Morgan Lewis

# Legal Issues in Outsourcing and Shared Services Engagements

April 19, 2012

Barbara Melby | Michael Pillion | Margaret Gatti | Vicki Phelan
Megan Gatto | Scott Richelson

# Introduction

# Agenda

- Introduction
- The Industry View: KPMG's Analysis for 2012 and Beyond (Vicki Phelan)
- Hot Topics in Outsourcing: Demystifying Cloud Computing (Barbara Melby and Scott Richelson)
- Moving Data Across Borders for Outsourcing Purposes (Margaret Gatti)
- Data Privacy (Michael Pillion and Megan Gatto)

# Logistics

- Facilities
- Contact Information

# Participants


**Barbara Melby**
**Partner**
Morgan Lewis
215.963.5053
bmelby@morganlewis.com



**Vicki Phelan**
**Director, Shared Services and Outsourcing Advisory**
KPMG
609.304.1030
vphelan@kpmg.com



**Michael L. Pillion**
**Partner**
Morgan Lewis
215.963.5554
mpillion@morganlewis.com



**Megan E. Gatto**
**Associate**
Morgan Lewis
215.963.5526
mgatto@morganlewis.com



**Margaret Gatti**
**Partner**
Morgan Lewis
202.739.5409
mgatti@morganlewis.com



**Scott Richelson**
**Associate**
Morgan Lewis
215.963.5071
srichelson@morganlewis.com






Morgan Lewis

# The Industry View: KPMG's Analysis for 2012 and Beyond

# Today’s agenda

| | |
|---|---|
| **1** | **Macro trends** |
| **2** | Global business services |

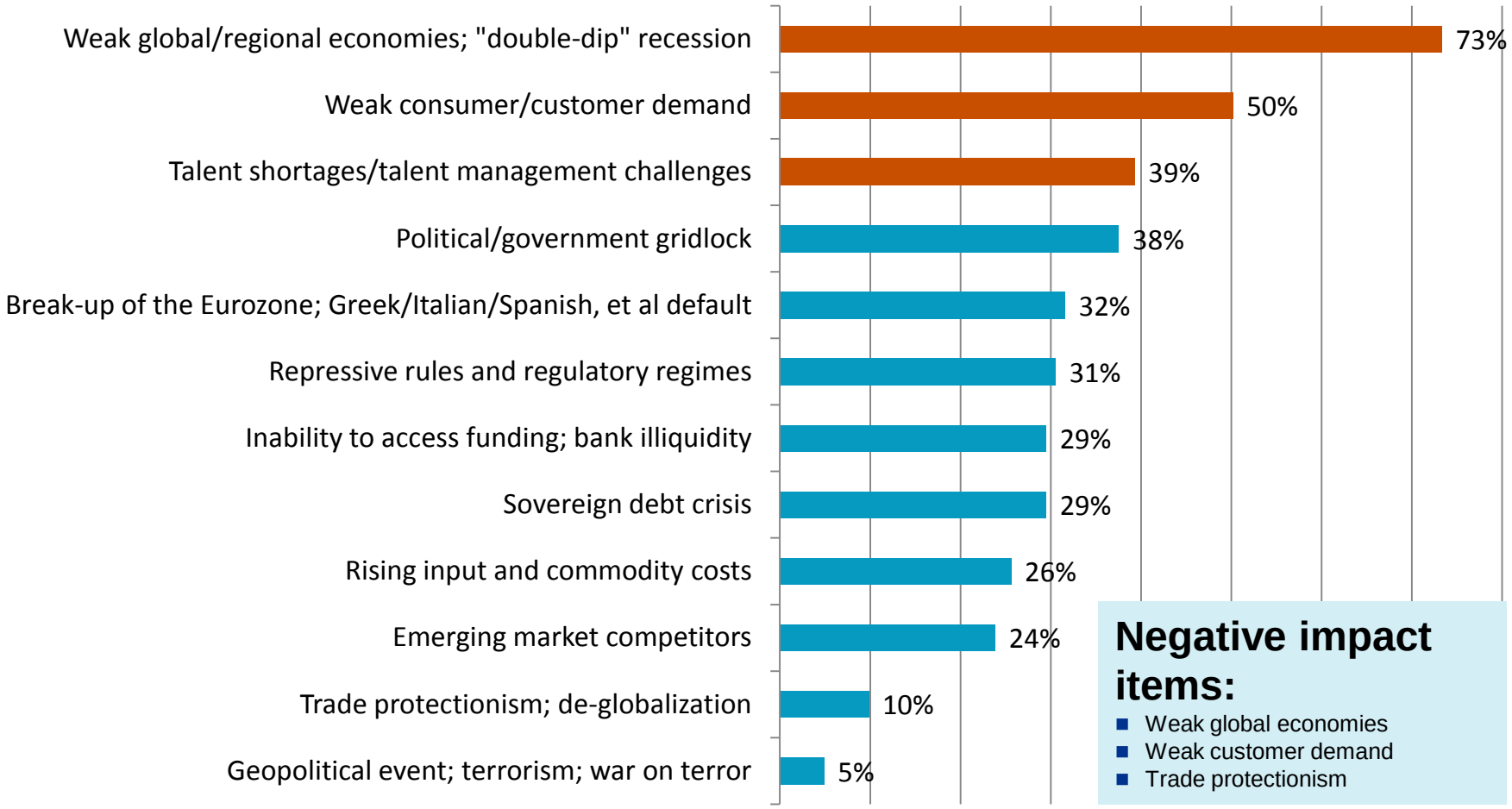
# Macro global business trends

- Recession, Double Dips & Debt
- Capitalism vs. State Capitalism vs. the State
- Demise in the West – or Not – Occupy This!
- Population Shifts in the World – Go East for Growth
- Next Gen (Again) IT: Social Media, Cloud, Crowd, Consumerization, Mobility
- Global Talent Management – Find, Attract, Retain
- All Create New and Greater Business and Information Management Challenges
- What does a more than 10-Year-Old Firm Do to Compete??

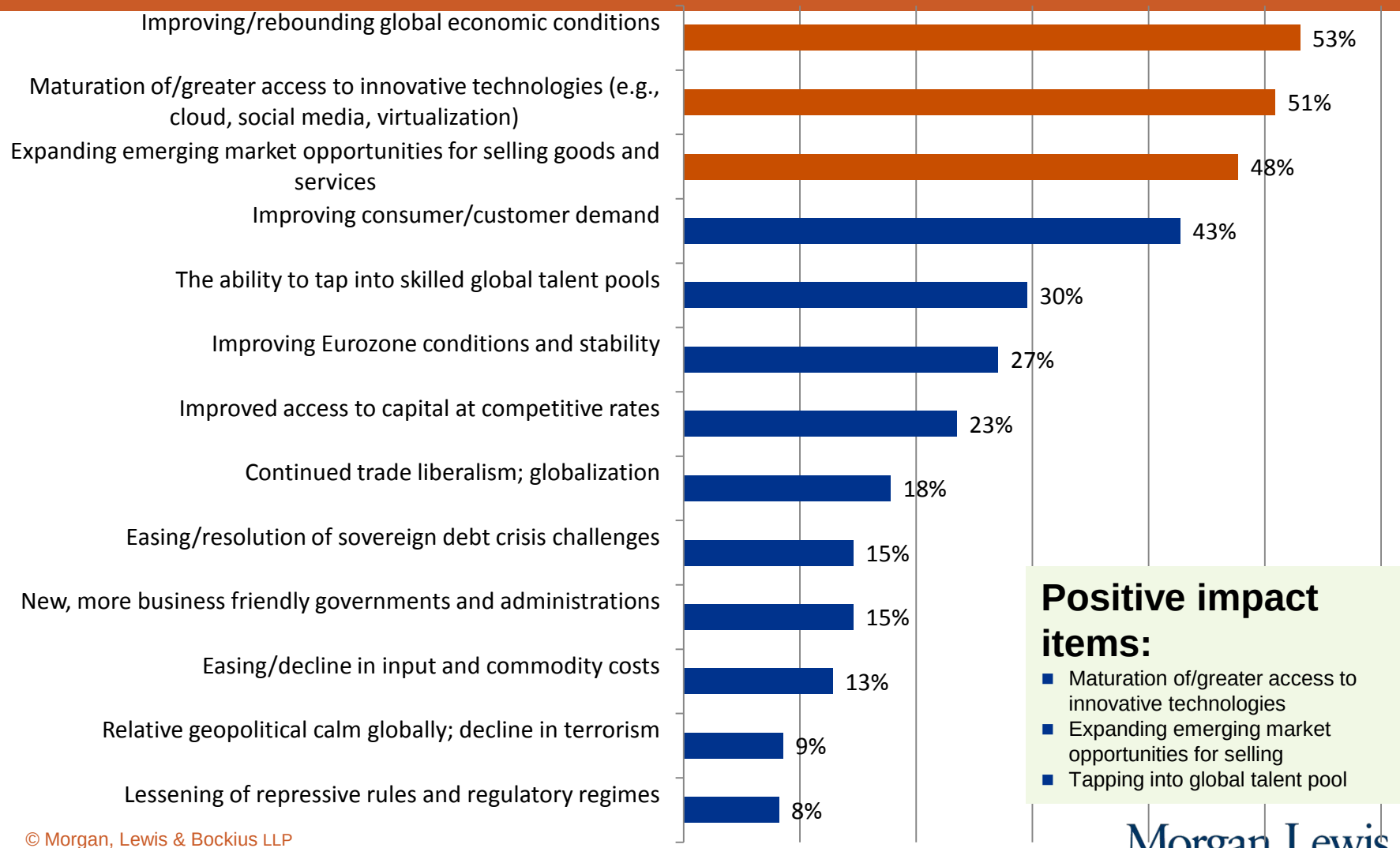


KPMG

# 2012 Trends with Biggest Negative Impact on User Organizations



# 2012 Trends with Biggest Positive Impact on User Organizations



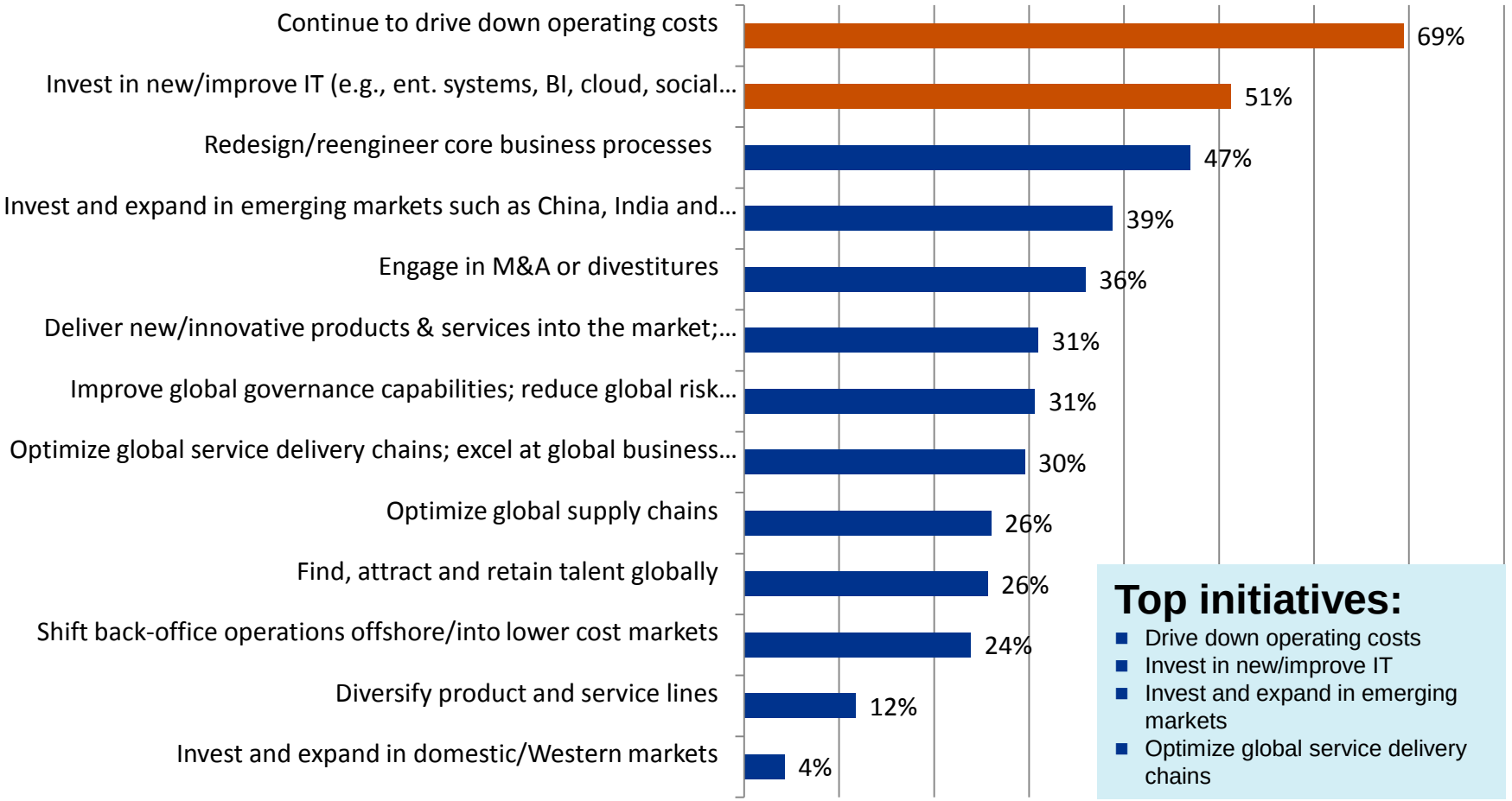

**Positive impact items:**

- Maturation of/greater access to innovative technologies
- Expanding emerging market opportunities for selling
- Tapping into global talent pool



Morgan Lewis

# Top 2012 User Organization Initiatives



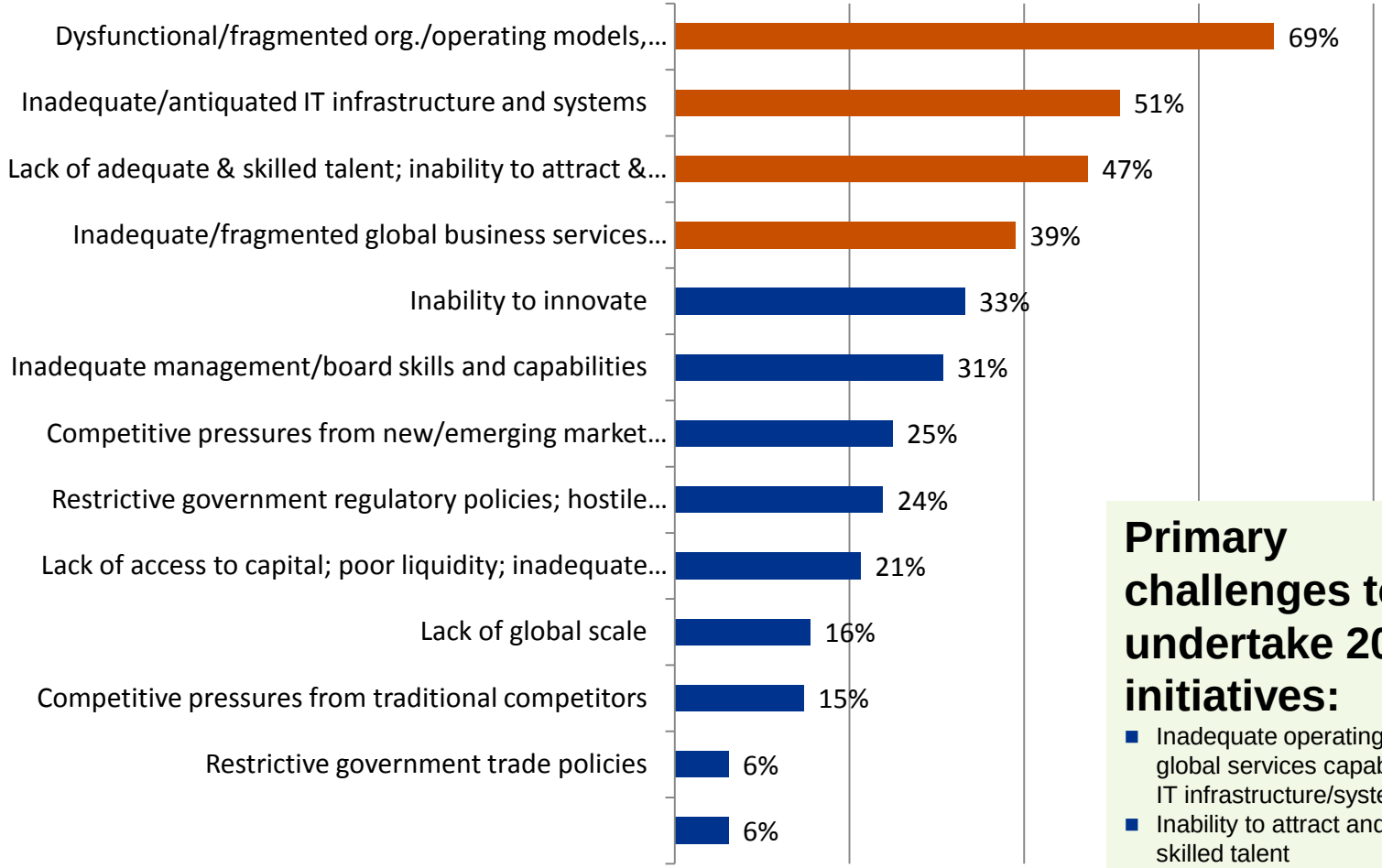

**Top initiatives:**

- Drive down operating costs
- Invest in new/improve IT
- Invest and expand in emerging markets
- Optimize global service delivery chains



KPMG

# Top Challenges to Successfully Undertaking 2012 Initiatives



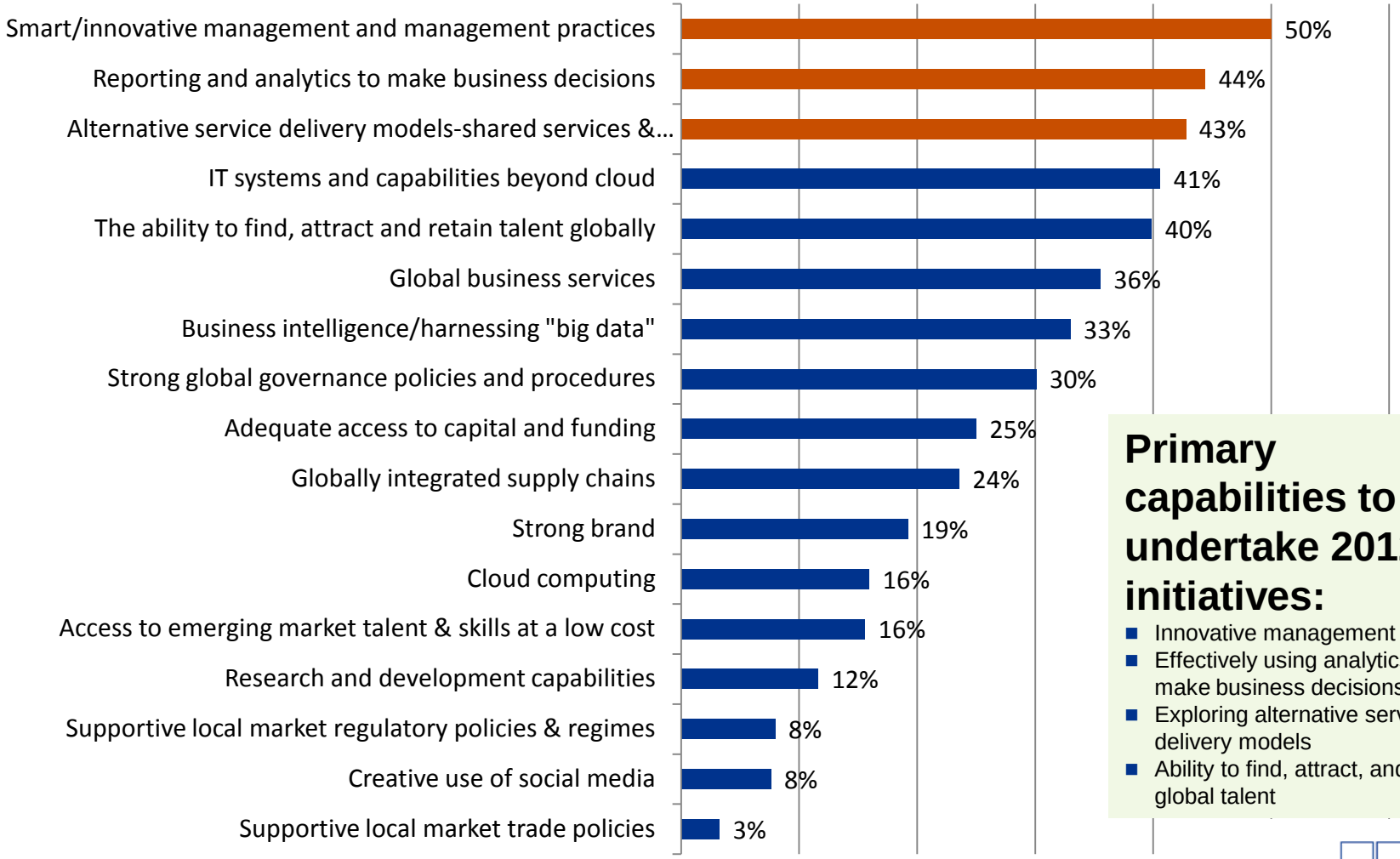

**Primary challenges to undertake 2012 initiatives:**

- Inadequate operating models, global services capabilities, and IT infrastructure/systems
- Inability to attract and retain skilled talent



KPMG

# Top Capabilities Required to Successfully Undertake Top 2012 Initiatives




**Primary capabilities to undertake 2012 initiatives:**

- Innovative management
- Effectively using analytics to make business decisions
- Exploring alternative service-delivery models
- Ability to find, attract, and retain global talent

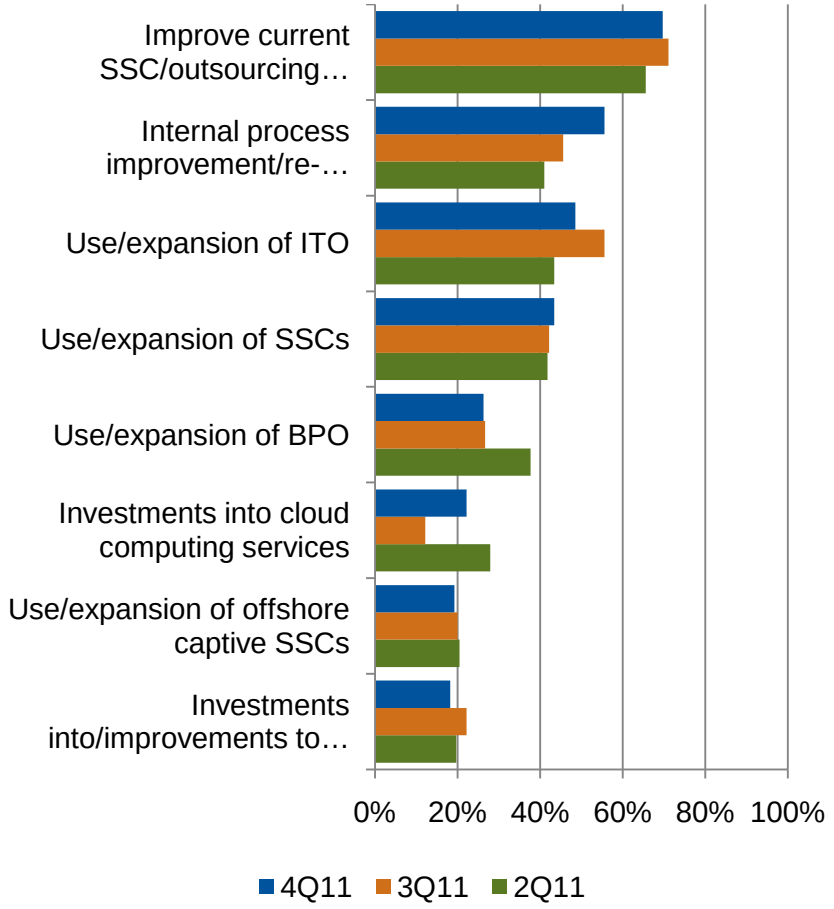


KPMG

# Assessing the Global Business Services Market

## Top Approaches to Improve Service Delivery Capabilities

- Organizations continue to focus more efforts on maximizing and better managing existing global business services investments ,recognizing there is the potential to wring much more benefit out of many existing efforts
- More interest is being placed on process redesign both to improve performance and better fit into GBS operating models
- While many organizations are more calculating, demanding and realistic on the potential benefits from new sourcing efforts, they struggle to achieve the benefits sought from efforts already in the field
- Cloud investments are occurring but more so in the context of other efforts than for their own sake and benefit



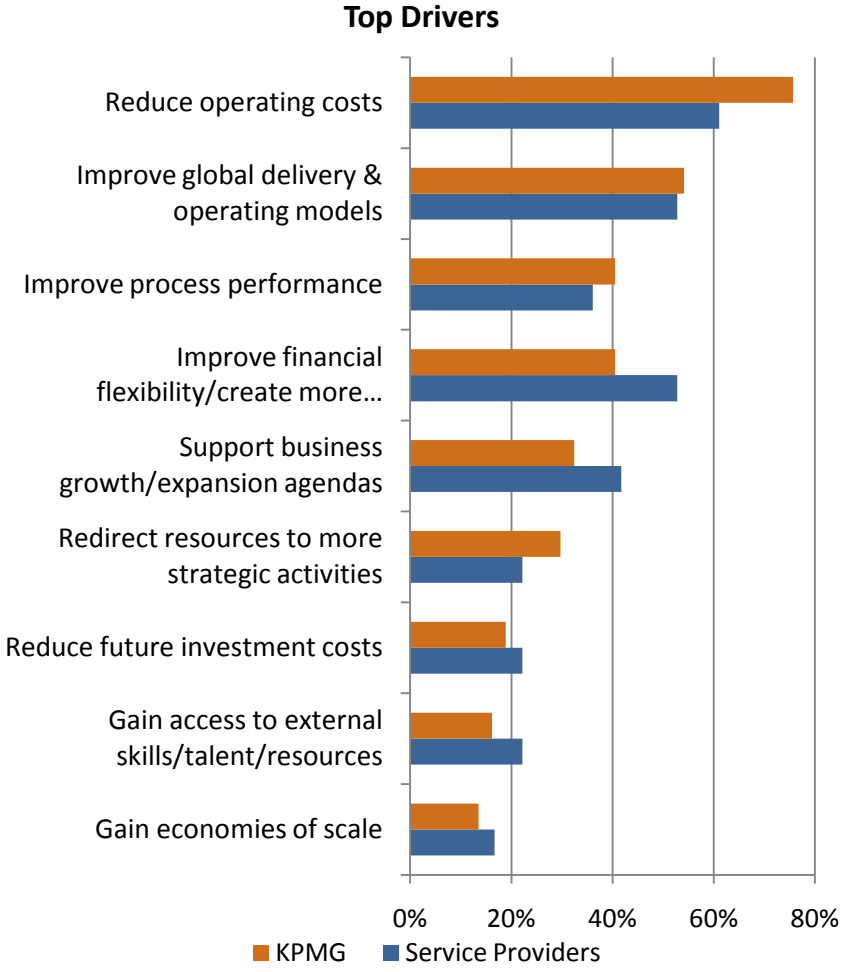

**Source: KPMG Global Pulse Survey 4Q11**

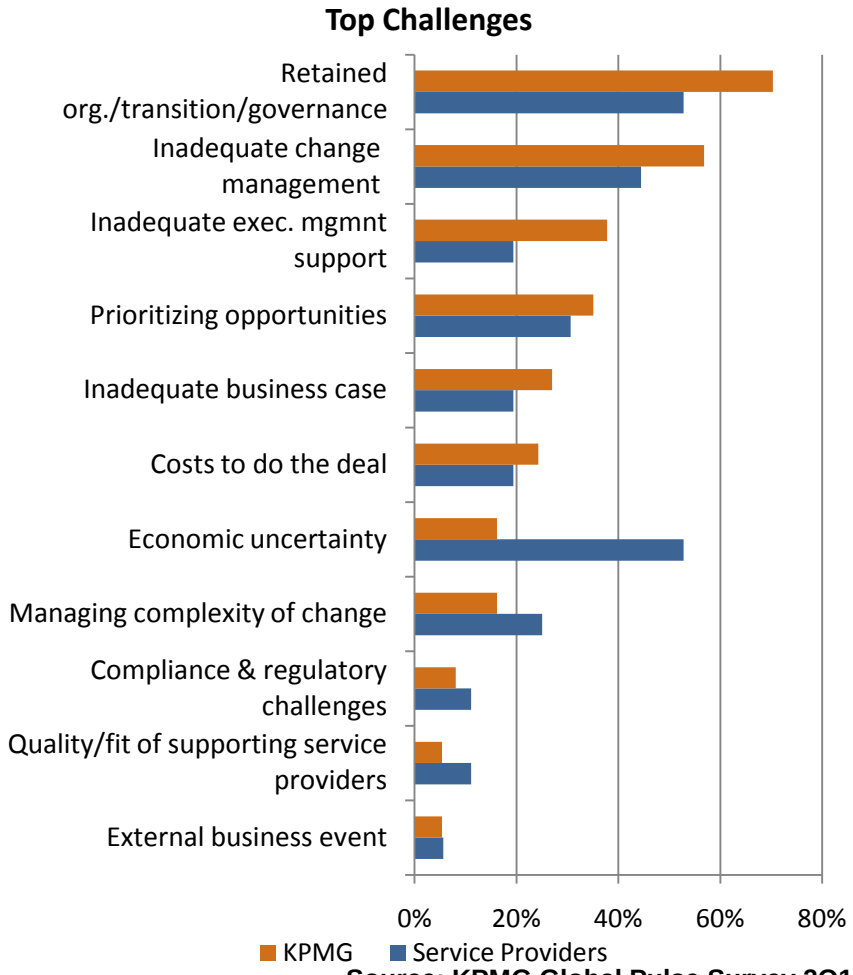


KPMG

# Assessing the Global Business Services Market

## Top Drivers and Challenges to GBS Efforts




**Source: KPMG Global Pulse Survey 2Q11**

# As the C-Suite agenda focuses on efficiency, compliance, and growth, GBS models must evolve

Align the operating model for efficiency and effectiveness

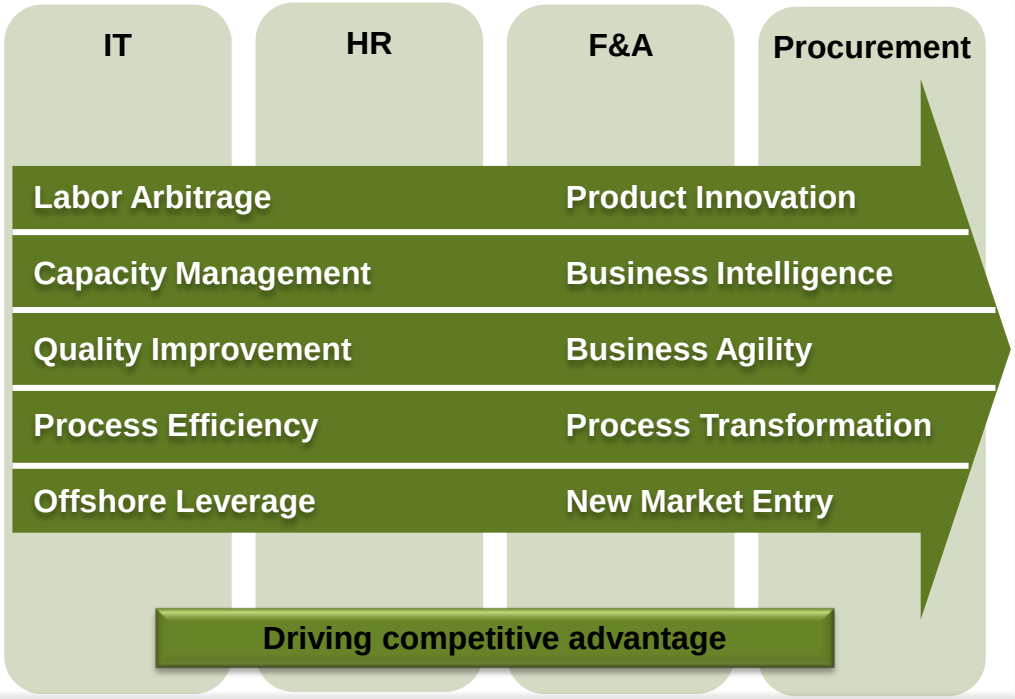
Optimize the global operations footprint

Drive growth in emerging markets

Manage global risk and compliance

Leverage investment in technologies

- Sourcing and Shared Service Goals are moving beyond just cost savings
- Leading sourcing and shared service organizations are advancing their capabilities, evolving to models engineered to be positive influencers of change
- Success in this new model depends on the ability to dynamically assemble a variety of capabilities – regardless of where those capabilities reside – into a seamless end-to-end process that's focused on a specific business outcome



# Cost Reduction has been a Primary Impetus for GBS Initiatives Key Cost-Reduction Levers

| Lever | Potential Reduction | Main Aspects |
|---|---|---|
| **BPR** | **10-25%** | Process Re-design, Benchmarking, Implementing and active management of KPIs |
| **Automation** | **10-60%** | Converting to electronic inputs, live data feeds, image & workflow systems, ICR/OCR, signature verification |
| **IT Optimization** | **10-20%** | Rationalize IT application, hardware portfolio |
| **Location** | **10-65%** | Move people in operations offshore to low-cost locations, e.g., India, South Africa, Indonesia, China, Europe |
| **Scale** | **5-20%** | Consolidate processes (within companies, within industries, across industries) |
| **Continuous Improvement** | **3-8% pa** | CI using factory mgmt (eg. incentives) and quality techniques (eg. Lean Manufacturing, Six Sigma) |



KPMG

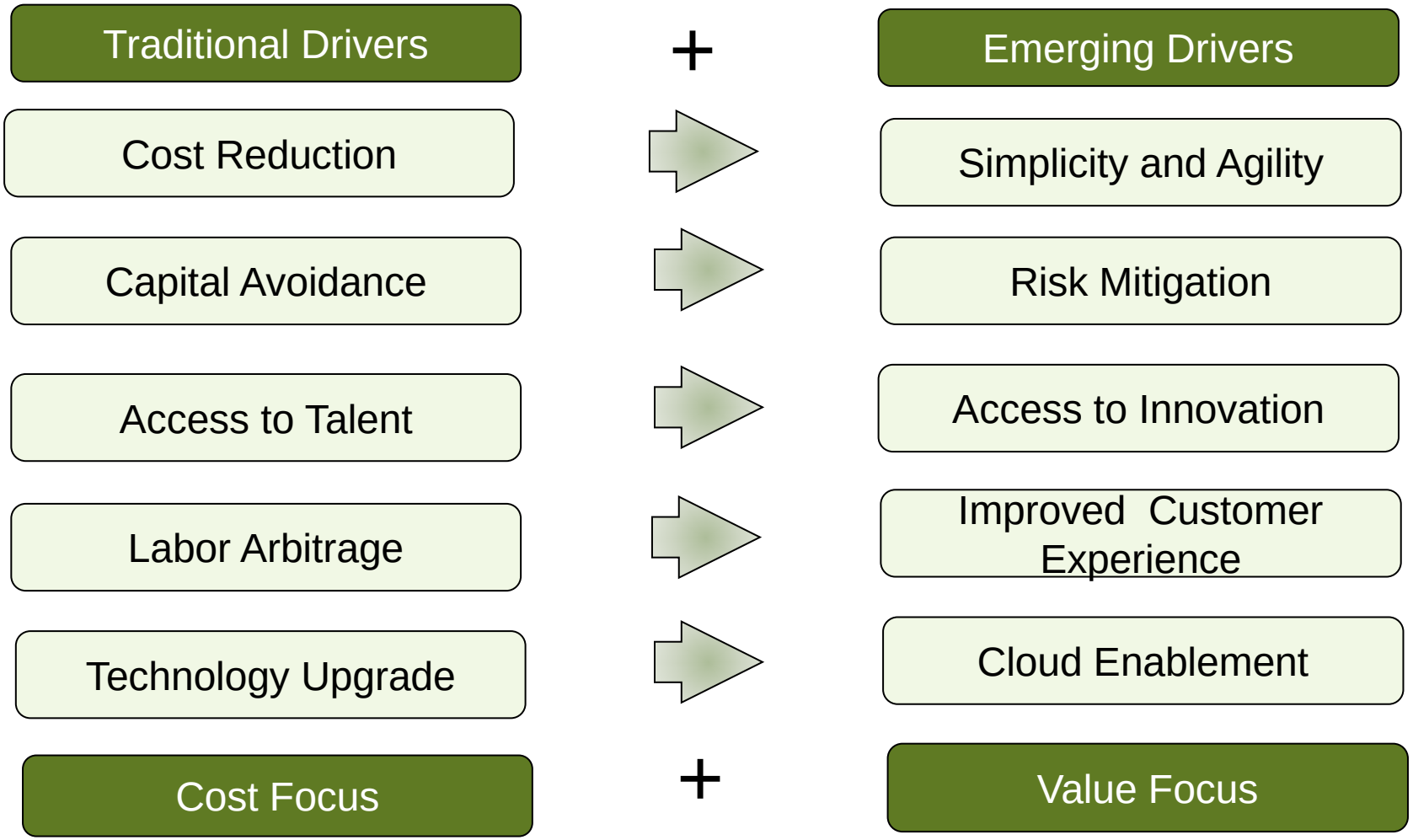
# Today's GBS Value Proposition Extends Beyond Cost Reduction

| | |
|---|---|
| **Administrative Savings** | • Economy of scale – consolidation, skill mix, productivity<br>• Economy of place – labor arbitrage, labor availability |
| **Customer Experience** | • Simplification, standardization and best practice deployment<br>• Continuous improvement and service quality management<br>• Customer satisfaction and demand management |
| **Transformational Impact** | • Automation, self-service, digitization<br>• Aggregation/reduction of 3rd party spend; cash management<br>• Data & information management; analytics |
| **Business Focus** | • BU focus on business specific activity: revenue generation and production<br>• SSC focus on leveraging expertise across back-office |
| **Flexibility** | • Adaptive to changes in the business model<br>• Ease of integrating acquisitions; cost variability |
| **Compliance & Control** | • Improved process documentation, visibility and data integrity<br>• Simplified compliance monitoring, reporting and transparency<br>• Business continuity and disaster recovery planning |

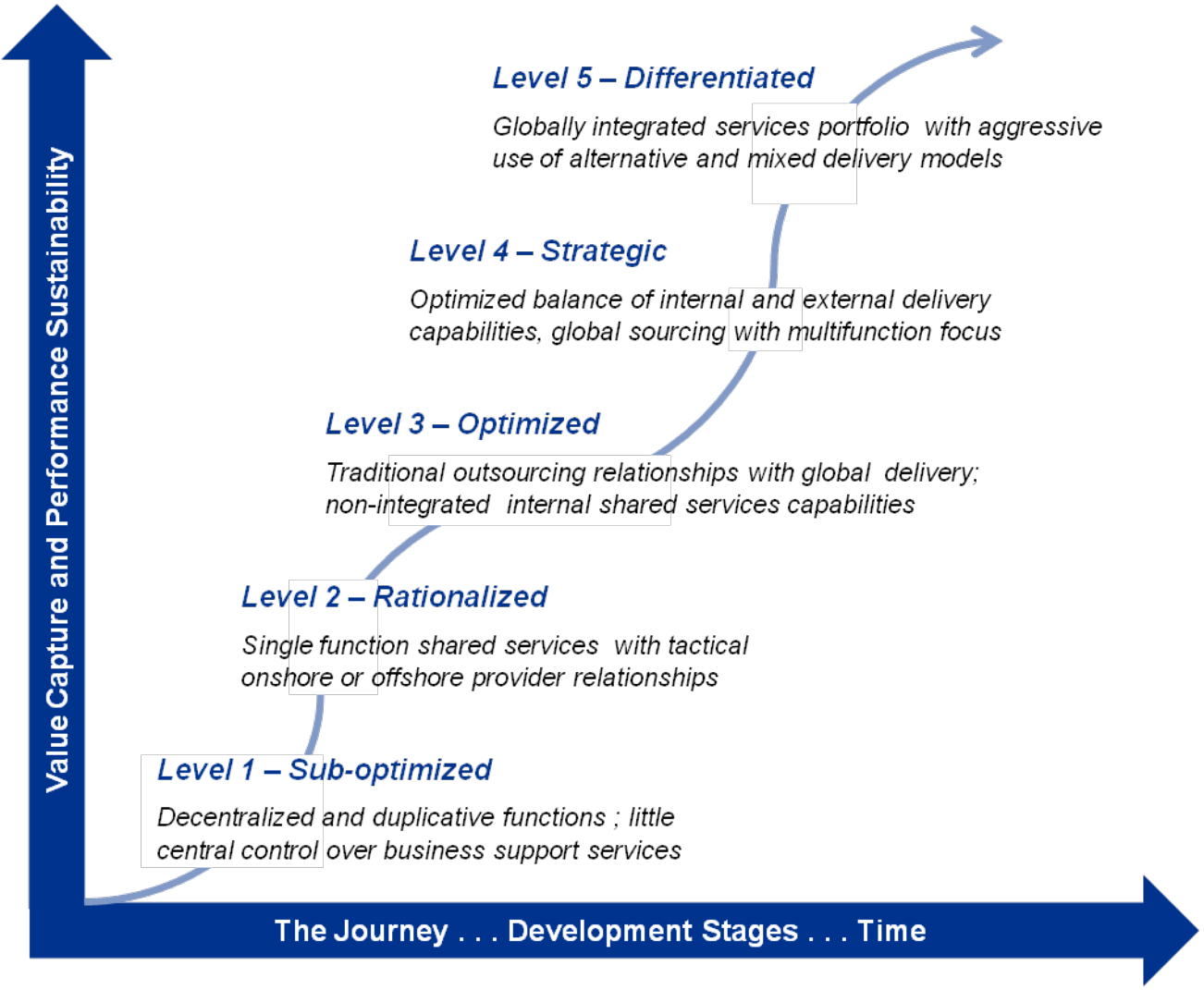


KPMG

# The Value Proposition Is Shifting from a Cost to a Value Focus in Mature Shared-Service Organizations



# What Does the Improvement Journey Entail? The Services Delivery Maturity Curve




## Attributes of a Mature Model

- Cohesive vision for **leveraging and integrating "horizontal" processes** across enterprise
- **Global process management** and service delivery platform
- Balance of **internal and external service delivery**
- Integrated delivery centers and COEs, with a focus on **customer experience and innovation**
- Strong emphasis on **governance**, performance, and talent management
- **Flexible** to dynamic business needs and priorities
- Ongoing **competition** within service supply chain
- **Outcome** focused

# Maturity Assessment Against the Shared Services Excellence Framework

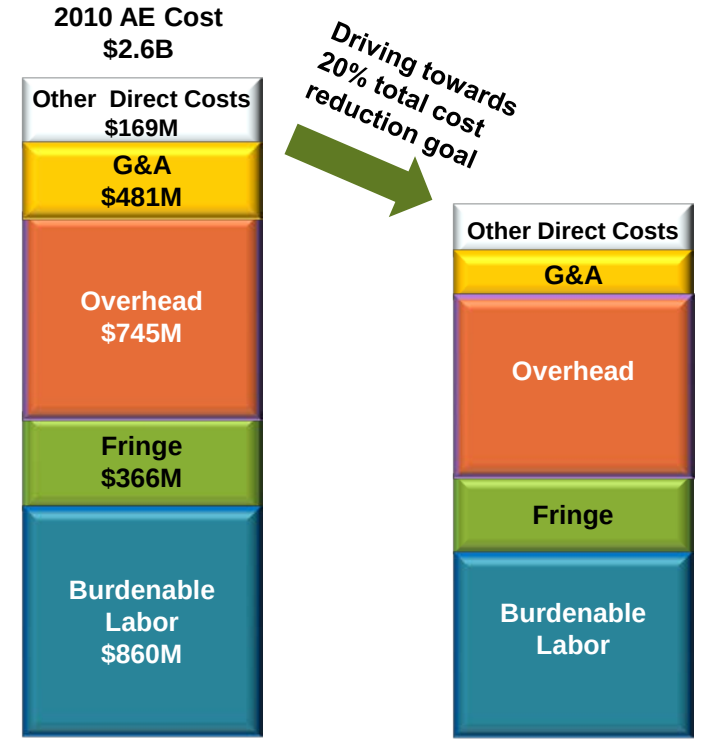
## Foundational Elements . . . *Getting it right*

| | | |
|---|---|---|
| Standardization | Joint Governance | Cost and Service Orientation |
| Service Levels and Measurement | **Visible Executive Sponsorship & Functional Alignment** | Best Practice Stewardship |
| Organizational Excellence | Commercial Orientation "Run it like a Business" | Timely Communication and Attention to Managing Change |

## Differentiators . . . *Taking it to the Next Level*

| | | |
|---|---|---|
| Broad Multi-Functional, Global Scope | Focus on Re-Skilling For Retained Organizations | Improvement Sequencing |
| Transparency to Business Case Realization | **Business Outcomes Focus Beyond Just Administrative Costs** | Global End to End Process Ownership |
| Aggressive Alternative Delivery Mechanisms | Aggressive Use of Enabling Technologies | Transformation Beyond the "Four Walls" |

# Cost Savings Remain a Primary Reason to Move Up the Maturity Curve




**Cost Reduction Levers**

- AE Organization Transformation
- ITS Transformation
- Product Affordability
- Design Escapes
- Engineering Productivity through Technology
- Post –Design Engineering Efficiency
- Reuse – Design/Parts
- New Business Models (Strategic)

Example - Major Defense Contractor a Level 3 Maturity With Targeted Savings of 20%

**While significant cost reductions were a major driver and ultimate result of the endeavor, major non-quantitative benefits were also sought, including:**

- 1st time technical quality
- Cost competitiveness and affordability
- Utilize full technology breadth
- Increase agility
- Empower personnel

KPMG

# Other Illustrative Examples from Client Organizations

- Global Retailer. CIO promoted to Chief Administrative Officer with responsibility for Shared Services, IT, and Process Innovation. Targeting Level 5 maturity, >10% SG&A cost reduction.
- Oil and Gas Major. Targeting Level 4 maturity. Reported >20% savings, largely from IT integration into GBS.
- Global CPG Company. Consolidated IT and GBS organizations, reporting to the CEO. Widely recognized as operating at Level 5 of the maturity curve. Reported >$800M savings from GBS initiatives.
- Global Logistics Company. Moving Level 4 maturity. GBS and IT reporting to the CIO. Target savings >15% from baseline cost structure.



KPMG

# The Benefits Extend to Themes Beyond Cost Savings

| *Theme* | **Benefit** |
|---|---|
| Better Customer Experience | Consistent approach to identifying & responding to voice of customer; single point of contact & accountability; common customer experience; consistent culture and approach to customer service |
| Governance & Sponsorship | Elevated decision and ownership (e.g., operating company Presidents rather than functional representatives) |
| Talent Management | Enhanced stature to attract & retain best people with both operational and commercial skills; scale to focus on employee development and rewards programs |
| Global Service Delivery Scale | Greater scale to facilitate offshore service model deployment and attraction of Tier 1 external service providers |
| Technology | Common tools and approaches (e.g., service -oriented architecture) and greater integration of technology into business processes |
| Infrastructure | Center infrastructure (e.g., building, network design, call center hardware & software, imaging hardware, data storage, DRP) |
| Process & Service Management & Expertise | Cross-functional process management; formal quality management and continuous improvement (e.g., Lean Sigma); common service level management; shared expertise (e.g., transition mgmt.); knowledge management |
| Business Requirements Flexibility | More rapid and cohesive response to major business changes such as acquisitions and divestitures |
| Impact & Access to Capital | Increased relevance and importance of shared services; improved ability to identify improvement synergies and prioritize investments |



KPMG

# Hot Topics in Outsourcing: Demystifying Cloud Computing

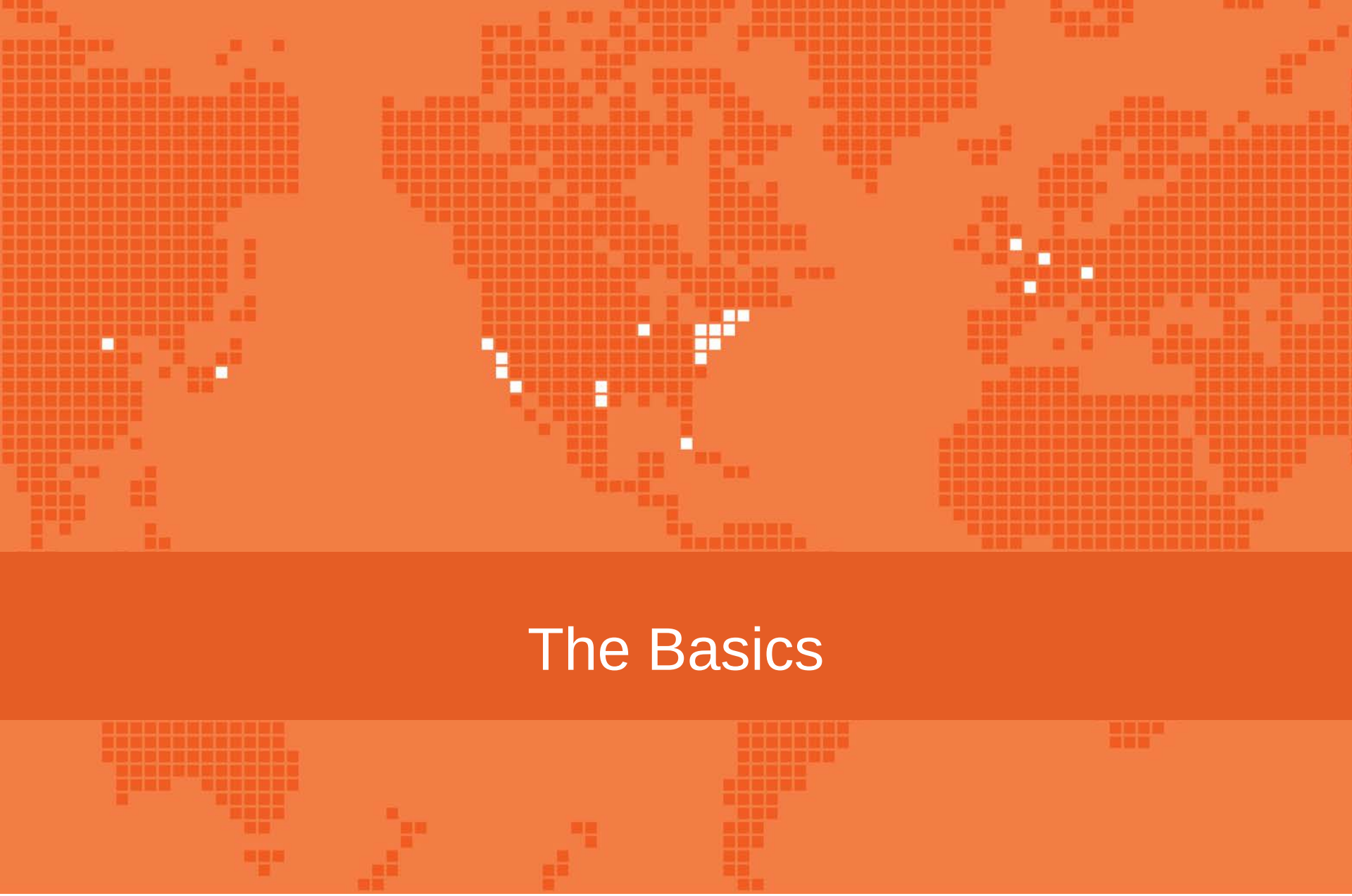




Morgan Lewis

# An Overview

- The Basics
- Security and the Cloud
- Focus on Data
- Other Key Contract Considerations



# The Basics

# Defining “Cloud Computing”

**From the National Institute of Standards and Technology (NIST)**

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. This Cloud model is composed of:

- five essential characteristics
- three service models
- four deployment models

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pd

# Defining “Cloud Computing”

**From SearchCloudComputing**

A Cloud service has three distinct characteristics that differentiate it from traditional hosting.

1. It is sold on demand, typically by the minute or the hour;
2. It is elastic — a user can have as much or as little of a service as they want at any given time;
3. Service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access).

# Essential Characteristics (NIST)

## On-Demand Self Service

- A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

## Broad Network Access

- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

## Resource Pooling

- The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

## Rapid Elasticity

- Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

## Measured Service

- Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

# Service Models (NIST)

## Software as a Service (SaaS)

- The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

## Platform as a Service (PaaS)

- The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

## Infrastructure as a Service (IaaS)

- The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

# Deployment Models (NIST)

**Private Cloud**

- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

**Community Cloud**

- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

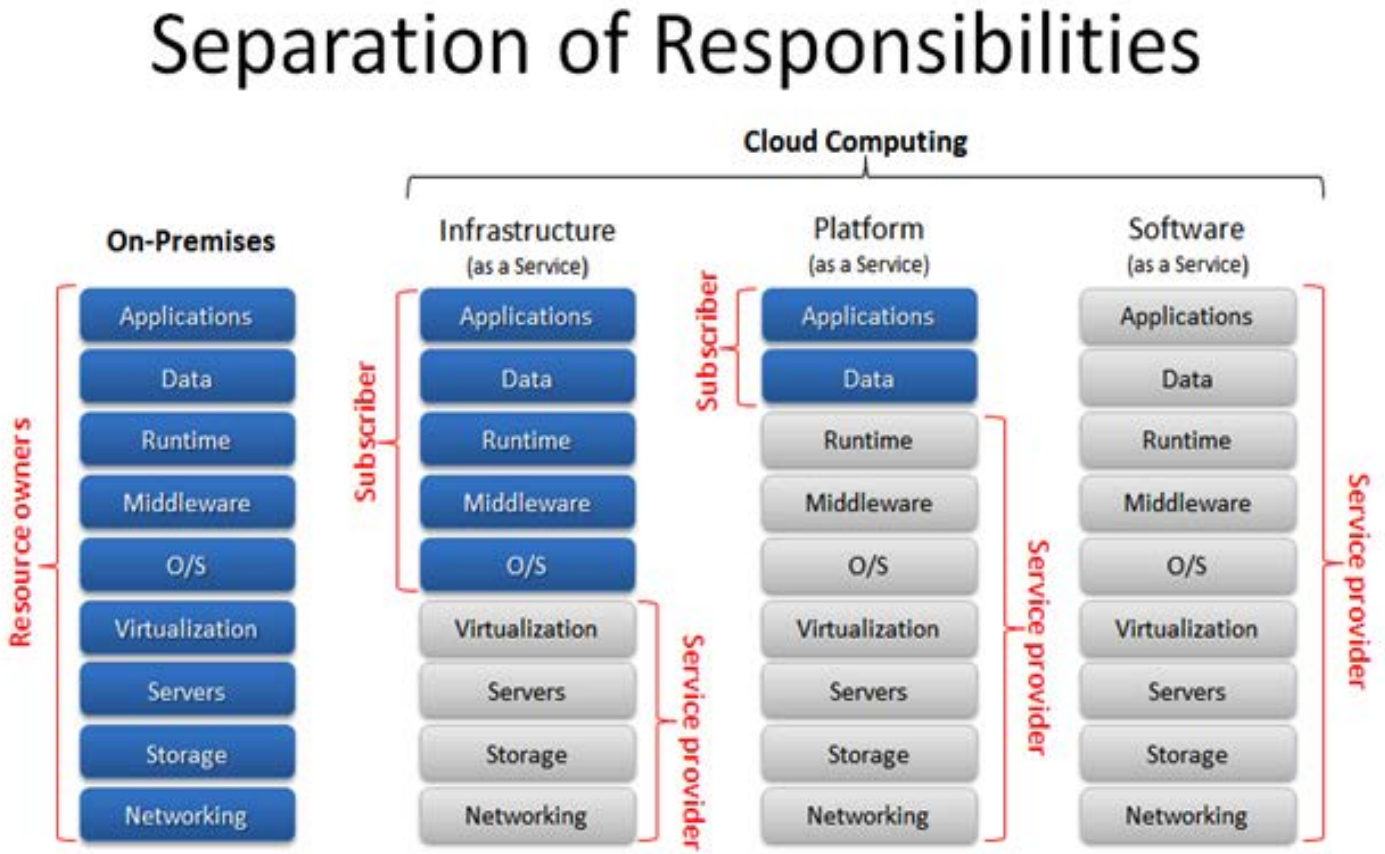
**Public Cloud**

- The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the Cloud provider.

**Hybrid Cloud**

- The Cloud infrastructure is a composition of two or more distinct Cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load balancing between Clouds).

# Service Delivery Models



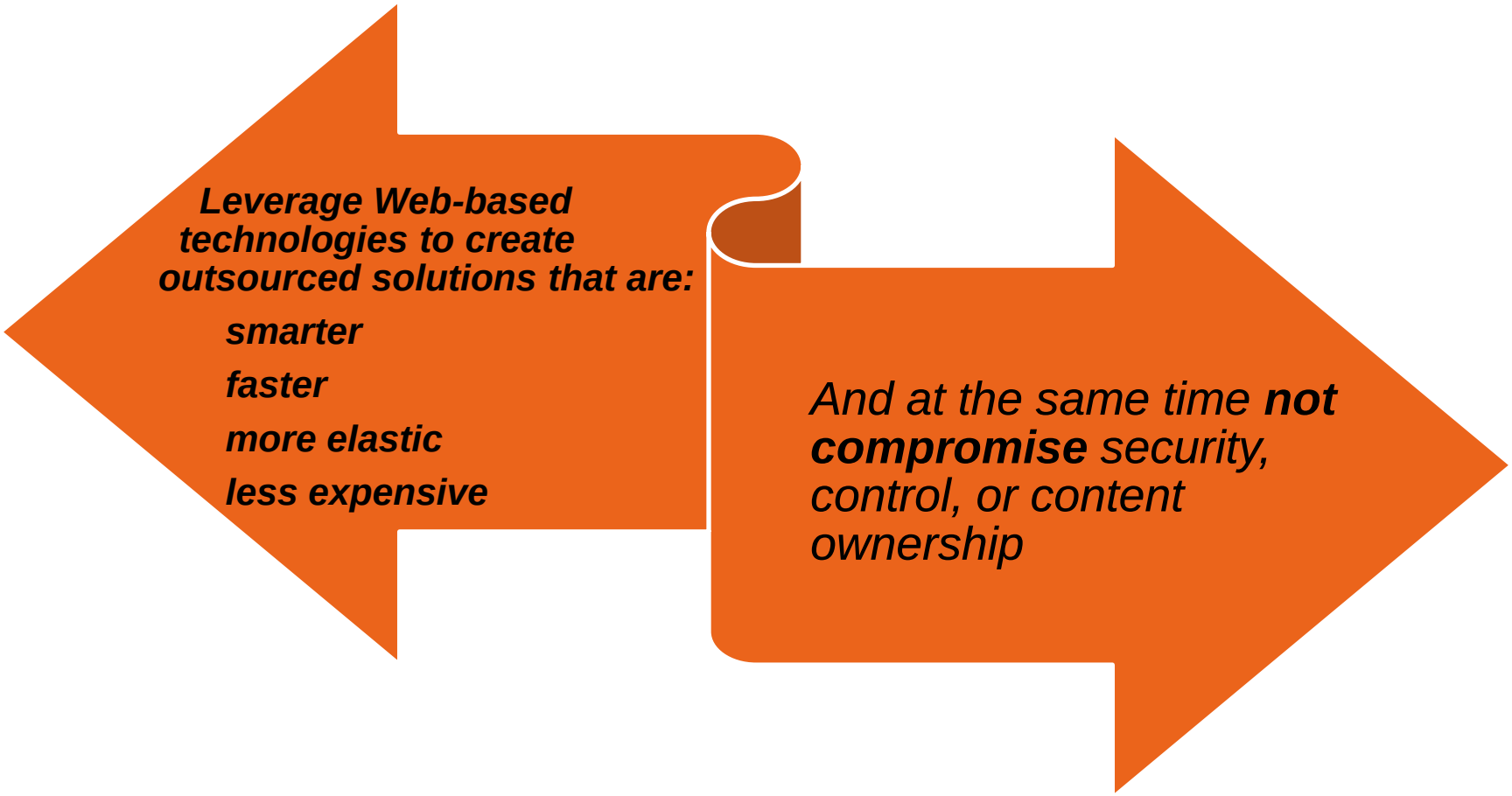

http://blogs.technet.com/cfs-filesystemfile.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-62-43-metablogapi/8551.image_5F00_12.png

# Market Drivers

- Technology innovations
- Improved access to high-speed Internet
- Cost savings
- Flexibility
- Minimized capital investment

# Security and the Cloud

# The Conundrum in What Outsourcing Customers Want …



# Can You Have It All …

- It may depend upon:
  - ✓ Solution
    - *Private vs. public (or hybrid)*
    - *Functional requirements*
    - *Security controls*
  - ✓ Appetite and readiness for change
  - ✓ Appetite and readiness (and ability) to let go of control
  - ✓ Data being processed/accessed
  - ✓ Contract

# Security and the Cloud – Key Considerations

## Understand the what, where, who, and how

- ✓ **What** is the security offering vs. **What** are the security requirements?
- ✓ **What** types of data will be processed/hosted?
  - Personal information, PCI, business sensitive information
- ✓ **Where** are the services being provided from?
- ✓ **Who** is providing the services?
- ✓ **How** is data segregated and used?
  - May vary by environment (production, DR, backup, archive)

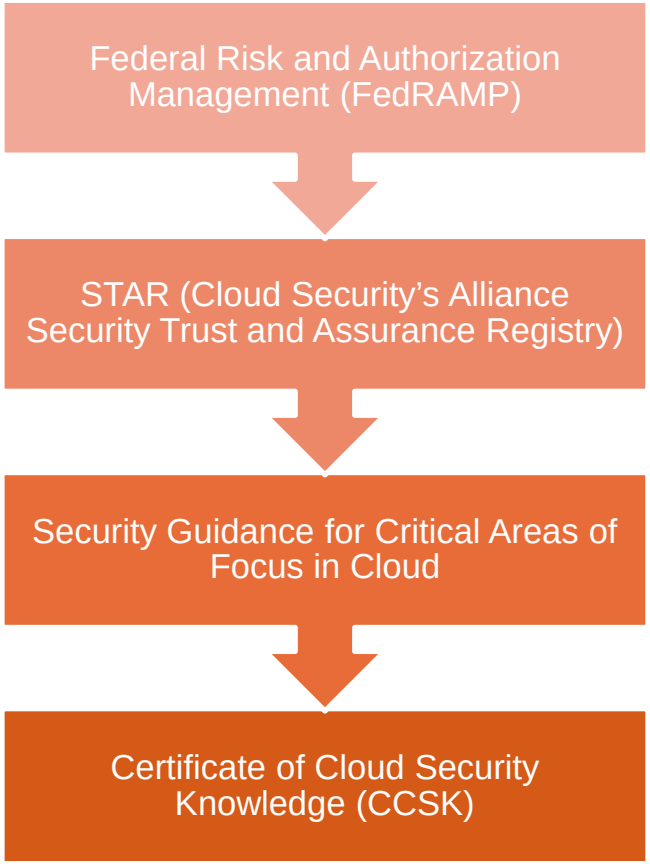
Work with Security, Audit, Risk, DR, Compliance

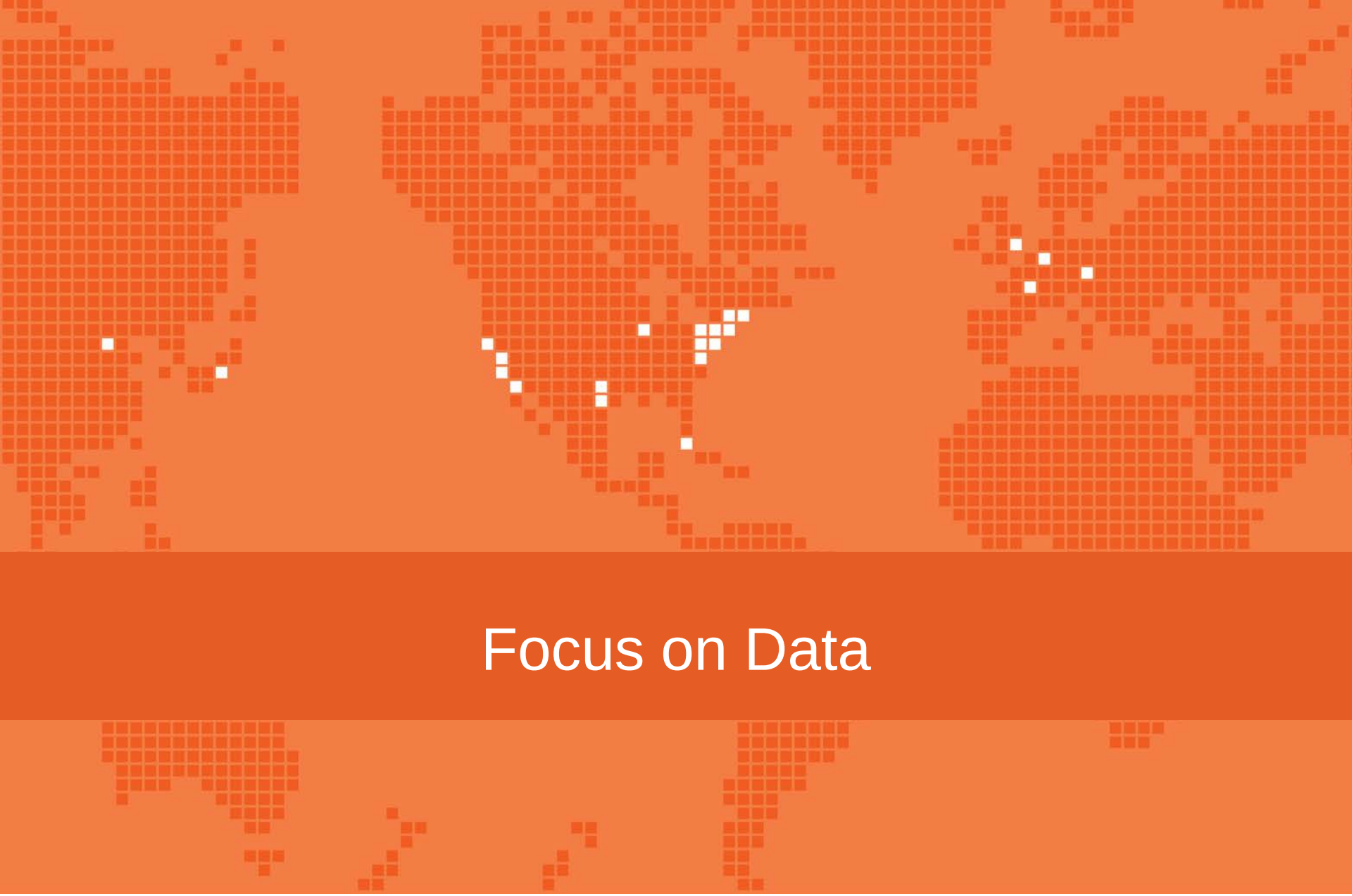
# Security and the Cloud – The Contract

- Security requirements
  - Compliance with internal vs. provider policies – can they be aligned? What is incorporated into the contract?
    - *Starting point*
    - *Bridging the gaps for signing and after*
    - *Hybrid security solution?*
  - Acceptable use policies
    - *What are they?*
    - *Surveillance rights*
    - *Beware of standardized/generic terms incorporated by reference*

# Compliance Issues

- Compliance
  - Internal requirements
  - External standards
    - *ISO*
    - *SSAE16*
    - *PCI*
      - Is provider certification enough? Customer controls still required (point-to-point encryption; tokenization)
    - *Cloud standards??*





# Focus on Data

# The Top Risk Factors

- Data Security
- Data Retention (and Comingling)
- Data “Purge-ability”
- Data Access (and Audit)
- Data Ownership

# Focus on “Data”

## Data segregation

- How is the data segregated?
- Check production and other environments
- Can you get it back (and at what cost?)
- Think about discovery implications
- Can you purge?

## Data and software backup

- How and how often?
- Where and on what type of media?
- Regular delivery?

## Access and audit

- Right to access data
- Right to audit/perform reviews
- Quality/compliance certifications
- Costs

## Ownership and Right to Use

- Software
- Data and content
- Reports
- Performance data
- Data analytics

# Other Key Contract Considerations

# Handling Change

- **Balancing** control and benefits of a leveraged model
- Right to change security requirements
  - Transparency —Will you know?
  - Notice and/or approval
- Customer vs. provider required change
  - Mandatory vs. discretionary
  - Can the systems be partitioned?
- Currency requirements
  - Update requirements (good and bad)
  - Downtime

# Handling Change

- Examples of changes that can be made without approval
  - Changes that do not materially adversely impact the customer, the end users, and the services
  - Changes that do not result in security risk, noncompliance with laws, or additional costs to customer
  - Changes that are consistent with industry standard?
- Examples of when provider pays for change
  - Change to compliance with law?
  - Change made across multiple customers?
  - Change necessary to stay current?
  - Note: Customization may = $$

# Service Locations and Personnel

- Service locations
  - Need to know where your data is
  - Primary and backup
  - Right to change
- Personnel
  - Background checks??
  - Training; certifications
  - Right to subcontract

# Compliance with Law Issues

- Compliance
  - With laws, regulations, and “guidance”
    - *US and beyond*
    - *Now and changes*
  - Industry regulations (financial, insurance, pharmaceutical)
  - Import and export issues
    - *Focus on location of servers and personnel*

# And finally …

- Liability
  - Data breaches
  - Service outage
- Termination
  - When and by whom?
  - Right to suspend services?
- Unwinding the arrangement

# What It Means for the Contract

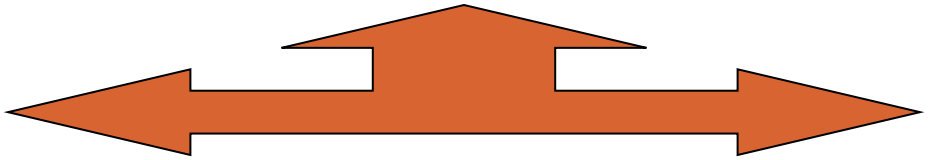
- Is it really different from what we have been doing in outsourcing deals?
  - Same issues
  - Shift in the paradigm
- Can the customer create negotiating leverage?
- Finding a solution that works

# Moving Data Across Borders for Outsourcing Purposes

# Consider U.S. Export Control Laws

- **Goods**
- **Services**
- **Technology / Technical Data**

**To**



**U.S. Person in Foreign Country**

**Foreign Person in Foreign Country**

**Foreign Person in United States**

# Technology / Technical Data

**Information required for:**

- ☑ Design or Development
- ☑ Production, Manufacture, or Assembly
- ☑ Operation
- ☑ Repair, Testing, or Maintenance
- ☑ Modification of Products

**In the form of Blueprints, Drawings, Plans, Photos, Instructions, or Documentation**

# Technology / Technical Data

- **Does <u>not</u> include:**

  Information that is in the Public Domain, i.e.:

  - ☑ ***Information that is <u>generally</u> accessible to the "interested"* public in any form <u>or</u>**
  - ☑ **Information that is available at a public library <u>or</u>**
  - ☑ **Information that is available through unlimited distribution at a conference**

# Technology / Technical Data

- **Also does not include:**
  - ☑ Published patents or
  - ☑ General scientific, mathematical, or engineering principles taught at universities or
  - ☑ "Fundamental research" — **CAREFUL!**

# Multiple
# Export Control Regimes

OFAC & OFACR Controls:

Neutral as to Type of Data

**DDTC & ITAR Controls**

**Exports of**

Military & Space Data

**BIS & EAR Controls**

**Exports of**

Dual Use Data

# U.S. Export Control Laws

- Under U.S. export laws and regulations, the transmission or re-transmission of technical data or technology may be:
  - prohibited or
  - subject to export licensing requirements
- Encryption of technical data or technology does not change this result.

# Export Control

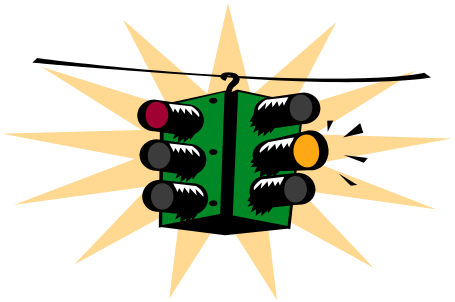
## Jurisdiction?

### DDTC & ITAR

**Prohibitions**
Country?
Recipient?

**Restrictions**
License Required

### OFAC & OFACR



### BIS & EAR

**Prohibitions**
Country?
Recipient?

**Restrictions**
Data?
Recipient?
End Use?
Red Flag?
License Required?

# Export Control Jurisdiction

**AECA/ITAR** versus **EAA/EAR**

1. Different Administering Agencies
2. Different Prohibitions
   - ✓ Countries: 25 versus 5
   - ✓ Data Recipients: 4 lists versus 4 lists
3. Different Restrictions (License Requirements)
   - ✓ Data-Specific: USML versus ECCN
   - ✓ Data Recipients
   - ✓ End Use
4. Different Licensing Analysis

# U.S. Export Controls & Cloud Computing

Moving data across borders for outsourcing purposes often involves “cloud.”

NO definition of “Cloud Computing” provided in the Export Administration Regulations [EAR] or in the International Traffic in Arms Regulations [ITAR] or in OFAC’s various sanctions regulations

# Cloud Computing and ITAR/DDTC

# Cloud Computing and ITAR/DDTC

- DDTC which administers ITAR, has **NOT** provided any formal written guidance on the application of ITAR or DDTC's enforcement policy with respect to export control violation exposure — either for Cloud computing service providers or users

- **We are informally advised that DDTC will strictly apply the ITAR pursuant to its provisions to all aspects of cloud computing and would so informally advise you in any one-on-one interaction that you initiate with DDTC**

# Cloud Computing and ITAR/DDTC

"Export" under ITAR means "sending a defense article out of the U.S. **in any manner.**" ITAR 120.17(a)(1). Defense article includes technical data ITAR 120.6.

Thus, the **de facto** DDTC position for **Cloud User**s appears to be:

- A cloud user may be exposed to an unlicensed export or reexport violation if the Cloud user's ITAR-controlled tech data is sent or transmitted from the U.S. or a third country to Elbonia as part of a Cloud computing computational process initiated by the Cloud user.

# Cloud Computing and ITAR/DDTC

And the **de facto** DDTC position for **Cloud Providers** appears to be that a Cloud provider may be exposed to an ITAR violation of:

- Causing an unlicensed export when the Cloud provider transfers ITAR controlled tech data from a **U.S. server to a foreign server**
- Causing **an unlicensed reexport** when the Cloud provider transfers ITAR controlled tech data from **one foreign server to another foreign server**
- Providing "defense services" without a required authorization if the Cloud computing user is a foreign person
- Making an unlicensed export of ITAR controlled tech data when the Cloud provider provides a **foreign national employee** access to a Cloud user's ITAR controlled tech data

# Cloud Computing and OFAC

# Cloud Computing and OFAC

- OFAC, which administers and enforces various trade sanctions and embargoes, has NOT provided any formal guidance on the application of OFAC's enforcement policy with respect to sanctions violation exposure — either for Cloud providers or Cloud users

- OFAC's likely concern would be that no blocked person or SDN receives Cloud computing services from a U.S. Cloud provider and that such services are not provided to any person in certain countries, i.e., services to Syria.

# Cloud Computing and EAR / BIS

# Cloud Computing and EAR / BIS

- Unlike DDTC and OFAC, BIS has formally addressed the export control implications of cloud computing by issuing two written advisory opinions
- BIS advisory opinion guidance applies only to facts discussed in the advisory opinions
- BIS advisory opinions interpret EAR but do not change EAR
- BIS advisory opinions address only Cloud providers – they do not address Cloud users
- BIS position cannot be assumed to be applicable by analogy to enforcement policies or actions by DDTC/ITAR or OFAC or any other USG agency

# Cloud Computing and BIS

- BIS issued **Advisory Opinion # 1** on January 13, 2009 [AO#1] with respect to five specific cloud computing questions that were posed to BIS by a U.S.-based Cloud computing service provider

- www.bis.doc.gov/policiesandregulations/advisoryopinions.htm

# Cloud Computing and BIS
## Advisory Opinion # 1

- BIS found that the user of the Cloud computing services is the Principal Party in Interest and thus the user of the services is the "exporter"

- Thus the Cloud service provider is not the Principal Party in Interest and is therefore not the exporter

# Cloud Computing and BIS
## Advisory Opinion # 2

- BIS issued **Advisory Opinion # 2** on January 11, 2011 [AO#2] with respect to **deemed export question** posed to BIS by a U.S.-based Cloud computing service provider

- **Question 1** - Does the EAR require Cloud computing service providers to obtain deemed export licenses for foreign national IT administrators/employees who service and maintain the provider's Cloud computing systems?

# Cloud Computing and BIS
## Advisory Opinion # 2

- The Cloud computing service provider is not an "exporter"

- Because the Cloud computing service provider is not an "exporter," it would NOT be making a deemed export if a foreign national network administrator/employee monitored or screened, as presented in the scenario, user-generated technology subject to the EAR

# Cloud Computing and BIS
## Advisory Opinions #1 and #2

- BIS AO #1 & #2 do NOT squarely address export control issues that arise from the service users' activities

- **Example A:** U.S.-based user accesses its Cloud service and performs a computational function with its own EAR-controlled technology or information, and a server or some software needed for the computation and provided through the Cloud is located in Elbonia

# Cloud Computing and BIS
## Advisory Opinions #1 and #2

- **In Example A,** User has made an (unknowing) export to Elbonia for which a BIS license may have been required

- Accordingly, notwithstanding BIS AO #1 & 2, **users** of Cloud computing services need to evaluate their usage in light of their risk for inadvertently being exporters of EAR-controlled technology and take reasonable precautions

# Observations and Recommendations for Consideration

# Observations for Cloud Service Providers

- Determine whether your services and activities established by BIS AO #1 & 2 are addressed
- **Caution:** Provider may actually export its own technology or software that is subject to the EAR and thus may require an export license – e.g., to set up, maintain, and troubleshoot the service on overseas servers
- Determine if your customer users are involved with **ITAR-controlled tech data** transmissions and computations – if so, AO #1&2 will NOT be relevant

# Observations for Cloud Service Providers

- Screen all customer-users against SDN and other prohibited parties lists
- Preclude access to service from OFAC-sanctioned countries and blocked parties
- Be careful of terminating relationship and ensure against tangible media return of Cloud user's technology – approach like "routed transaction"
- Provide U.S.-ONLY location and no foreign person employee Cloud services as a possible option as may be requested by users, e.g., ITAR tech data involved

# Observations for Cloud Users

- Cloud computing usage requires export control compliance procedures and coverage in your export manual
- Export compliance officer MUST clearly comprehend export control consequences if user places export-controlled tech data and/or technology and/or information in the Cloud for operational or computational functions – i.e., exactly what will be uploaded or downloaded

# Observations for Cloud Users

- Users should scrutinize and closely read their Cloud computing service provider's contract and consider how, through/to whom, and physically where the user's tech data and/or technology and/or information will be transmitted and stored
  - Where are Cloud provider's servers located?
  - Does Cloud provider transfer data to servers in other countries during peak or off-times?
  - Will Cloud provider employ foreign nationals to work on "Cloud user's account"?

# Observations for Cloud Users

- Users should consider contractual requirement that no non-U.S. location for Cloud server will be involved with user's account where user has ITAR-controlled tech data
- Users should consider contractual requirement that no non–expressly specified location for Cloud server, etc. will be involved for user's account for EAR-controlled technology [countries for which user clearly knows that its EAR-controlled technology is NLR to such countries]

# Observations for Cloud Users

- Seek contract language with provider that no unlicensed foreign national IT administrator and/or employee of service provider will access user's export-controlled tech data and/or technology and/or information

- Limit Cloud usage to only data/software that are EAR 99

# Observations for Cloud Users

- Determine which particular countries your tech data and/or technology and/or information may be transmitted to or through or in and/or stored by the Cloud computing service provider, and then apply for the relevant export or reexport licenses before using the Cloud service
- Apply for export license if required
- **Encrypting your data is irrelevant for export licensing analysis!**

# Closing

- Cloud computing presents complex export control challenges

- U.S. export regulations as currently written actually do expose **both users and service providers** to possible export violations, e.g., unlicensed export, aiding/abetting unlicensed export, unlicensed defense service.

# Closing

- While BIS has provided two Advisory Opinions regarding EAR applicability to Cloud computing service providers, DDTC and OFAC have not provided any public written guidance — thus providers are exposed to unlicensed activity under ITAR and OFAC as discussed

- Cloud computing service users must assume that their services that involve foreign-located servers do constitute exports subject to licensing by the relevant export control agency

# Ignorance Is No Excuse

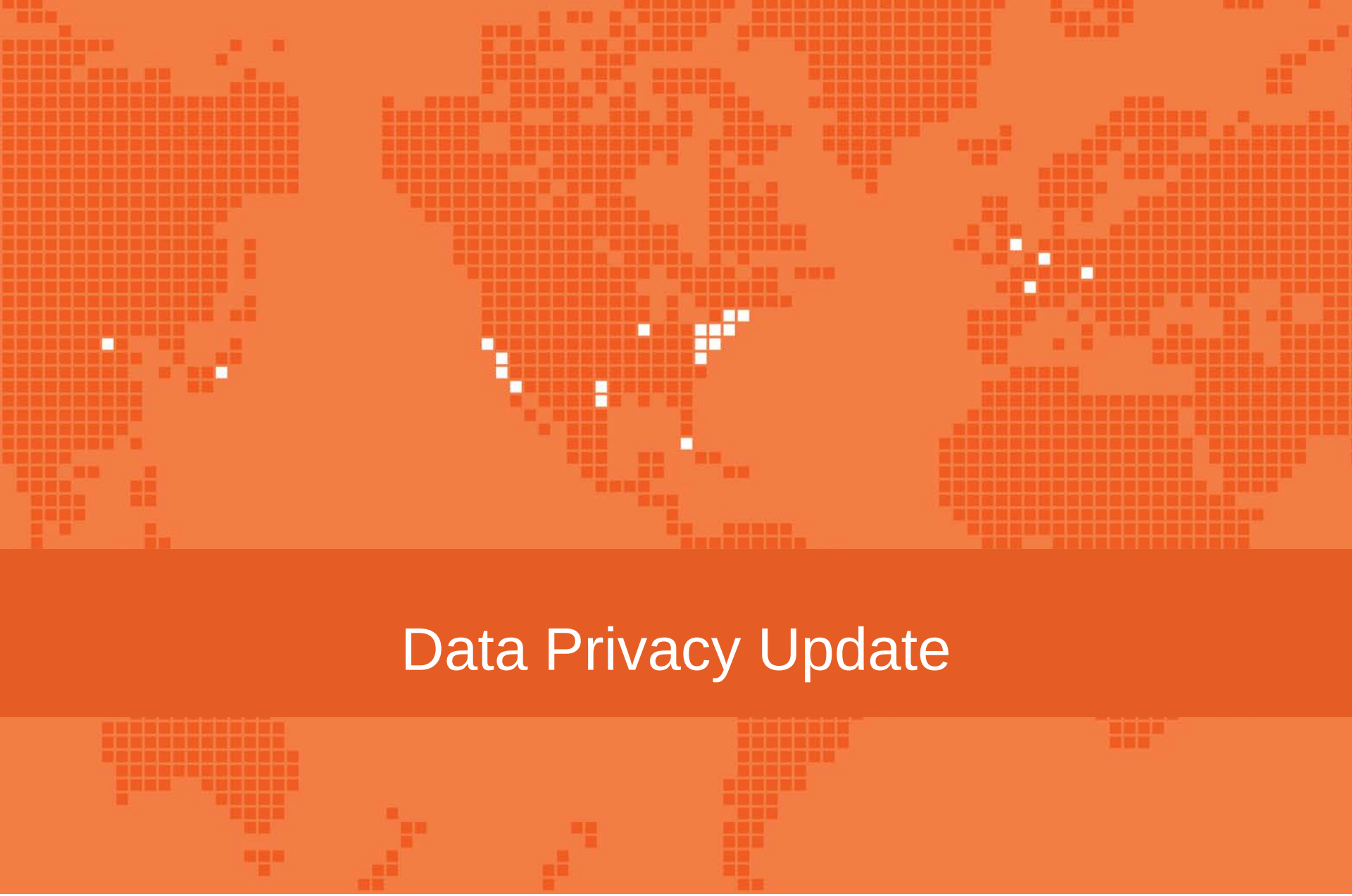
**ITAR, EAR and OFACR apply a standard of "Strict Liability" in assessing violations!**

**There Is No Margin for Error!**

**Negligent versus Criminal**

# Penalties for Violations

- **EAR civil violations can lead to a civil monetary penalty of $250,000 per violation**
- **ITAR civil violations can lead to a civil monetary penalty of $500,000 per violation**
- **EAR & ITAR criminal violations can lead to debarment/denial and possible imprisonment**



# Data Privacy Update

# Data Privacy Update

- Upcoming and recent changes in the regulatory environment
  - New EU Data Protection Regulation (draft issued January 2012; final law anticipated 2014/2015/2016)
  - SEC Disclosure Guidance Relating to Cybersecurity Risks and Cyber Incidents (issued October 2011)
  - Massachusetts Regulations (compliance grace period ended March 1, 2012)
  - SSAE 16 (effective June 2011)

# Overhaul of EU Data Protection Law

- On January 25, 2012, European Commission published proposals for reform of the European Union's data protection laws.
- Current EU Data Protection Directive, implemented in 1995, would be replaced.
- Key reasons for change:
  - Each EU Member State adopted its own law based upon the Directive. New General Data Protection Regulation will be a direct law, applicable to each EU Member States.
  - Single, consistent set of rights and rules.
  - To update the law to meet new challenges for the protection of personal data brought on by technological developments and globalization.

# Timing and Relevancy

- The draft Regulation will be considered and adopted by the European Parliament and the Council of the European Union.
  - Most likely effective two years after adoption (2014/2015/2016?)
  - Subject to amendment during adoption process.
  - However, most commentators expect the key parts of the draft Regulation to survive.

# Scope of the New Regulation

- Like the current Directive, the new Regulation will continue to apply to businesses based in the EU.
- Unlike the current Directive, the new Regulation will apply to businesses based outside of the EU that process the personal data of EU citizens, or monitor the behavior of EU citizens (e.g., by tracking them on the Internet).
- Large number of U.S./other international businesses will be affected.
- With certain exceptions (including businesses with 250 or fewer employees), international entities covered by the Regulation will be obligated to designate a data protection representative in the EU.

# Single Regulator

- Currently, businesses are regulated by each Member State in which they process personal data.

- Under the draft Regulation, businesses will only have to interact with the one regulator in the Member State in which it has its main establishment.

# Data Controllers

- More responsibilities for data controllers (parties that determine the purposes and manner in which personal data is processed)
  - As in the Directive, data controllers have to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.
  - In addition, certain types of processing that present "specific risks" (examples of which are given in the draft Regulation) will require a data protection impact assessment, including seeking the views of data subjects.
  - Additional new requirements described below.

# Data Processors

- New responsibilities for data processors (businesses that process personal data on behalf of data controllers)
  - Under the Directive, the legal obligations fall on the data controllers rather than the data processors.
  - The new Regulation introduces certain obligations that apply to data processors.
  - For example, data processors, like data controllers, will be obligated to maintain documentation of all their processing operations.

# Contracts between Data Controllers and Data Processors

- Processing must be under a contract obligating the data processor in particular to:
  - (a) act only on instructions from the Controller;
  - (b) employ only staff bound by confidentiality obligations;
  - (c) take all security measures required by the Regulation;
  - (d) subcontract only with the prior permission of the Controller;
  - (e) assist the controller in ensuring compliance with its obligations under the Regulation;
  - (f) hand over all processing results to the Controller after the processing and not process other than as authorized; and
  - (g) make available to the controller and the supervisory authority all information necessary to control compliance (e.g., audit rights).

# New Data Breach Notification Requirements

- The draft Regulation introduces data breach notification requirements, which the Directive did not have.
- Under the draft Regulation, data controllers must notify supervisory authorities of a security breach "*without undue delay, and where feasible, not later than 24 hours after having become aware of it.*"
- If notification is not made within 24 hours, a *"reasoned justification"* must be provided.
- In addition, individuals whose data could be adversely affected by the breach should be notified without undue delay in order for them to take necessary precautions.

# Individual Consents in the New Regulation

- Under the draft Regulation, in order to be lawful, personal data must be processed on the basis of the consent of the individual *"or some other legitimate basis, laid down by law."*
- Principle of Transparency – clear, plain language.
- Consent by an individual must be a *"clear affirmative action,"* including by ticking a box.
- Silence or inactivity does not constitute consent.
- Data controller bears the burden of proof for the data subject's consent.
- Where individual has no real choice to refuse or withdraw consent, or where there is a clear imbalance of power between the data subject and the controller, then consent does not provide a lawful ground to process.

# New Rights of Individual Data Subjects

- "Right to be Forgotten" and Erased. Individuals will have the right, at their request, to have their data no longer processed and erased.
- Right to Data Portability. Individuals will have the right to obtain a copy of their data and to have it transmitted to another provider.
  - For example, from one social network to another
  - Service providers have raised issues regarding feasibility of compliance, including format and compatibility issues and security risks during transmission.

# International Transfer of Personal Data

- Like the Directive, the draft Regulation governs the international transfer of personal data from the EU.
- Like the Directive, transfer allowed to a country that the European Commission has decided ensures "*an adequate level of protection*."
  - Transfers of personal data from any EU Member State to these countries may take place without further authorization
  - No express mention of the safe harbor, but expected to continue to be applicable

# International Transfer of Personal Data

- Where EC has not decided that a country ensures an adequate level of protection, transfer may only be made where "*appropriate safeguards*" have been set out in a "*legally binding instrument*," which include:
  - The EC's standard data protection clauses;
  - Standard or specific contractual clauses adopted or authorized by a supervisory authority in an EU Member State; and
  - Binding corporate rules (BCRs).
- Where no such appropriate safeguards are used, transfer is allowed only with prior authorization by a supervisory authority.

# Binding Corporate Rules

- Binding Corporate Rules (BCRs) are legally binding policies and rules for international transfers of personal data by a corporate group. Binding both within the corporate group and outside of the group – i.e., provide rights and remedies to data subjects.
- Once approved, personal data may thereafter be transferred anywhere within that affiliated group in accordance with the BCRs.
- To date, not used much because BCRs have to be approved by each of the applicable EU Member States.
- Under the new Regulation, BCRs will need to be approved by a single Supervisory Authority and are likely to become a more widely used solution.

# Higher Fines

- For example, in the UK, the current maximum fine for breach of the UK Data Protection Act 1998 is £500,000.

- The draft Regulation provides for much higher penalties for noncompliance – up to £1,000,000 or, for “enterprises,” up to 2% of annual worldwide revenues.

# SEC Disclosure Guidance

- October 2011: SEC's Division of Corporate Finance published Guidance on the Disclosure by Public Companies of Cybersecurity Risks and Cyber Incidents.
- Not a Rule or Regulation.
- Intended to assist public companies in preparing disclosures required in registration statements under the '33 Act, periodic reports under the '34 Act and other filings required by law.

# General Guidance on Disclosure of Cybersecurity Risks

- General guidance is that cybersecurity risks must be disclosed in a manner consistent with the disclosure of any other operational or financial risk – material information must be disclosed.
- Would a reasonable investor consider it important in making an investment decision?
- Cybersecurity risks must be disclosed if the risk is among the most significant factors that make an investment in the company risky or speculative.

# Specific Considerations for Disclosure of Cybersecurity Risks

- Companies must consider the probability of cyber incidents.
- Both vulnerability to third-party actors and events (e.g., hacker attacks and viruses) as well as the potential for inadvertent disclosure of confidential information by the company and others (e.g., outsourcing service providers).
- Also, the adequacy of preventive actions taken in the context of the industry in which the company operates and the prevailing risks in the industry, including threatened or actual attacks of which it is aware.

# Specific Considerations for Disclosure of Cybersecurity Risks

- If company outsources functions that have material cybersecurity risks
- If cybersecurity related costs materially impact operating results (both before and following an incident)

# What Not to Do

- Do not make generic disclosures.
- Do not make disclosures that compromise a company's security – do not give a "roadmap" to the company's weaknesses.

# Disclosure of Incidents and Consequences

- If an incident occurs that results in material costs or consequences or that may show potential for future incidents, it must be disclosed.
  - Material remediation costs.
  - Materially increased prevention efforts and costs.
  - Loss of material business.
  - Material incentives to customers to keep business.
  - Material litigation.

# Disclosure of Incidents and Consequences

- Significant incidents may require current reporting on Form 8-K or a press release.

- Effect on future disclosures of cybersecurity risks now that an incident has actually occurred.

# Post-Issuance Disclosures

- Following the Guidance, disclosures have not been forthcoming in many cases
  - Several companies known to have experienced major security breaches have not mentioned the incidents in subsequent regulatory filings – companies did not view as "material"?
  - Many companies: while descriptions may be longer, still generic in nature

# Disclosure by Global Payments

- Processor of card payments suffered data breach – credit and debit card information of up to 1.5 million accounts were exported by hackers.
- Says incident occurred in early March 2012.
- Described the breach in Form 8-K filed Friday, March 30, then issued press release statement on Sunday evening, April 1 — data breach affected “fewer than 1.5 million” accounts and the impact was contained to North America.
- Consequence: Visa dropped Global Payments from its registry of service providers that meet data security standards.

# Disclosure by Global Payments

- Global Payments April 2, 10-Q: Highlights
  - We announced an unauthorized access into OUR processing system…we believe that the affected portion…is confined to North America and less than 1,500,000 card numbers may have been exported… but that cardholder names, addresses and social security numbers were not obtained by the criminals. Based on our forensic analysis to date…we believe that this incident is contained.
  - Visa has removed us from Visa's published list of PCI-DSS compliant service . . .
  - Because we are in the early stages of our investigation, we cannot reasonably estimate the amount or range of any potential losses related to this incident…Any such losses could be material and may adversely impact our results of operations.
  - We have insurance that we believe may cover certain costs and losses . . . but we have not yet confirmed coverage.

# Disclosure by Global Payments

- Global Payments April 2, 10-Q: Highlights
  - Computer malware, viruses and hacking attacks have become more prevalent in our industry, have occurred on our systems in the past, and may occur on our systems in the future. For example, recently we announced . . .
  - Risks of this and other security breaches – include reputational harm, increased operating expenses, regulatory scrutiny, and adverse effects on card network registration and financial institution sponsorship.
  - Despite our efforts . . . it is possible that we may not be able to anticipate or to implement effective preventive measures against all security breaches of these types, especially because the techniques used change frequently or are not recognized until launched . . .

# Massachusetts Data Security Regulations

- Regulations effective March 1, 2010.
- Grace period ended March 1, 2012 for companies to obligate compliance by their third-party service providers by contract.
- Regulations applicable to companies, wherever located, that own, license, store, or maintain "personal information" of MA residents, including customers and employees.
- Not just Massachusetts companies.
- "Personal information" means first initial/name and last name, in combination with another important data element such as SSN, driver's license number or credit card or bank account number.

# Massachusetts Data Security Regulations

- Key requirements:
  - Adopt a Comprehensive Written Information Security Program (for both paper and electronic information)
    - *Detailed list of required contents*
    - *For many companies, memorializing existing process and enhancing administrative discipline*
  - Encrypt personal information of MA residents that is:
    - *On portable devices (e.g., smartphones, laptops)*
    - *Stored in portable media (e.g., memory sticks, DVDs)*
    - *Transmitted over a public or wireless network*
- Similar to laws in effect in other states including CA, CT, NV

# Massachusetts Data Security Regulations

- Companies subject to the MA Regulations must take reasonable steps to ensure that their third-party service providers that have access to personal information of a MA resident will comply with the Regulations.
- Contracts with third-party service providers must require compliance with the MA Regulations.
  - Compliance grace period ended March 1, 2012.

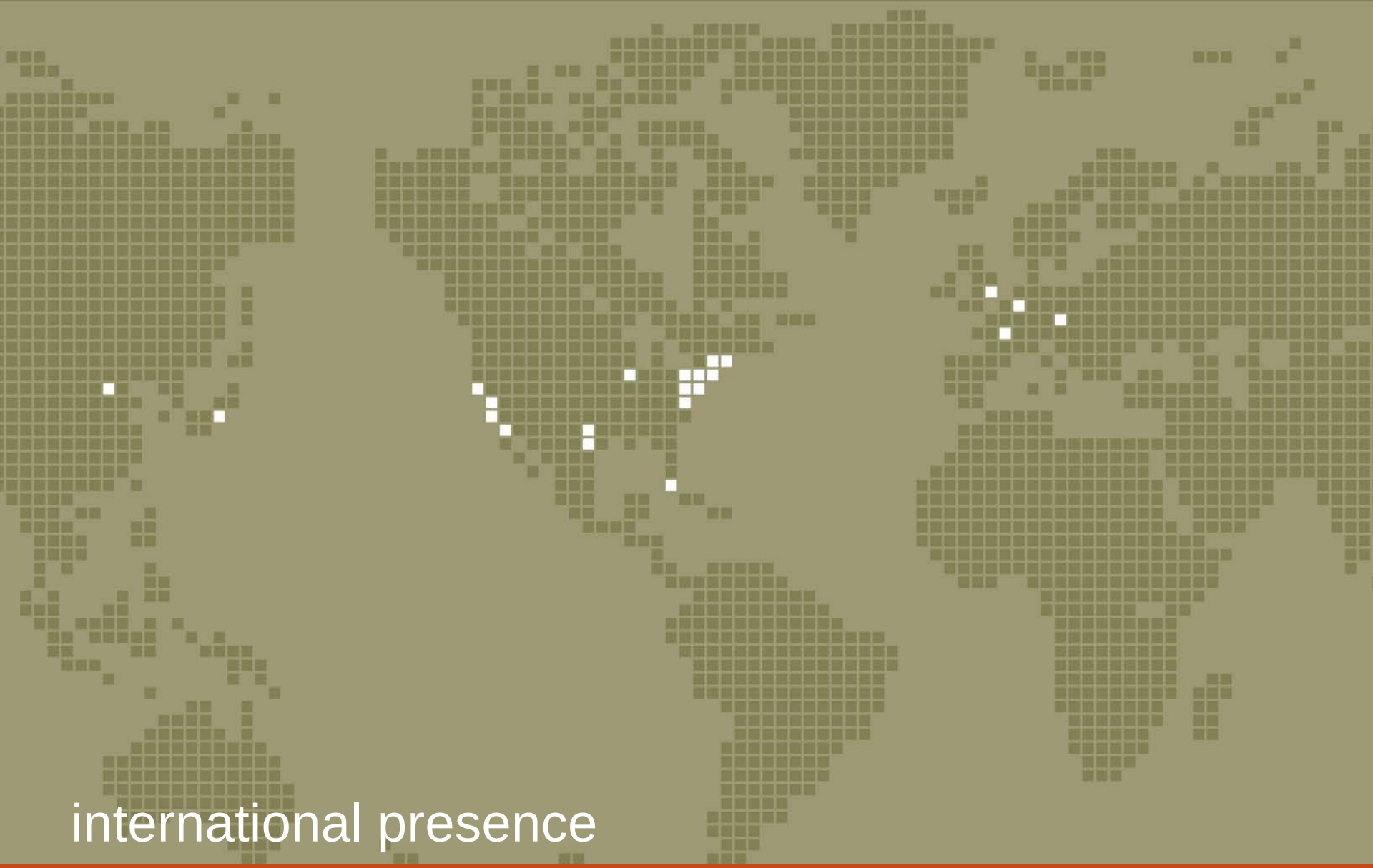
# Practice Points

- Confirm that contracts with third-party service providers that receive, store, maintain, or process personal information of a MA resident are required to protect it as required by the MA Regulations.
  - Language can be simple – e.g., that the vendor is required to comply with applicable Laws (and new or modified Laws), and that the MA Regulations are covered by the definition of “Laws”
  - Right to audit the vendor’s compliance (including the right to receive a copy of the vendor’s written security program)
  - Requirement that the vendor return or destroy all personal information upon termination
  - Requirement to provide prompt notification of breach

# SSAE 16

- SSAE 16 replaced SAS 70 as the relevant audit standard in the U.S. as of June 15, 2011.
  - SSAE 16 = Statement on Standards for Attestation Engagements No. 16, Reporting and Controls at a Service Organization, promulgated by Auditing Standards Board of the American Institute of Certified Public Accountants.
- Reminder to update older agreements – Vendor may (should) already be in compliance.
  - Instead of SAS 70 Type II, now SSAE 16 SOC 1, Type 2 (ISAE 3402 is the international standard).
  - Key difference: Vendor's systems and controls evaluated over the entire period covered by the audit, not just a specific date.

# Thank you



# international presence

Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston Irvine
London Los Angeles Miami New York Palo Alto Paris Philadelphia Pittsburgh
Princeton San Francisco Tokyo Washington Wilmington