LLC, June 2010.

What the analysts are saying

IDC's estimated market size for overall cloud computing market



IDC's estimated IT cloud services revenue by product/service type



Cloud installation – rewards

- Why Cloud ?
  - **Ease of deployment**
  - Broad network access
  - Elastic scalability
  - Efficient resource sharing
  - Measured services
  - Lowers cost

- On-demand self service
- No cabling or hardware
- Deploy infrastructure with software

Cloud installation – rewards

- Why Cloud ?
  - Ease of deployment
  - **Broad network access**
  - Elastic scalability
  - Efficient resource sharing
  - Measured services
  - Lowers cost

- Capabilities available over Internet
- Can be accessed through PDAs, Laptops, mobile phones

Cloud installation – rewards

- Why Cloud ?
  - Ease of deployment
  - Broad network access
  - **Elastic scalability**
  - Efficient resource sharing
  - Measured services
  - Lowers cost

- Add or remove computing capacity instantly
- Control infrastructure as per application demands
- Flexible with variable workload

Cloud installation – rewards

- Why Cloud ?
  - Ease of deployment
  - Broad network access
  - Elastic scalability
  - **Efficient resource sharing**
  - Measured services
  - Lowers cost

- Serve multiple consumers
- Sense of location independence
- Resources include memory, bandwidth, virtual machines, etc.

Cloud installation – rewards

- Why Cloud ?
  - Ease of deployment
  - Broad network access
  - Elastic scalability
  - Efficient resource sharing
  - **Measured services**
  - Lowers cost

- Metering capability
- Resource usage can be monitored and controlled
- Provides transparency to provider and consumer

Cloud installation – rewards

- Why Cloud ?
  - Ease of deployment
  - Broad network access
  - Elastic scalability
  - Efficient resource sharing
  - Measured services
  - **Lowers cost**
    - Pay as per usage
    - Avoids maintenance cost for servers
    - No contracts or buying servers

Cloud Computing Overview
Definition & Key Characteristics

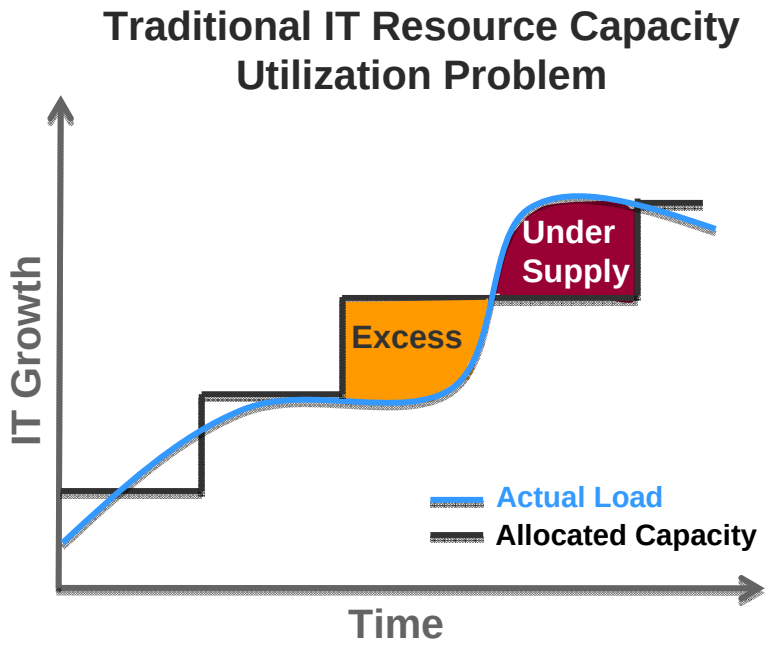
"Cloud computing is a **pay-per-use** model for enabling available, convenient, **on-demand** network access to a shared pool of configurable computing resources that can be **rapidly provisioned** and released with minimal management effort or service provider interaction"

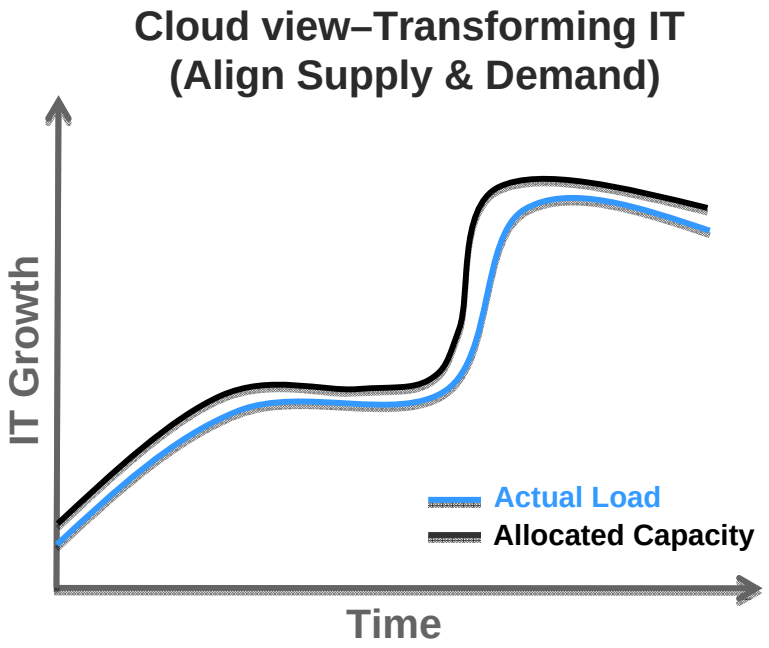
National Institute of Standards and Technology (NIST)

Characteristics of the cloud

Essential characteristics and business benefits		Traditional IT-Outsourcing	Cloud Computing
On-demand self-service	► Consumer provisions computing capabilities as needed ► automatically without human interaction of service provider	✘ (usually multi-year contract)	✓
Broad network access	► Available over the network ► Access mechanisms promote use by heterogeneous client platforms (e.g., mobile phones, laptops, and PDAs).	partly	✓
Resource pooling	► Provider's computing resources are pooled to serve multiple consumers ► Multi-tenant model ► Physical and virtual resources are dynamically assigned and reassigned according to consumer demand ► Customer generally has no control or knowledge over the exact location of the provided resources	✘ (dedicated servers)	✓
Rapid elasticity	► Rapidly and elastic provisioning ► Quickly scale out and quickly scale in ► Capabilities appear to be unlimited to the consumer and can be purchased in any quantity at any time	partly	✓
Measured Service	► Metering capability at some level of abstraction appropriate to the type of service ► Usage can be monitored, controlled, and reported ► Transparency for both the provider and consumer of the utilized service.	partly (but usually fixed and flat-fee contracts)	✓

Align Supply and Demand





Adoption Model

Cloud Computing Overview

The Cloud Services Delivery Model

Software as Service (SaaS)

- Applications that are enabled for the Cloud
- Support of an architecture that can run multiple instances
- Stateless application architecture

Platform-as-Service (PaaS)

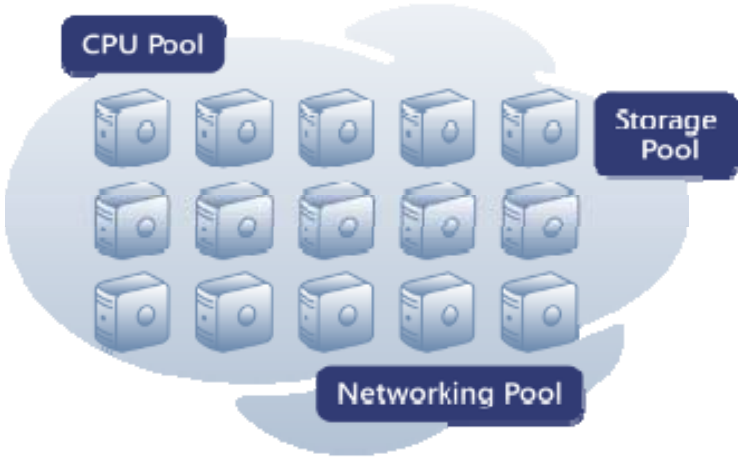
- A platform that enables developers to write applications that run on the Cloud
- A platform would usually have several application services available for quick deployment

Infrastructure-as-Service (IaaS)

- A highly scaled redundant and shared computing infrastructure accessible using Internet technologies
- Consists of servers, storage, security, databases, etc.

Cloud Computing Overview
Defining IaaS

- The Cloud offers scalable **hardware resources** (e.g., CPU cycles, storage, networking, etc.) as a service
- Customers don't need to own or manage hardware or data center facilities
- Applications are built natively in the Cloud to leverage this infrastructure, **or** existing Windows/Linux workloads are hosted as virtual machines in the Cloud
- Enterprises can run their apps on this Cloud infrastructure, paying-as-they-go for raw server resources (e.g., CPU cycles, storage MBs, bandwidth, etc.) they consume
- On-premise workloads can tap into the Cloud for additional serving capacity on demand (**augmenting on-premise infrastructure**). Enterprise workloads can be hosted entirely in the Cloud (**replacing on-premise infrastructure**)

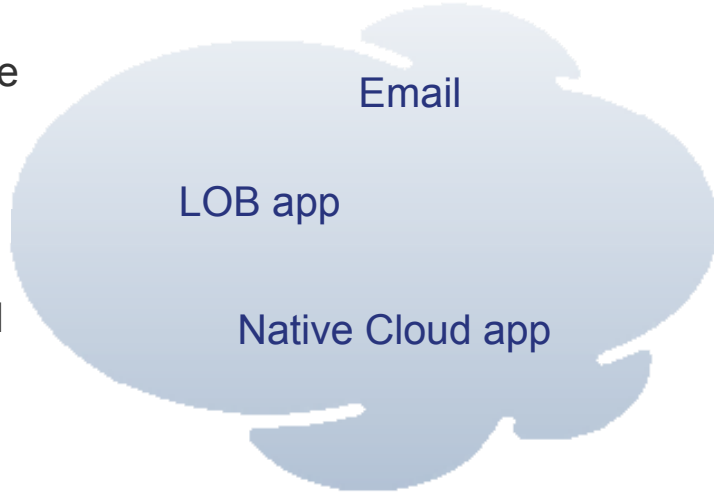


Potential Adoption

•Replace your on-premise physical servers/ datacenters with Cloud based infrastructure
•Cloud for storage, backup and disaster recovery
•Get additional compute capacity (CPU, storage, etc.) for on-premise apps on-demand, i.e., "burst capacity"

Cloud Computing Overview
Defining PaaS

- "OS environment in the sky", running in an Internet scale data center
- The hardware, Cloud operating system and data center facilities are owned and managed by the Cloud provider, and not by the enterprise
- Shared multi-tenant infrastructure offers infinite scale, pay-as-you-go use model, metered billing, anywhere access, etc.
- Third party ISVs can also build/host their applications on this Cloud infrastructure, and expose them as SaaS offerings to enterprise customers
- Enterprises run their apps on this Cloud infrastructure, paying-as-they-go for the server resources they consume (e.g., CPU, storage, bandwidth)
- Enterprise IT admins mainly need to be concerned about the application layer. The OS and hardware layers are the responsibility of the Cloud provider
- The Cloud environment can co-exist with on-premises IT, or can replace it

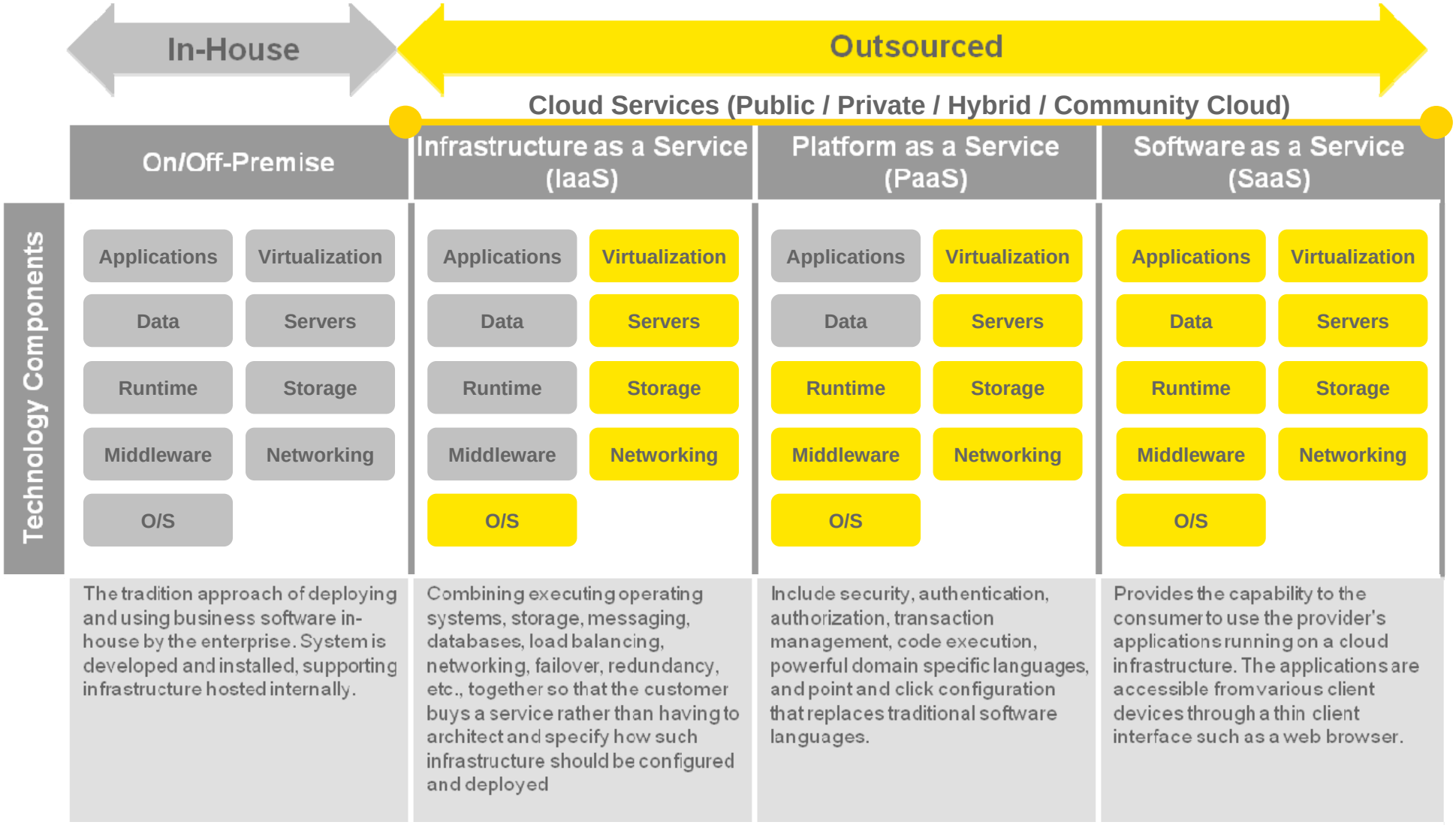


Delivered as a service

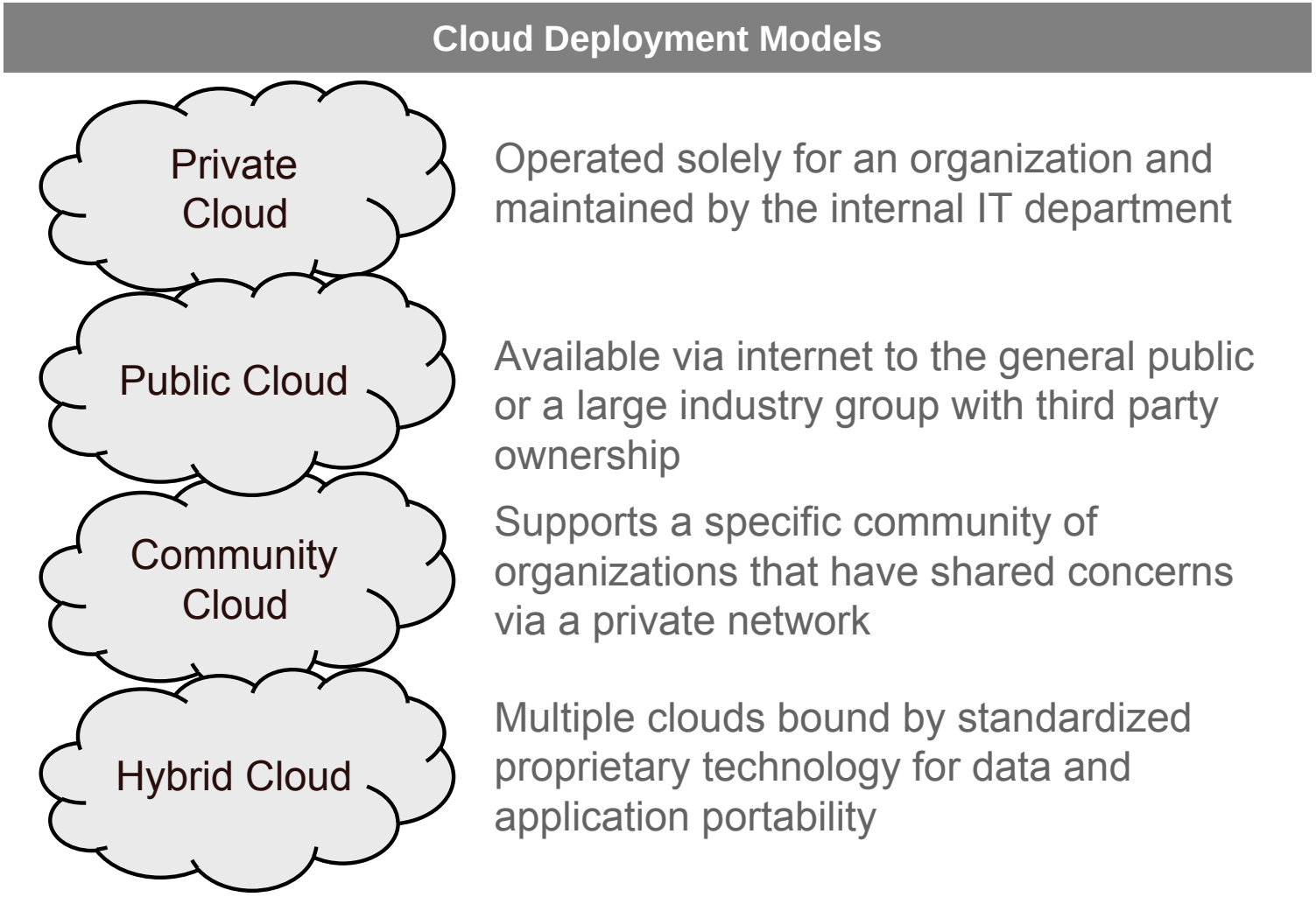
Potential Adoption

•**Build native Cloud applications** that leverage available Cloud provider APIs and services
•**Host your existing LOB and packaged applications** as virtual machines in the Cloud
•**Consume SaaS offerings** from enterprise software vendors

The cloud can be delivered and deployed differently



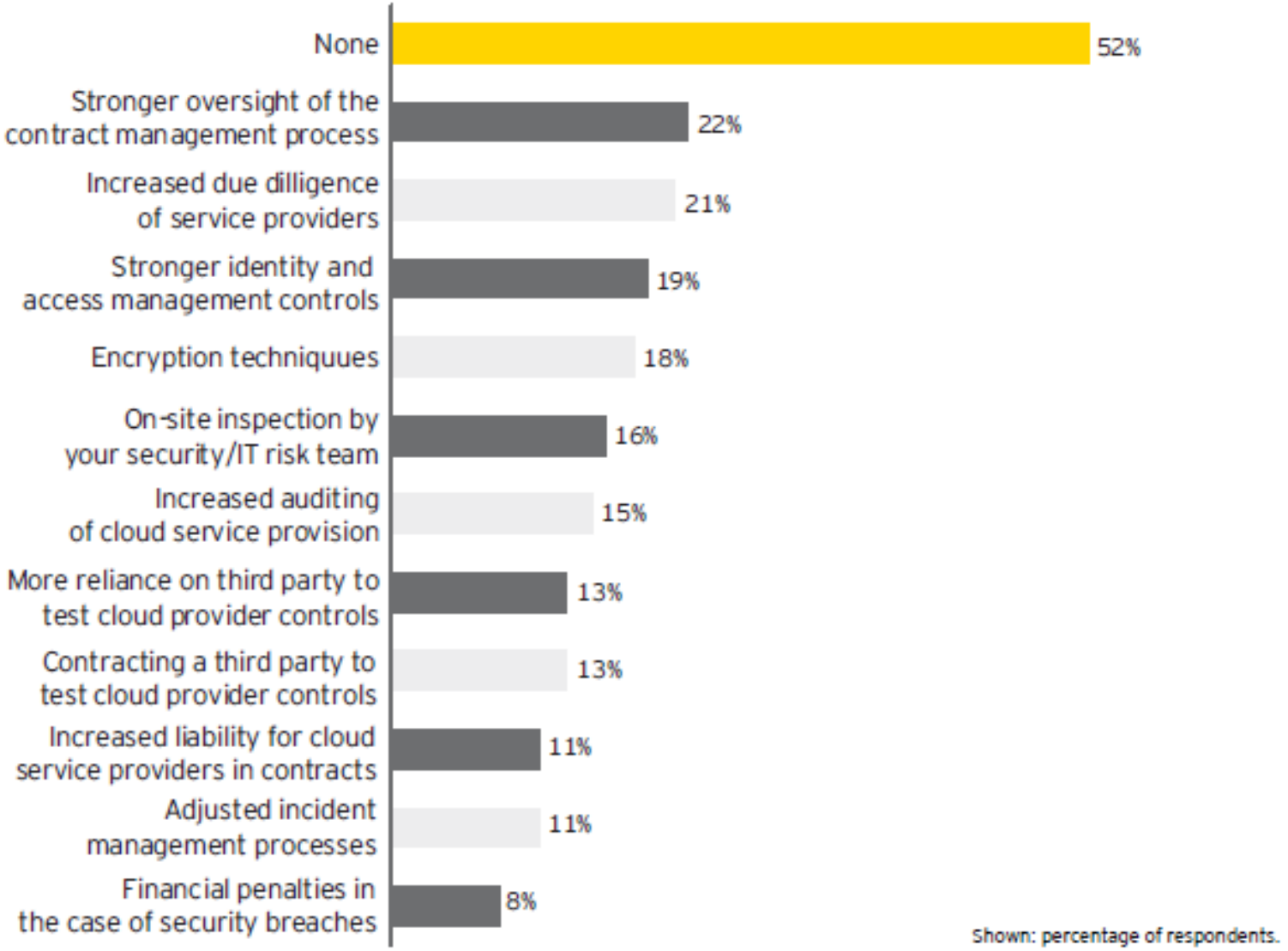
Adoption Model
Types



Cloud Challenges

Organizations not taking appropriate mitigation measures

Controls implemented to mitigate cloud computing risks



Shown: percentage of respondents.

Cloud installation – risks

- Security issues include but are not limited to:
  - Privileged user access
  - Regulatory compliance
  - Data location
  - Data segregation
  - Recovery
  - Investigative support

Cloud installation – risks

- What security issues?
  - **Privileged user access**
  - Regulatory compliance
  - Data location
  - Data segregation
  - Recovery
  - Investigative support

- Sensitive data processed outside the enterprise
- Outsourced services bypass physical, logical and personnel controls

Cloud installation – risks

- What security issues?
  - Privileged user access
  - **Regulatory compliance**
  - Data location
  - Data segregation
  - Recovery
  - Investigative support

- Customers ultimately responsible for security and integrity of own data
- Traditional service providers are subjected to external audits and security certifications

Cloud installation – risks

- What security issues?
  - Privileged user access
  - Regulatory compliance
  - **Data location**
  - Data segregation
  - Recovery
  - Investigative support

- Consumer won't know where the data is stored.
- Service provider may not be storing and processing data in a specific jurisdiction

Cloud installation – risks

- What security issues?
  - Privileged user access
  - Regulatory compliance
  - Data location
  - **Data segregation**
  - Recovery
  - Investigative support

- Data is present in a shared environment
- Encryption is effective but is not full proof

Cloud installation – risks

- What security issues?
  - Privileged user access
  - Regulatory compliance
  - Data location
  - Data segregation
  - **Recovery**
  - Investigative support

- Data might be lost in disaster.
- Provider may not be able to do a complete restoration in a short duration

Cloud installation – risks

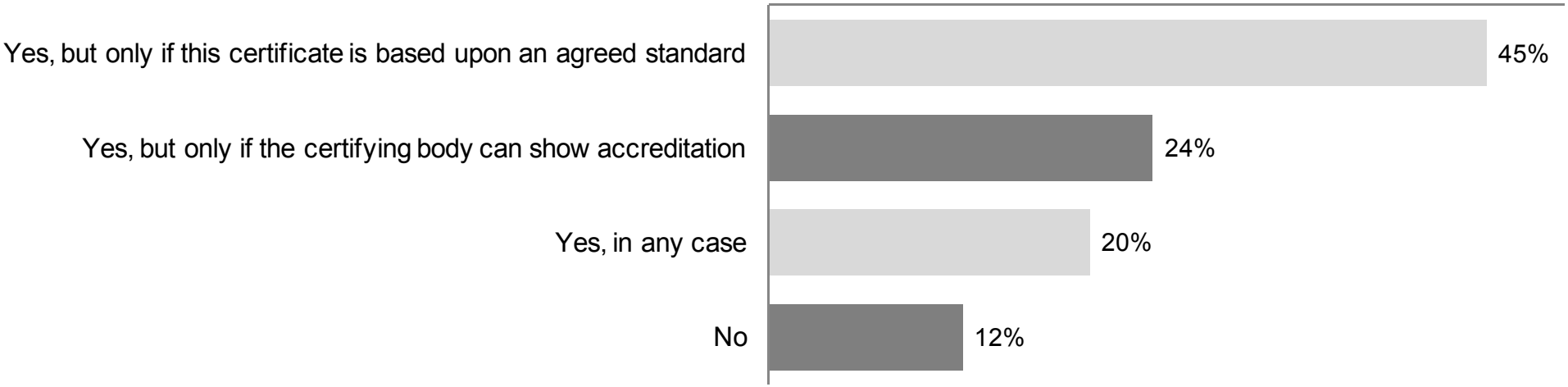
- What security issues?
  - Privileged user access
  - Regulatory compliance
  - Data location
  - Data segregation
  - Recovery
  - **Investigative support**

- Investigating inappropriate activity with data may be impossible
- Data for multiple customers may be co-located and spread across changing set of hosts and data centers

Auditing the Cloud

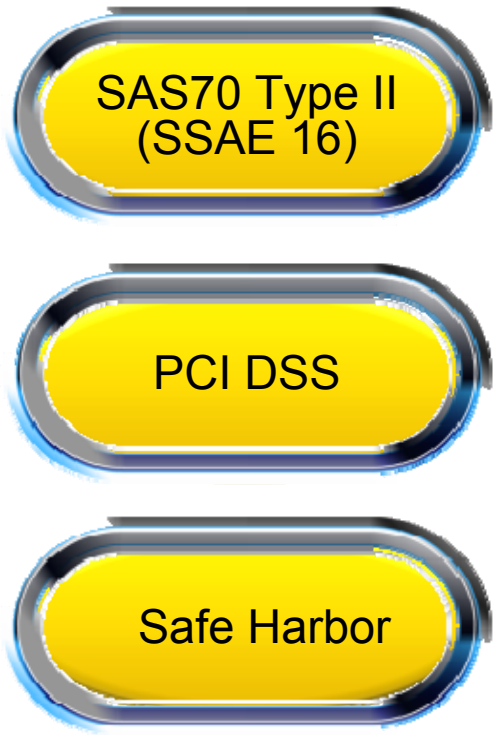
Certifications are key tipping points

Would external certification of cloud service providers increase your trust in cloud computing?



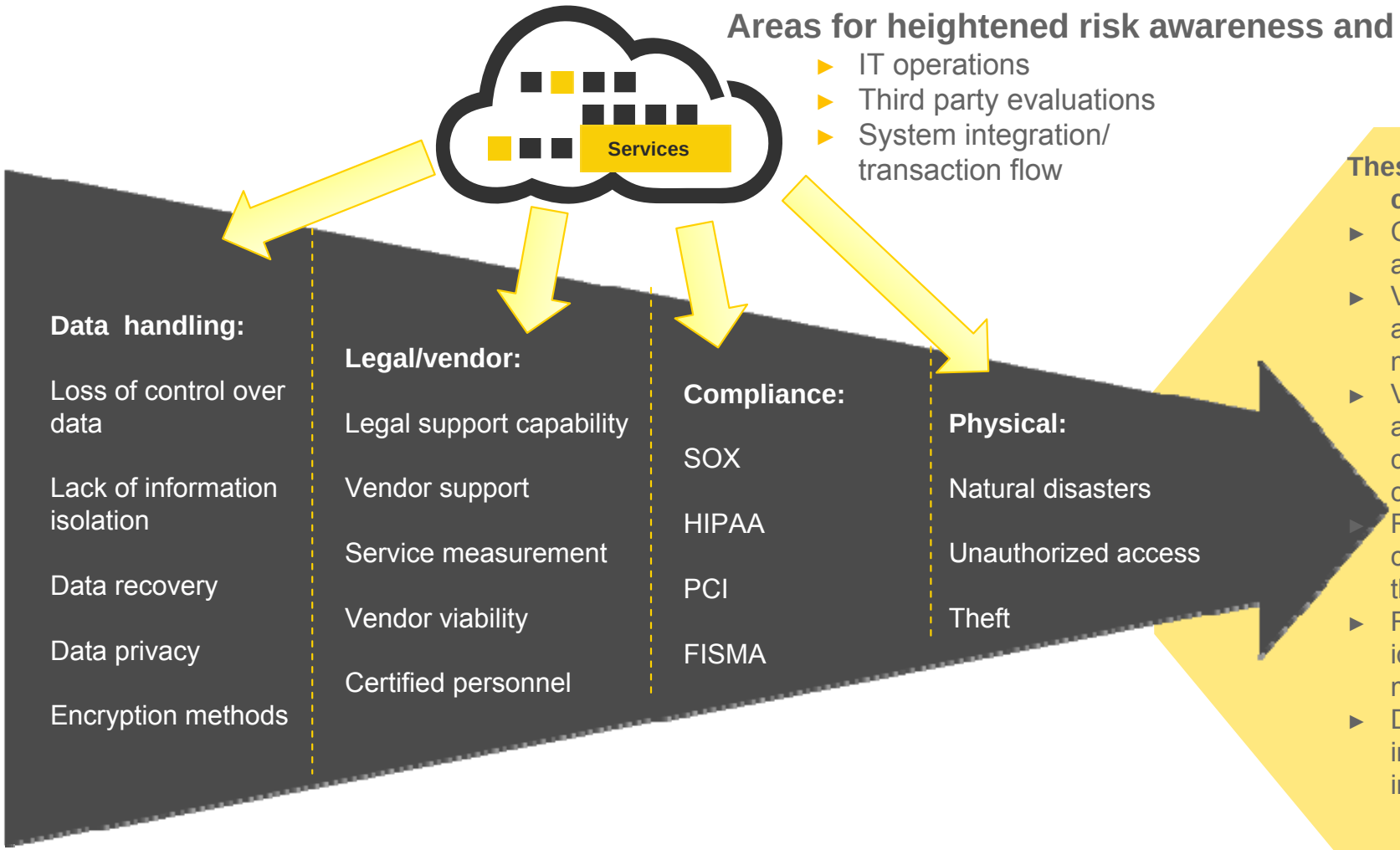
Almost 90% of respondents believed external certification would increase their trust in cloud computing

Auditing the Cloud Compliance



- Cloud computing architectural framework
- Governance
- Legal and eDiscovery
- Data center Tiers, business continuity & disaster recovery
- Infrastructure & application security
- Servers and storage infrastructure (e.g. multi-tenet)
- Information lifecycle management
- Cloud operations and service management
- Portability and interoperability

Risk and audit



Areas for heightened risk awareness and audit focus:

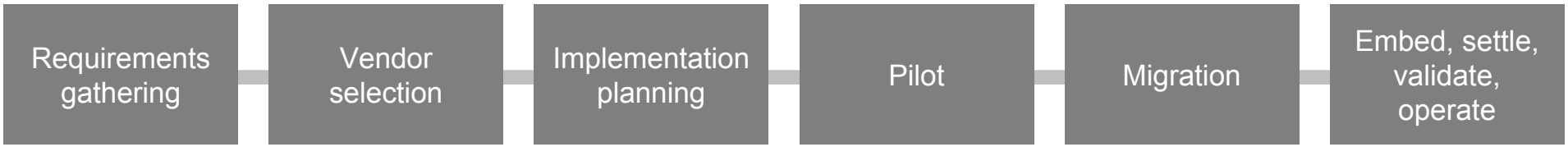
- IT operations
- Third party evaluations
- System integration/ transaction flow

These may be addressed by a combination of:

- Continuous monitoring for availability statistics
- Validating data concerns by assessing vendor data management methods
- Validating vendor longevity and capability using contractual methods with contingencies in place
- Reviewing the vendor compliance policies and third-party certification
- Reviewing access and identity management methods and controls
- Defining and validating integration points both internally and externally

Audit strategies for Cloud implementation

- Audit strategies consider the following aspects
  - Organizational issues
  - Security and privacy issues
  - Legal and compliance issues
  - Performance issues
- Auditing for Cloud is a challenging process, it plays role at each stage in cloud implementation

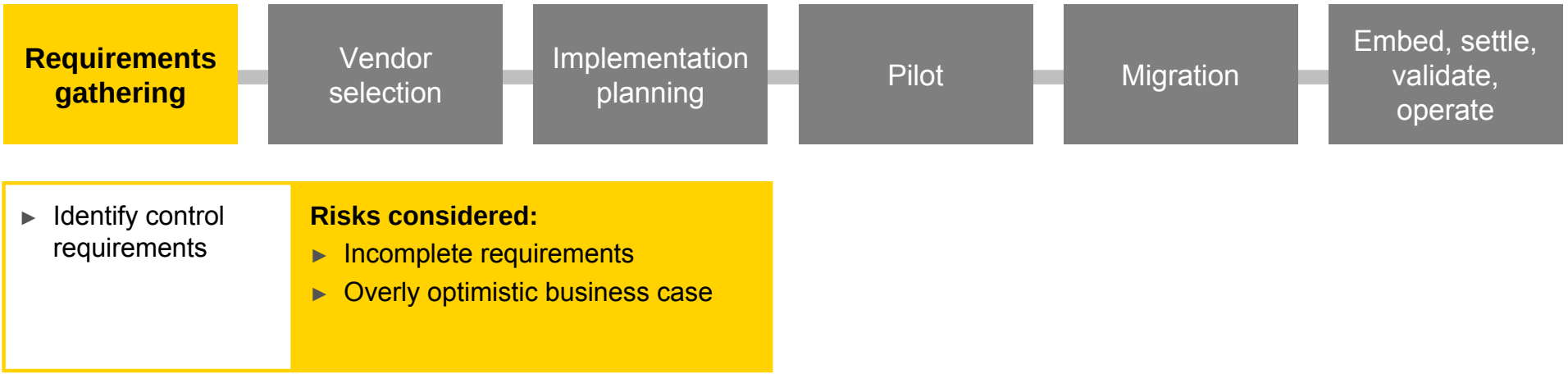


- Investigating inappropriate activity with data may be impossible
- Data for multiple customers may be co-located and spread across changing set of hosts and data centers

- Investigating inappropriate activity with data may be impossible
- Data for multiple customers may be co-located and spread across changing set of hosts and data centers

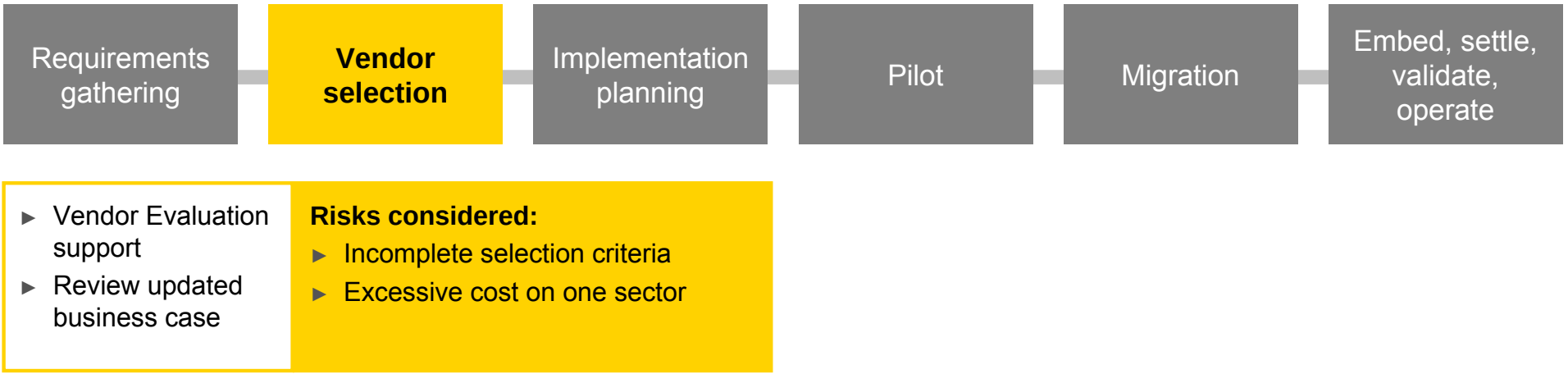
Audit strategies for Cloud implementation

- Audit strategies consider the following aspects
  - Organizational issues
  - Security and privacy issues
  - Legal and compliance issues
  - Performance issues
- Auditing for Cloud is a challenging process, it plays role at each stage in cloud implementation



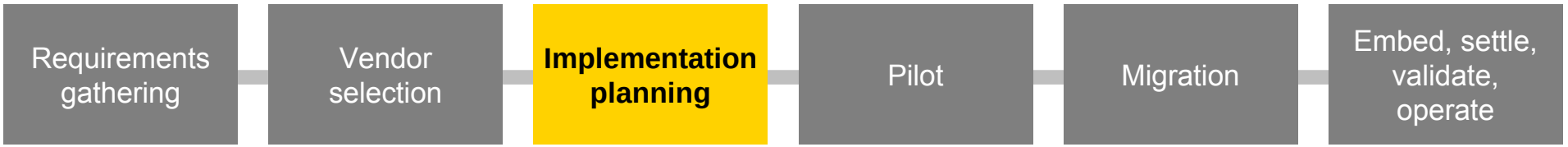
Audit strategies for Cloud implementation

- Audit strategies consider the following aspects
  - Organizational issues
  - Security and privacy issues
  - Legal and compliance issues
  - Performance issues
- Auditing for Cloud is a challenging process, it plays role at each stage in cloud implementation



Audit strategies for Cloud implementation

- Audit strategies consider the following aspects
  - Organizational issues
  - Security and privacy issues
  - Legal and compliance issues
  - Performance issues
- Auditing for Cloud is a challenging process, it plays role at each stage in cloud implementation



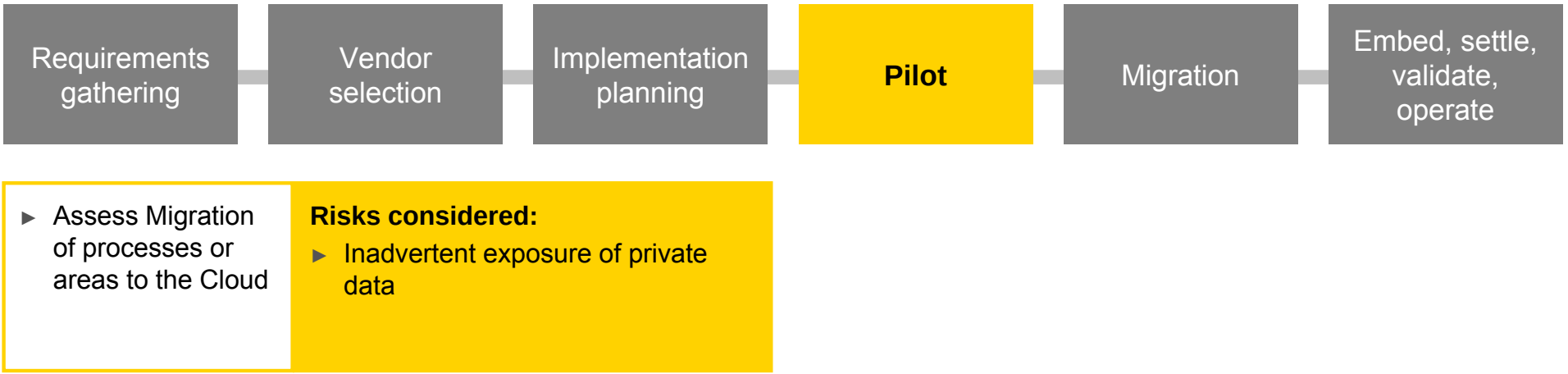
- Data Migration assessment
- Vendor Management Review

Risks considered:

- Design is not secure, fault tolerant or traceable
- Controls not considered

Audit strategies for Cloud implementation

- Audit strategies consider the following aspects
  - Organizational issues
  - Security and privacy issues
  - Legal and compliance issues
  - Performance issues
- Auditing for Cloud is a challenging process, it plays role at each stage in cloud implementation



Audit strategies for Cloud implementation

- Audit strategies consider the following aspects
  - Organizational issues
  - Security and privacy issues
  - Legal and compliance issues
  - Performance issues
- Auditing for Cloud is a challenging process, it plays role at each stage in cloud implementation

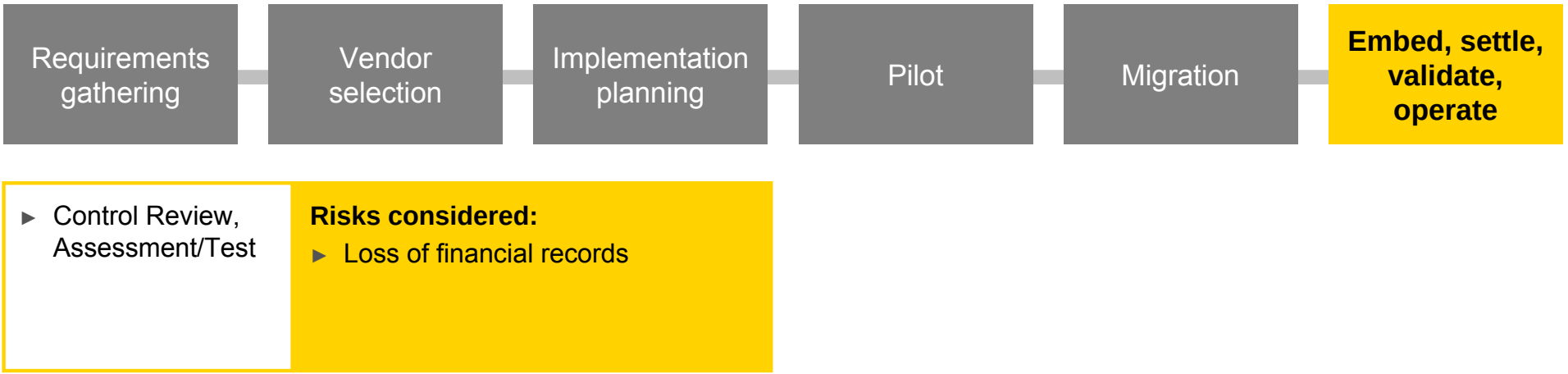
- Data Migration Assessment
- Project Assessment

Risks considered:

- Inadvertent exposure of private data
- Business process don't work as expected

Audit strategies for Cloud implementation

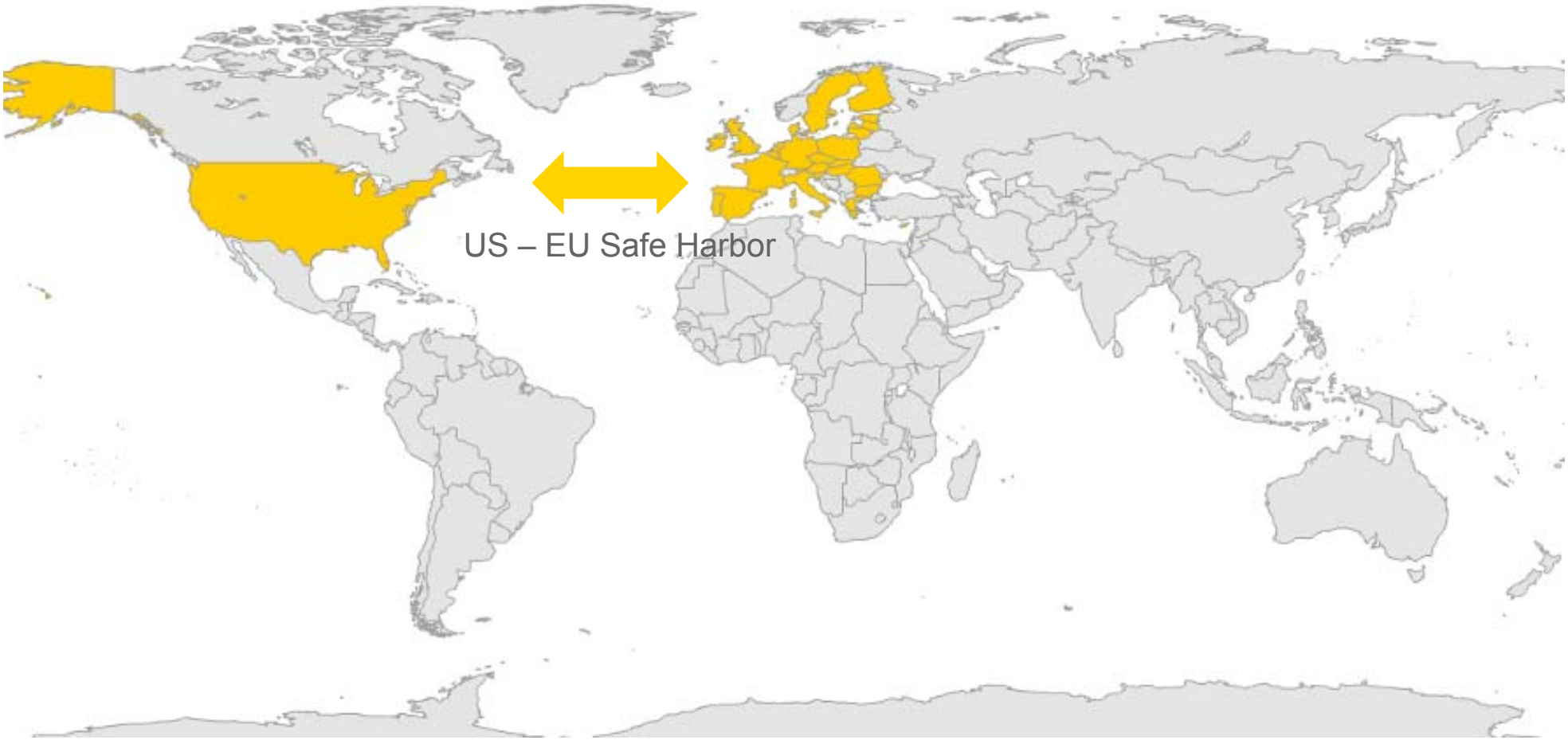
- Audit strategies consider the following aspects
  - Organizational issues
  - Security and privacy issues
  - Legal and compliance issues
  - Performance issues
- Auditing for Cloud is a challenging process, it plays role at each stage in cloud implementation



Sensitivity of Laws Based on Geographical Boundaries

America:
- USA PATRIOT Act

European Union:
- Data Protection Act



Measures to Address Legal Challenges

PROPOSED METHODOLOGY

- Form a team consisting of IT professionals and lawyers
- Assess the organization's compliance with laws that restrict trans-border information flow
- Create a roadmap outlining risks and mitigation strategies
- Communicate with sponsors and get approval
- Communicate expectations with cloud service provider (electronic discovery, litigation hold, discovery searches, etc.)
- Obtain visibility on the region of data hosting
- Create a unified process to respond to subpoenas, service, legal requests

Measures to Address Governance Challenges

2) Define the internal metrics and acceptable performance levels

3) Assess vendor capabilities, maturity and consistency

1) Form a strong internal governance team

GOVERNANCE CHALLENGES

- Inability to achieve performance metrics
- Immature processes that lead to unstable services

4) Communicate expectations to vendor

6) Conduct periodic tests on vendor – penetration test, activity monitoring, vulnerability test, etc.

5) Define a common governance model

Measures to Address Compliance Challenges

Sarbanes-Oxley (SOX) Compliance

Compliance Challenges

HIPAA Compliance

PCI-DSS Compliance

4 Key Strategies

- Identify the applications that are least subject to compliance regulations
- Assess vendor certification – SAS 70, ISO/IEC 27001
- Conduct regular audits on the cloud service provider
- Formulate a process to collect and store compliance evidence – audit logs, activity reports

Evaluate key service agreement areas

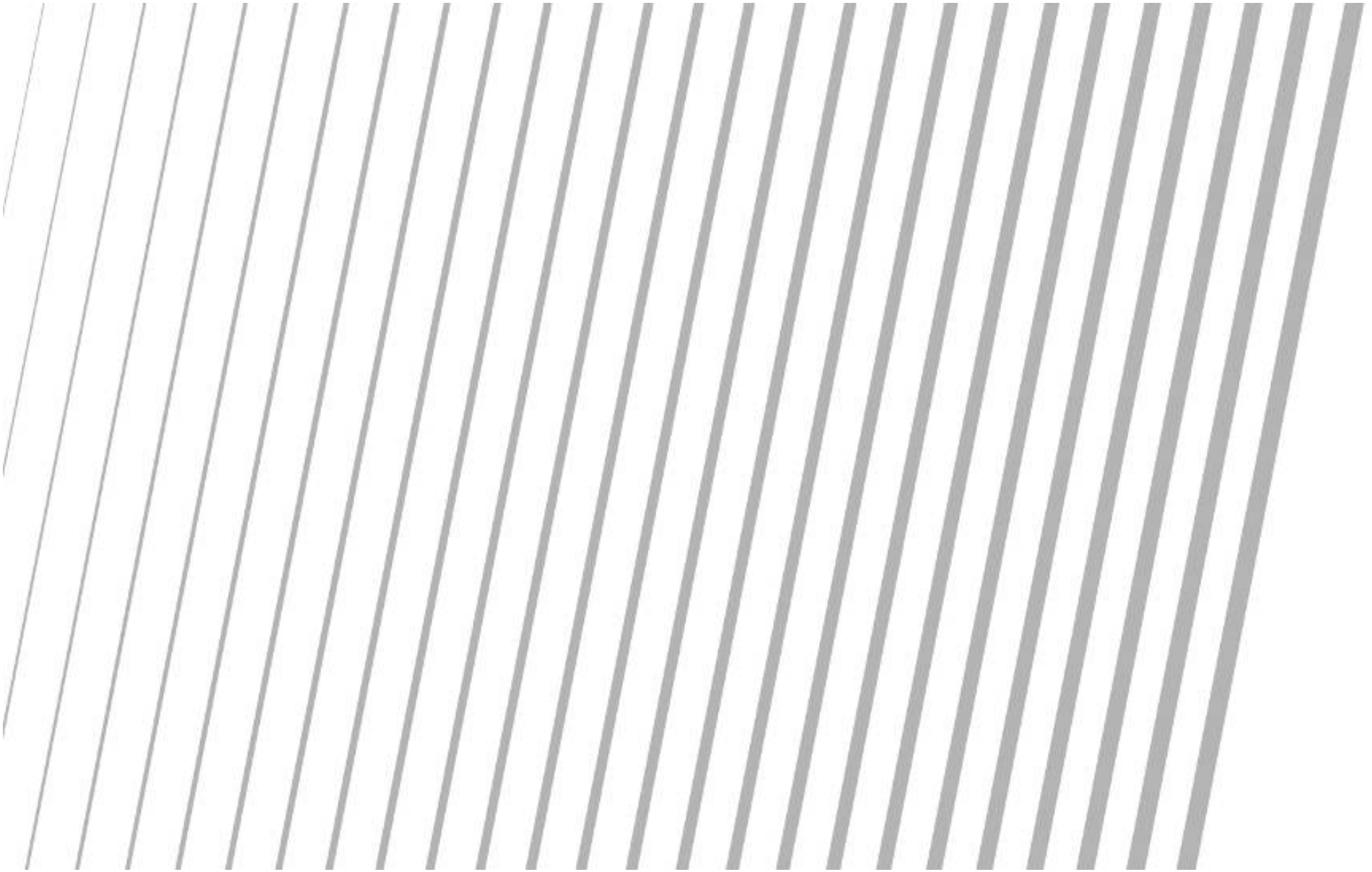
- Physical
  - Locations of organizational data
- Organizational
  - The cloud provider's points of interface with the organization
  - Incident response coordination and information sharing
- Process
  - Independent audits and testing
  - Procedures for handling sensitive data
  - Disaster recovery processes
- Technical
  - Service availability and contingency options
  - Data backup and recovery terms
- Legal
  - Ownership rights over data
  - "Blind subpoena" clauses
  - Specific remedies for harm caused or non-compliance by the cloud provider
  - The cloud provider's obligations upon contract termination
  - Restrictions on the use of customer metadata (payment data, data usage statistics, etc.)

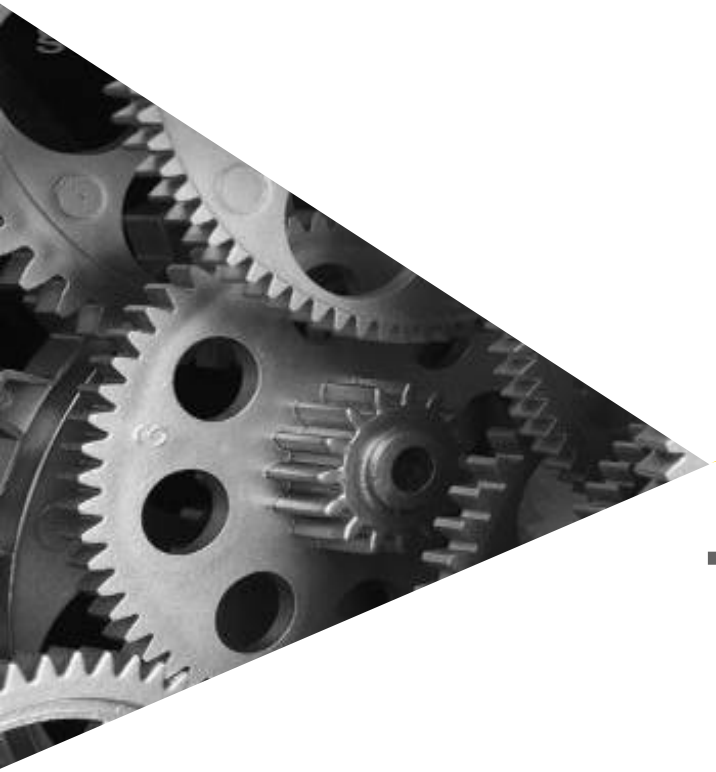
Challenges can be managed

- Review the SLA for the following key points:
  - Service availability and contingency options
  - Independent audits and testing
  - Specific remedies for harm caused or noncompliance by the cloud provider
  - Procedures for handling sensitive data
  - Ownership rights over data
  - Locations of organizational data
  - “Blind subpoena” clauses
  - Data backup and recovery terms
  - Incident response coordination and information sharing
  - Disaster recovery processes
  - The cloud provider’s obligations upon contract termination

- Just because it is on premise does not mean it is more secure
  - ***“What we’re finding is that, in a lot of cases, our clients’ data is more secure on the cloud than it is on the premises because of some of the measures taken by some of the cloud-based vendors we work with.”*** **- Michael Smith**, CPA/CITP, managing director of RSM McGladrey’s consulting practice and a member of the AICPA’s IT Executive Committee.

Questions and answers





Thank You