



Introduction

Please note that any advice contained in this presentation is not intended or written to be used, and should not be used, as legal advice.

Agenda

- Introduction
- Cloud Solutions: The top technology trend. How are Customers and Vendors mitigating the risks? (*Michael Pillion*)
- “Right” Sourcing: The analysts are heralding a wave of onshoring. How are companies building flexibility into their contracts to enable “right” sourcing of their onshoring and offshoring mix? (*Vito Petretti*)
- Service Integration: What it means and how it is impacting the IT outsourcing contract. (*Barbara Melby*)
- Wrap-up and CLE information

Participants



Michael Pillion

Partner
Morgan Lewis
P: 215.963.5554
E: mpillion@morganlewis.com



Vito Petretti

Partner
Morgan Lewis
P: 212.309.6755
E: vpetretti@morganlewis.com



Barbara Melby

Partner
Morgan Lewis
P: 215.963.5053
E: bmelby@morganlewis.com



Cloud Solutions: The top technology trend. How are Customers and Vendors mitigating the risks?

An Overview

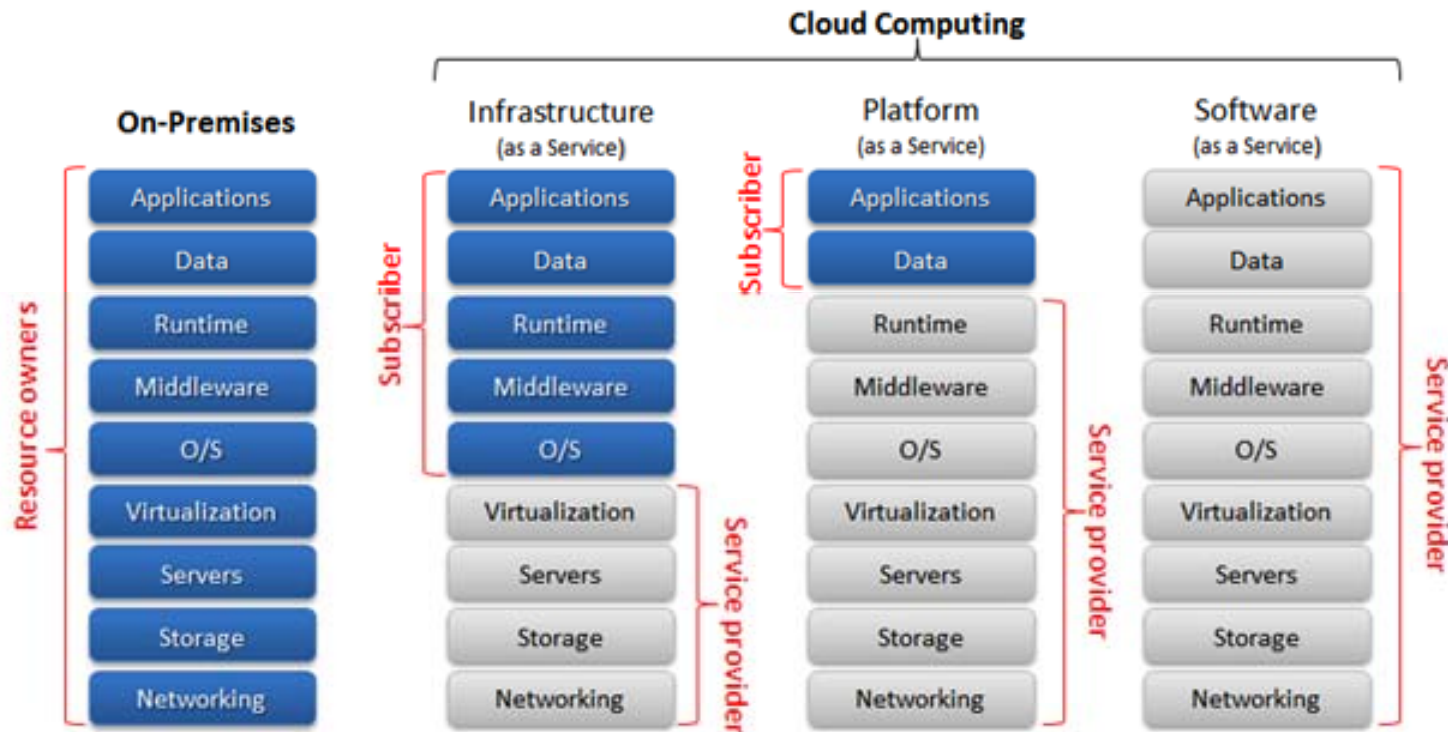
- ❑ Cloud Basics
- ❑ Business Drivers and Benefits of the Cloud
- ❑ Key Risks and Trade-Offs of the Cloud
- ❑ Key Contract Positions and Negotiation Strategies

Cloud Service Delivery Models

- Infrastructure as a Service (IaaS)
 - Provider manages infrastructure
 - Users include network architects
 - Storage, servers, etc.
- Platform as a Service (PaaS)
 - Provider manages infrastructure, operating system, and middleware, enabling Customer to deploy its own applications
 - Users include application developers
 - Web servers, databases, development tools
- Software as a Service (SaaS)
 - Provider manages everything from infrastructure to middleware to applications
 - Users include end users
 - CRM, social media, email, virtual desktop

Cloud Service Delivery Models

Separation of Responsibilities



Common Examples of Cloud Delivery Models

- IaaS
 - Amazon Web Services
 - Rackspace
 - HP IaaS Solutions
- PaaS
 - Google App Engine
 - Windows Azure
- SaaS
 - Salesforce
 - Gmail
 - Microsoft Office 365
 - GoTo Meeting

Cloud Deployment Models

- Private Cloud
 - Exclusive use by a single Customer
- Public Cloud
 - Supports multiple Customers
- Community Cloud
 - Exclusive use by defined community of organizations
- Hybrid Cloud
 - Two distinct clouds (Public, Private, or Community) bound together by technology that enables data and application portability between clouds

Business Drivers and Benefits of the Cloud

- Cost savings; minimized capital investment
 - Pay as you go
 - Pay for service; no hardware costs
- Straightforward and faster implementation
- Reduced operational management by Customer
- Flexibility and portability
- Scalability
- Low-cost experimentation
- Vendor's core business is the cloud service
- Customer focus on its core business

Key Risks and Trade-Offs of the Cloud

- Lack of customization – standardized solutions
 - Loss of ability to dictate changes necessary to keep compliant with Customer-specific laws
- Service may change at an inconvenient time (or may not change as fast as desired)
- More exposure to potential threats – big providers as targets
- Loss of control over access, retention and security of data
 - Storing data in the cloud does not relieve Customer organization of the responsibility for protection, management, or retention of data
- Vendor oriented “standard” contracts
 - Policies and other terms incorporated by reference
 - Subject to changes
- Purchase and implementation by business units without IT or legal review

The Conundrum

In What Outsourcing Customers Want ...

Leverage Web-based technologies to create outsourced solutions that are:

smarter

faster

more elastic

less expensive

*And at the same time **not compromise** security and control*

Key Contract Positions and Negotiation Strategies

- Data
 - Ownership and Vendor's use
 - Vendor's data security offering
 - Customer access; Vendor production
 - Data segregation, retention, and return
 - Data breach and response
- Compliance with laws applicable to Customer
- Service availability
 - Uptime and responsiveness SLAs
 - Backup and disaster recovery
- Change management and approval rights
 - Vendor Initiated
 - Customer Initiated
- Unwinding the Deal

What Contract Protections of Data are Required?

- Customer cannot delegate its security and privacy obligations
- Depends on the particular facts and circumstances of the relevant transaction, taking into account:
 - The sensitivity of the Customer data involved, including whether personal data or other sensitive business information is involved
 - The results of the Customer's due diligence of the Vendor's service solution and Vendor's capability to comply with the Customer's (and its customers') requirements (security, SLAs, etc.)
- Depends on any specific legal requirements and guidelines applicable to the Customer (and its customers) and the data, including under HIPAA, the HITECH Act, the Gramm-Leach-Bliley Act, financial industry guidelines and directives, State privacy laws, EU data-protection directives and similar privacy laws, and other laws, rules, regulations and guidelines
- Depends upon the business criticality of the service and the problems presented by an interruption in data access or delivery

Data Ownership and Vendor's Use

- Ownership
 - Data provided to the Vendor
 - All data resulting from the Vendor's processing of that data
- Vendor use rights
 - Use of aggregated and deidentified data?
 - *For use in security and operational management of the service*
 - *For use in marketing and developing service offerings*
 - Analytics?

Vendor's Data Security Offering

- Vendors typically not willing to offer a customized data security approach
- Customers must conduct gap analysis on Vendor's policies
- Vendors will generally accept obligations to keep their policies consistent with industry standards, but...
- Watch for industry-specific security requirements, which may not be met with non-industry specific cloud offerings
- Due diligence and selection of Vendor is more important than the contract
 - Location of servers, both primary and backup
 - Subcontractors/subprocessors
 - What security certifications does the Vendor maintain?

Customer Access; Vendor Production

- Can the Customer access and retrieve the data at all times (subject to system downtime)?
- If not, can Vendor (and is Vendor contractually obligated) to provide requested data in a timely manner?
- Is the data stored in a format that is useful to the Customer as-is?
- Goals are to enable Customer to comply with its data production requirements and to reduce the ability of the Vendor to hold data “hostage”
 - Timely, reliable access to data
 - Requirement that Vendor return (or enable Customer to recover) data/provide conversion assistance upon request, with equitable relief available for breach

Data Segregation, Retention, and Return

- How is the data stored, both in production and backup environments?
 - Physical segregation: unlikely if not impossible
 - Logically segregated or otherwise identified as Customer's data?
 - Confidentiality – lessens risk of inadvertent disclosure
 - Data integrity
- Some type of segregation, search functions, and/or metadata likely required in order to enable:
 - Customer-specific retention and destruction requirements
 - Ability to require the timely return or secure destruction of specific data
 - Compliance with litigation hold and e-discovery requirements/avoiding spoliation – no exceptions for data in the cloud
- Also consider: is Vendor assistance required to execute instructions as to particular data?

Data Breach and Response

- In the face of a data breach:
 - Investigation, remediation, and appropriate modifications to practices going forward
 - Customer right to participate and control breach notifications/messaging to customers
 - Vendor liability
 - *Vendors are increasingly not agreeing to unlimited liability (in many cases, even for indemnified third-party claims) for a breach of data security obligations*
 - *Separate, higher direct damages cap for breach?*
 - *Consider allowing consequential damages to be recovered up to the amount of the separate damages cap, or predefining certain categories of data breach remediation expenses (e.g., as required by laws applicable to the Customer or the data) as direct damages*

Compliance with Laws Applicable to Customer

- Compliance
 - With laws, rules, regulations, and “guidance” applicable to the Customer and the data
 - *United States and beyond*
 - Current, modified, and new
 - Industry regulations (financial, insurance, pharma, etc.)
 - Import and export issues based on server locations and data flows
- Does the Vendor’s solution match up with the Customer’s needs to stay in compliance with laws? Can it be configured to do so, within existing functionality?
- Challenging negotiations with respect to changes to the cloud that are required for Customer-specific laws and standards

Service Availability: SLAs

- Traditional approach: Negotiated SLAs, with Customer rights to introduce new measurements and detailed reporting
- Cloud Vendor approach: Standard SLA offering and reporting for all Customers
- Vendors unlikely to agree to specific or enhanced SLA metrics. However, consider seeking protection within the SLA definitions:
 - Requiring service to be reasonably responsive to users in order for “uptime” or “availability” to be achieved (no sluggish performance—define minimally acceptable process time)
 - Carefully defining downtime
 - Numbers can be gamed – get an IT expert to review

Service Availability: SLAs

- Credits as exclusive remedy?
- Customer responsible to monitor and report SLA performance and report an SLA failure?

Service Availability: Backup and DR

- Traditional approach: Deal-specific DR plan that takes into account the Customer's own DR plans
- Cloud Vendor approach: Standard DR plan for all Customers; summary available upon request
- As with SLAs, unlikely to achieve any customization. However:
 - Watch the definition of Force Majeure Event, and add the Vendor's execution of its DR plan as an exception to excused performance
 - Define required recovery and restoration time
 - Ask to be given at least the same recovery and restoration priority as other Customers
- Regardless of the contractual remedies, be prepared to address the practical consequences of an interruption, such as a Denial of Service attack
 - Check the Vendor's RTOs and RPOs to confirm that Customer will have a workaround during downtime and the ability to restore data outside the RPO
 - Regular deliveries to Customer of the Vendor's back up files?

Change Management: Vendor-Initiated

- Cloud Vendors want (and need) the ability to make changes without the approval of all Customers
 - Impractical to get all Customers to approve
 - Vendors keeping pace within industry and technological changes
- Unrealistic to expect approval rights, but Vendors will agree to some boundaries:
 - Not material and does not materially degrade the service offering
 - Does not diminish the protections of Customer under the contract
 - Scheduling restrictions on upgrades/downtime (though not as narrow of downtime windows as a non-cloud-based deal)
 - Notice to Customer

Change Management: Customer-Initiated

- More limited rights of Customers to seek changes in a cloud deal, but in some cases Vendors will agree to the following types:
 - Requirement to keep practices (such as data security policies) consistent with industry standards
 - Compliance with generally applicable laws (whether to the solution or to the Vendor's Customer base)
 - What about Customer-specific laws?
- Customizations may not be feasible unless the Customer is willing to pay for a separate, partitioned environment... and the Vendor is willing to create one
- Must the Customer pay for a change?

Unwinding the Deal

- Termination and Suspension
 - When and by whom?
 - Additional rights to terminate in the face of a compliance with law issue that the Vendor cannot (or will not) address?
 - Vendor's rights to suspend services?
 - *Violation of acceptable use policy?*
 - *Nonpayment?*
- Unwinding the Arrangement
 - Data return and conversion assistance
 - Notification and grace period prior to deletion of data
 - Secure erasure



“Right” Sourcing: The analysts are heralding a wave of onshoring. How are companies building flexibility into their contracts to enable “right” sourcing of their onshoring and offshoring mix?

The Press

- New Onshore IT Outsourcing Centers Outnumber New Offshore Locations (*CIO Magazine*)
- Will Banks Keep 'Onshoring' IT Jobs in 2013? (*American Banker*)
- Market Trends: Providers Expand U.S. Onshore Delivery, Invigorate Investments in Low-Cost Domestic and Rural Sourcing Options (*Gartner*)
- 36% of organizations are actively relocating or planning to relocate contact center facilities and the United States is the location of choice for many relocation and/or growth plans (Deloitte Survey)

What We Are Seeing

- It is not an all-offshore or all-onshore model
- Companies are looking at their IT services holistically and strategically determining the right onshore/offshore mix

Strategic Considerations

- Cost/Benefit Analysis
- Onsite Presence
- Customer Facing vs. Back Office
- Language
- Culture
- Legal Requirements
 - Onshore Requirement
 - Import/Export Regulations
- IP issues
- Security/Privacy Concerns
- Public/Customer Demands
- Availability of Skill Sets
- Turnover

Diligence

- References
- Site Visits
- Current Operations and Plans for Expansion
- Personnel
 - Language capabilities
 - Skill sets
 - Turnover
 - Staff retention
 - Background checks

Diligence

- Access
 - Remote access
 - Connectivity
- Audits
- Legal Limitations
 - Type of data
 - IP ownership
- Security and Privacy Requirements
 - What if there is a breach?

Consider All Costs

- Travel
 - Transition
 - Training
 - Governance
 - Audit
- Inflation
- Foreign Exchange Risk
- Compensatory Tax Requirements
- Connectivity
- Security Requirements
- Background Checks

Once Decided – Retain Approval and Flexibility

- Specify the specific sites and services provided from those sites
- Reserve approval of any relocation/reallocation of services
- Reserve right to require a relocation
- Specify events that may require a relocation

Site Approval Is Not Enough

- Require vendor to provide staffing plans
- Designate Onshore/Offshore Mix
 - By service
 - By role
- Require that certain key positions be filled by onshore resources
- What happens if mix is not maintained?

Back Up Sites

- In addition to naming primary sites, any outsourcing agreement should also specifically identify the vendor's backup sites and the type of services that can be provided from such sites
- Backup sites should be subject to the same scrutiny as the primary site (as described above)

Blended Rates

- Some deals include blended rates for roles, for example:
 - \$XXX for XXX role
 - Vendor chooses whether resource is onshore or offshore
 - If so, include mix of onshore and offshore resources
 - Consider whether “landed” resources are onshore or offshore or a different rate

Subcontractors and Staff Augmentation Count

- Understand vendor's solution with respect to its use of subcontractors
- Reserve approval of any subcontractor/scope of services
- Reserve right to require a replacement of subcontractors
- Depending on the services to be provided by subcontractors, consider diligence required on subcontractor sites

Consider Remote Workers

- Does vendor allow personnel to work remotely?
- What security controls are required for remote workers?
- How does vendor ensure compliance with data security and confidentiality requirements when personnel work remotely?

Ticketing and Reporting Tools and Databases

- Will onshore and offshore resources use the same ticketing and reporting tools and databases?
- Are processes in place so that the data entry and use of such tools and databases are consistent?
- Are hours tracked using same codes and tracking tools?
- Do reports consolidate data from onshore and offshore sites?
- Is documentation and are tickets entered and tracked in the same language?

Data and IP Access

- A key issue in determining whether to allow work to be performed offshore is the nature of the data and intellectual property that vendor will have access to.
 - Personal Information
 - Export Control Data
 - Sensitive/Business Critical Intellectual Property
- Data segregation issues: can the customer even control what data will be accessed by vendor?

Reporting

- Resource usage by role and location
- Onshore and offshore ratios and staffing against ratios
- Rate of staff augmentation vs. employees
- Turnover/Retention

Governance of Onshore and Offshore

- Overarching governance layers
- Single point of contact for each delivery center
- Regular meetings and checkpoints
- Key personnel?
- Issue escalation

Conclusion

- Retain flexibility
- Know where the services are being provided
- Understand what data/IP will be shared
- Consider length of new contracts



Service Integration: What it means and how it is impacting the IT outsourcing contract.

Service Integration (SI) Services – An Overview

WHAT is it



WHERE we are seeing it



WHO plays the role



WHY companies are looking at it



HOW it is impacting the outsourcing contract

Sources

1. *Advantages of Service Integration and Management (SIAM) in a Multisourced Operating Model*, Lois Coatney, Director, ISG
2. *Assembling the Jigsaw, Service Integration and Management in a Multisourced IT Operating Model*, Hannah Patterson, Principal Consultant, ISG
3. *Core ITSM*, Brandon Lane CIO
4. *Evolution of IT Service Management in a Multi Sourcing World*, Neha Sharma, TATA Consultancy Services
5. *Joline: Service Integration in a Multivendor Outsourced IT Environment*, Jan Vromant
6. *Play Nice, Facilitating Collaboration in a Multi-sourced Environment*, Lois Coatney, Director, ISG
7. *Service Integration, A blueprint for regaining control of a complex IT vendor landscape*, Capgemini
8. *Service Integration and Management, An Idea Whose Time Has Come*, Jimit Arora, Chirojeet Sengupta, Yugal Joshi, Everest Group Research
9. *Service Integration, Enhancing the Benefits of a Multi-sourced IT Environment*, Phil Brooke and Tony Rawlinson, EquaTerra/KPMG



WHAT is it

Shift in IT Organizations

Traditional silo-based organizations

- Lack of common processes; each IT function/service provider has own processes and performance requirements
- Lack of common tools and integration; minimal data sharing

Organizations with highly integrated set of service, processes, and data

- Service Integration layer is moving up value chain; not just setting processes but enabling strategic decisions across IT functions and creating platform linking business and IT

Shift shaped in part by move to multi-vendor outsourcing models and need to manage multiple vendors with integrated processes and tools

For organizations with retained organizations or full scope outsourcing, integration layer ties together IT functions to address business needs holistically

Shift in IT Organizations

- Many IT environments are made up of software and hardware that each adequately performing its own tasks, but linked together by patchwork processes and customized integration.
 - A change to or issue with respect to one component may have unforeseen and adverse impacts on other parts of the infrastructure, causing risk to availability and performance of IT services
- Service Integration is intended to: *(Tata White Paper)*
 - √ Break down traditional domain silos
 - √ Provide increased visibility for decision makers across the IT environment (as to cost and impact of change)
 - √ Mitigate risks from change requests
 - √ Integrate data from disparate sources and manage rising complexity

What is it

Business Stakeholders



Service Integration

Level 1 Service Desk (Ticket Management)

Data Center

- Servers
- Storage
- DR

Network

- Infrastructure
- Unified Communications

Application Services

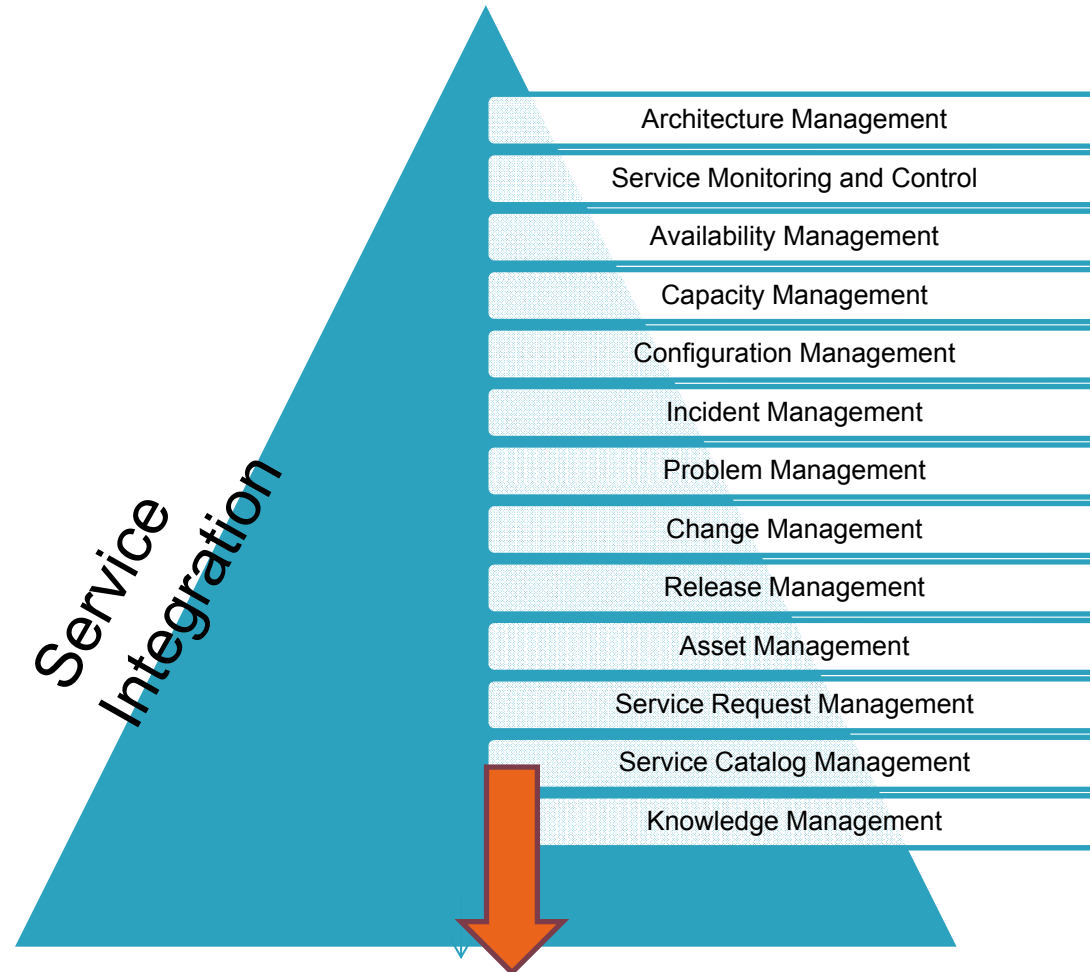
- Maintenance
- Development

End User Services

- Onsite Services
- Remote Services
- Service Desk?

Security?

Common Processes and Repositories



Apprehension

Additional \$\$

- Restructuring organizations
- Identifying processes
- Implementing and training
- Integrating tools
- Sharing data and reports

Response

- Activities currently are being performed by various people/departments spread across the organization
- Service Integration is about **restructuring and consolidating various activities spread all across to a more optimized model**
- Long term benefits

What is it – A look at the industry definitions



KPMG (EquaTerra)

Growing recognition of SI as a service and potentially a function in its own right

- Specific internal function
- Outsourcing as a discrete service

Key Components

- Process standardization and deployment
- Tool/technology standardization
- Driving higher availability, better issue resolution, and service reliability
- Single point of responsibility
- Overseeing compliance with client policies and standards
- Coordination function across towers and service providers
- Monitoring, measuring, and reporting of end to end service

ISG

SI oversees service management processes deployed across the enterprise and enforces compliance

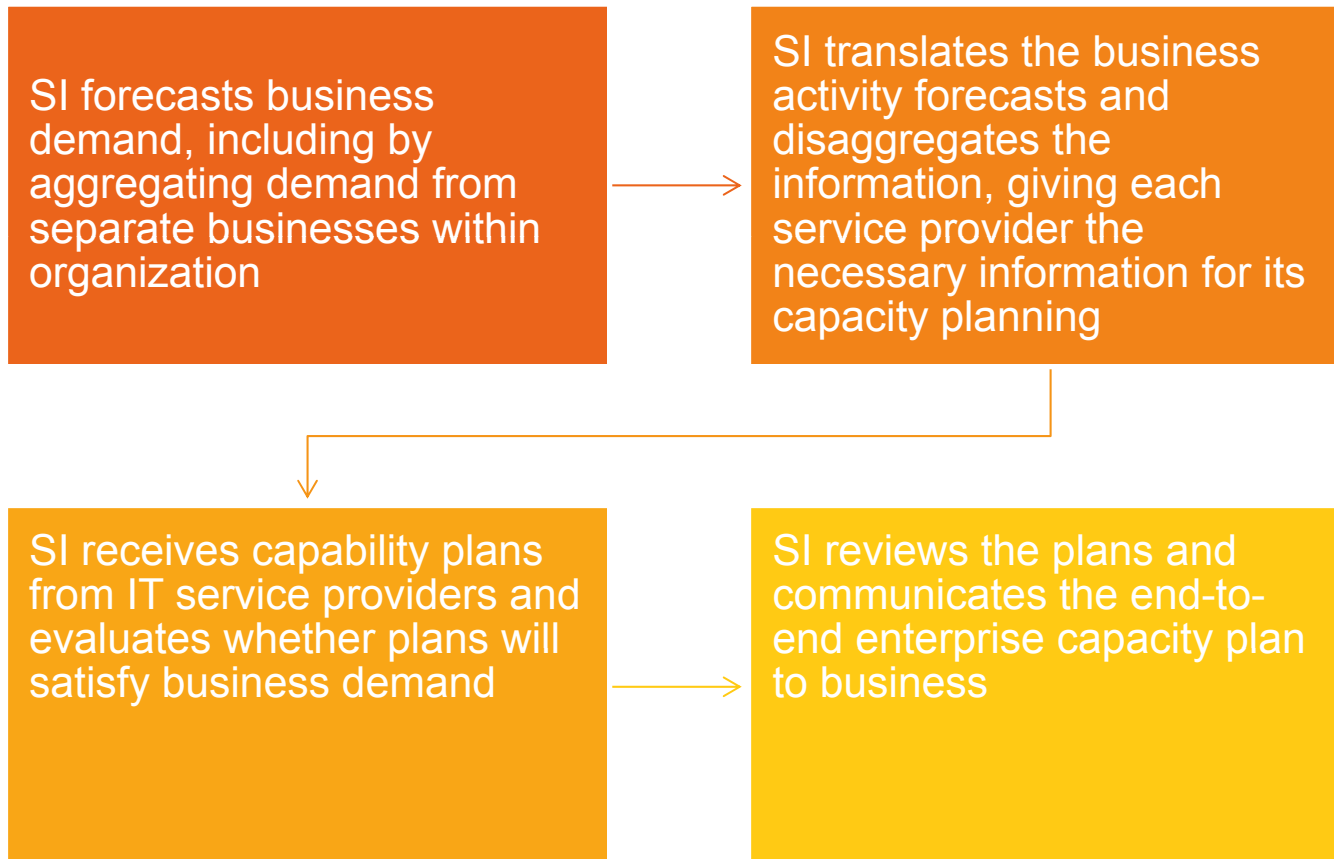
- Ensures that multiple service providers (internal and/or external) deliver services in cohesive and efficient manner
- Maximizes performance of end-to-end IT services to the business

Gatekeeper to enterprise-wide IT services by enforcing change, security accreditation, testing and release processes

- Ensures readiness of changes made to the IT estate
- Enables flexibility in service provider and business landscape by maintaining uniform framework of processes, governance, and supporting tools, including an enterprise-wide configuration management database capturing relationships between business areas and IT services
- Enables effective exit management of providers and the introduction of new providers

Example – Demand and Capacity Management

Assembling the Jigsaw, Service Integration and Management in a Multisourced IT Operating Model, Hannah Patterson, Principal Consultant, ISG



WHERE we are seeing it

Where we are seeing it

Full scope (or almost full scope)
IT outsourcing that calls out SI as
a separate tower or service line
(separate scope and pricing)

- Implementing standard processes and repositories
and setting the stage for breaking out the function

Retained function that manages
multiple vendors

Stand alone third- party service?

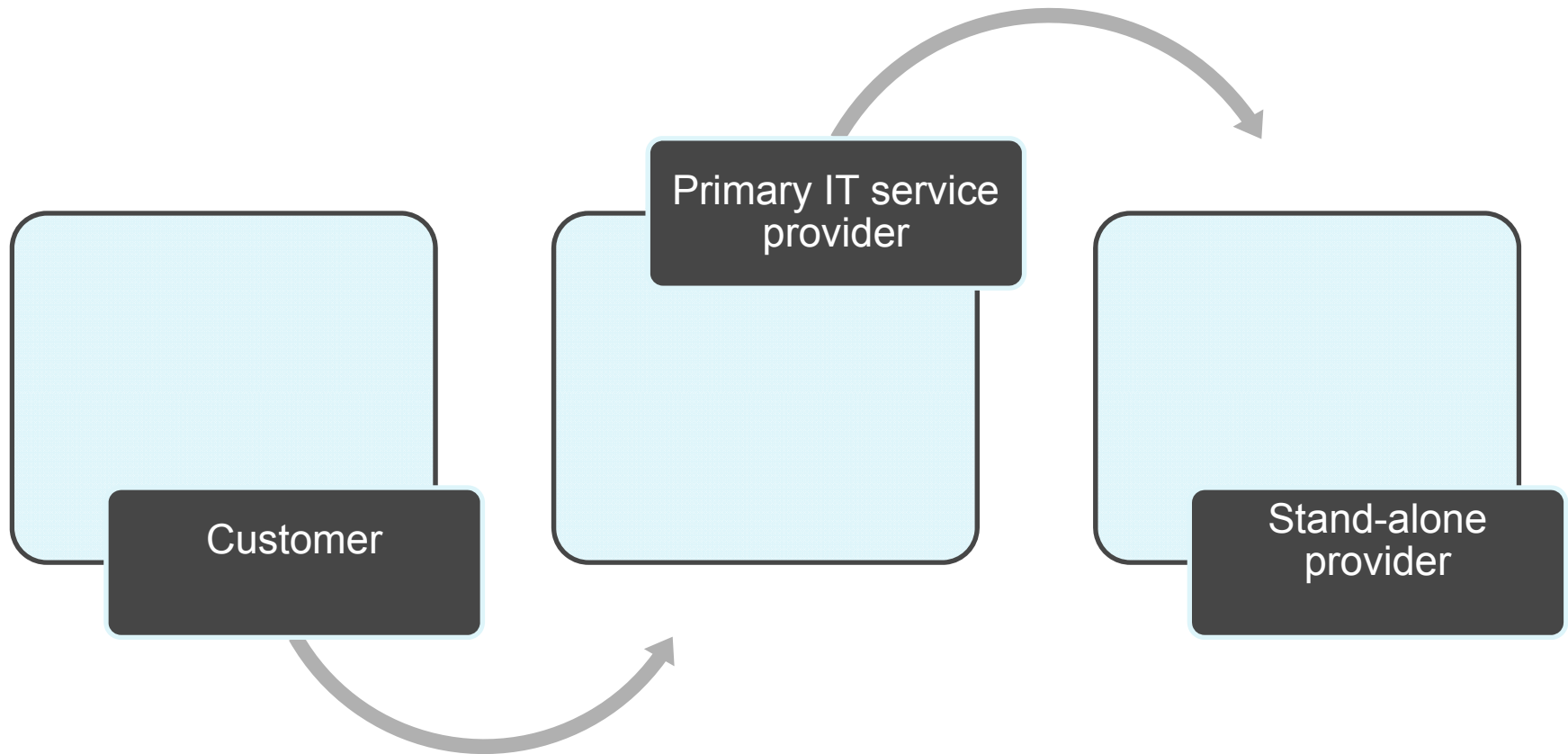
Requires understanding
across all IT functions
and across business

- Communication and training
- Standard procedures
- Access to and use of
integrated tools
- Shared information
- Cross-function reporting
- Collaborative governance
meetings



WHO plays the role

Who plays the role



Who plays the role

SI held responsible for own performance and monitors and reports on other suppliers

SI held responsible for end to end issue resolution and coordination

SI held responsible for end to end service levels with penalties for missed performance

Risk borne by SI provider must be aligned with level of authority it will have over other suppliers

WHY companies are looking at it

Trying to address ...

Assembling the Jigsaw, Service Integration and Management in a Multisourced IT Operating Model, Hannah Patterson, Principal Consultant, ISG

- ✓ Redundant governance
- ✓ No one IT view; siloed operations
- ✓ Lack of standard processes and tools
- ✓ No one point of accountability
- ✓ Misaligned SLAs
- ✓ No incentive to collaborate across service providers

Issues fall into the gaps between service providers, leading to finger-pointing and poor overall performance

Restoration times at risk as service providers determine which service is down and who is responsible

Focus is on attributing blame rather than identifying root cause

No consistent escalation and issue resolution processes followed across IT functions

More examples of specific issues arising from lack of integration ...

- ✓ Releases made into production environment without sufficient testing and IT-wide awareness
- ✓ Ineffective or incomplete understanding of interdependencies between each component service, resulting in poor risk management (e.g., security, availability)
- ✓ Finance overwhelmed by different invoices from service providers
- ✓ Poor coordination between service providers for incident resolution, disaster recovery, and test environment provision
- ✓ Lack of understanding of the relationships between business and technical services, resulting in irrelevant SLA reporting, failure to meet required business outcomes, and an inability to assess the potential impact of changes
- ✓ Numerous level 1 help desks for users to call
- ✓ Businesses holding direct relationships with service providers, causing the client's IT department to have limited visibility of requests made and services provided
- ✓ Duplicated efforts when businesses request additional services that are designed in silos

Assembling the Jigsaw, Service Integration and Management in a Multisourced IT Operating Model, Hannah Patterson, Principal Consultant, ISG

Intended to provide ...

Standard
practices

Better services

Better
communications

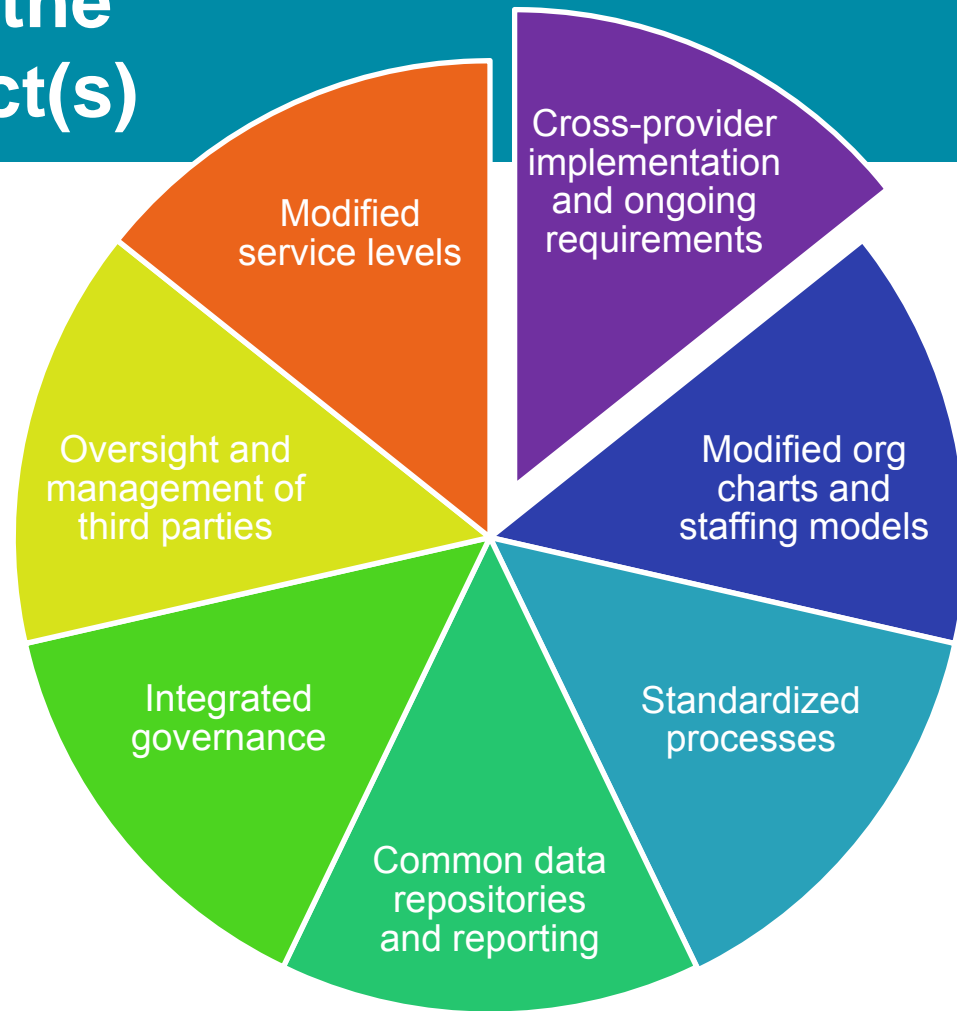
Continuous
improvement

Innovation



HOW it is impacting the outsourcing contract

How it is impacting the outsourcing contract(s)

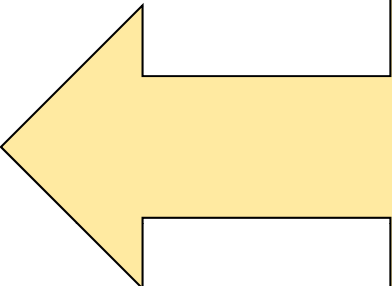


Stand-alone SI Scope

- Stand-alone statement of work
 - Separate scope
 - Separate staffing
 - Separate pricing
 - Separate termination rights
- Include tool implementation and maintenance?

Cross-provider requirements

- **Cooperation**



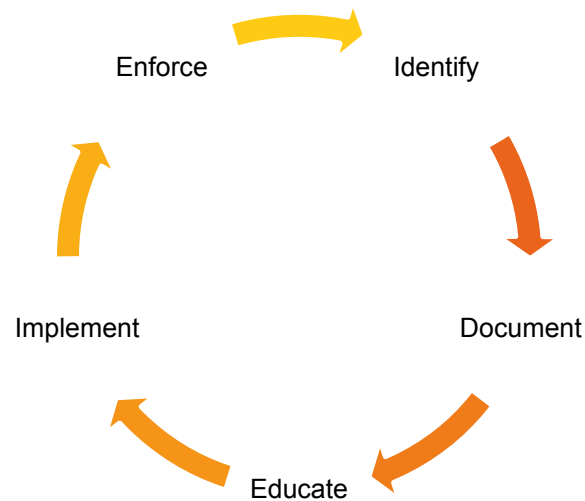
After deciding on the sourcing strategy and service integrator role, customer to enter into an **open dialogue with several suppliers.**

The focus of the cooperation is aimed at the future and on the transformation.

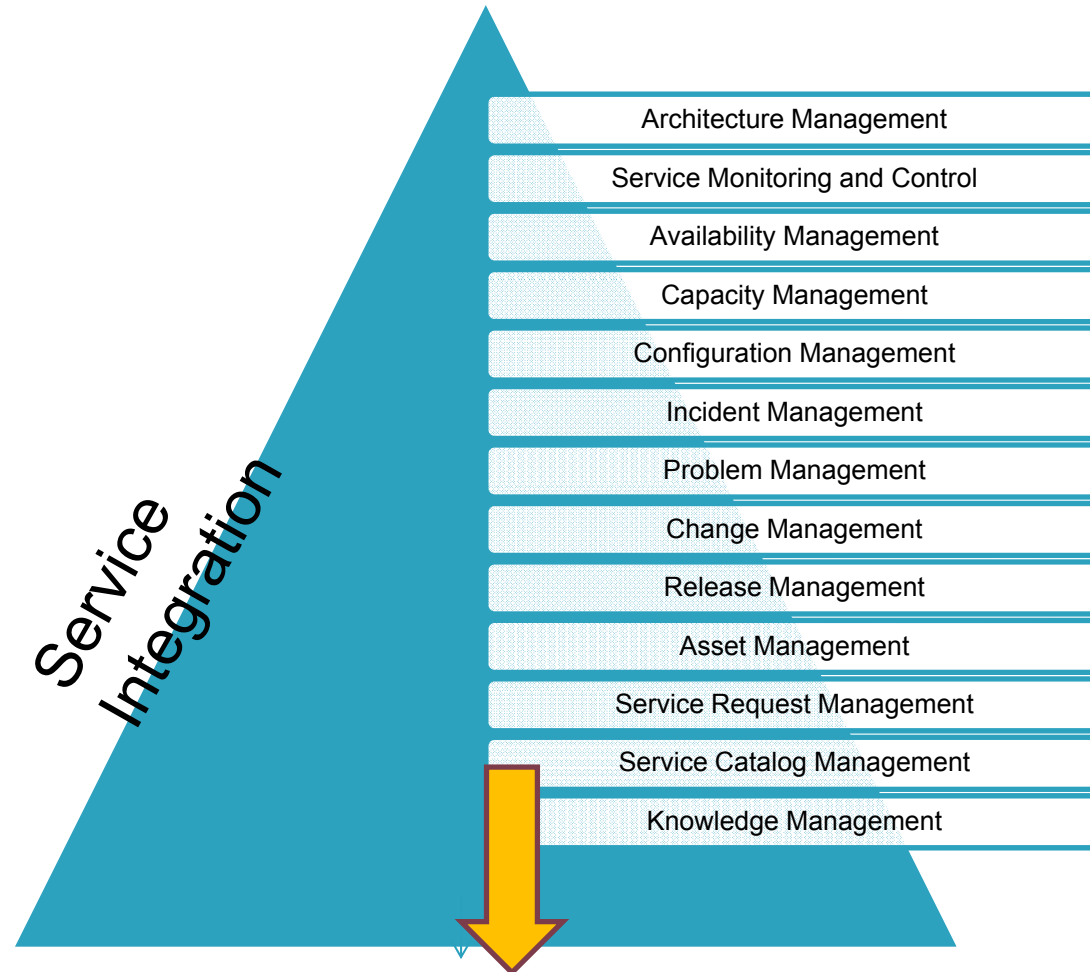
- **Communication and Training**

Cross-provider requirements

- Organizational charts and staffing models
 - Staffing of the SI organizations
 - Changing the staffing and reporting lines
- Standardized processes



Standardized Processes



Common Data Sources

✓ Who holds licenses to tools

✓ During term

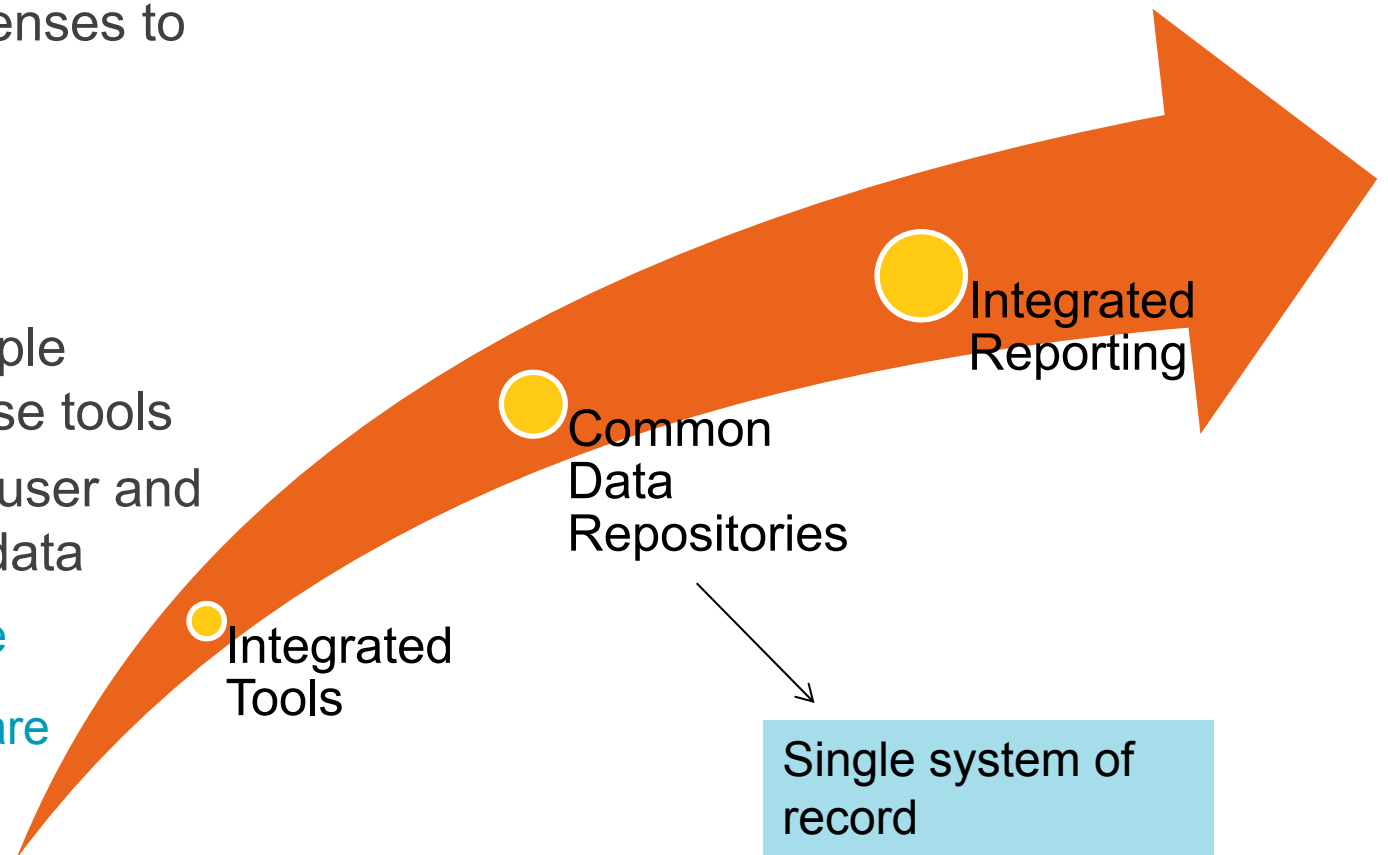
✓ Post term

✓ Right for multiple providers to use tools

✓ Ownership of user and performance data

✓ Right to use

✓ Right to share



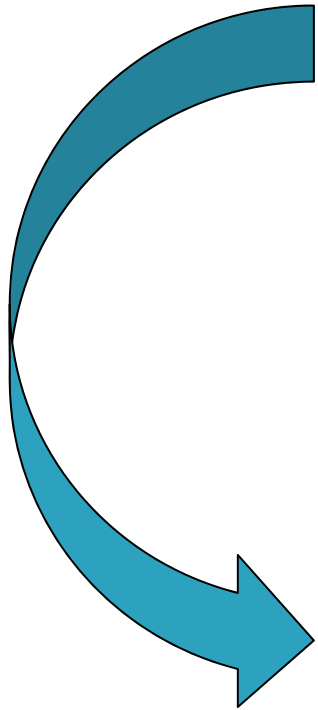
Integrated Governance

- Management across providers
 - cross-provider governance forums to manage performance, issues, and decisions
- Score Cards
 - process performance evaluation within each provider's performance scorecard, and address operational performance jointly across providers
- Shared reporting and monitoring

Modified Service Levels

- End to end service levels

- Oversight and tracking across vendors
 - » Add right to allow for this!
- With one system of record
- Align “excuse” language with level of accountability



Issue
Resolution

Availability

Conclusion

An IT-wide initiative that needs to be embraced by all components

May take some upfront work to communicate and implement (part of transition/transformation)

Adjustment to current and future contract provisions to ensure that the model is reflected and can be implemented



international presence

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

*In association with Mohammed Buhashem Advocates & Legal Consultants